



CERTIFIED  
MISSION CRITICAL  
OPERATOR

TONY ROSSI

PAUL TANKEL

STUDENT MANUAL

---

# Certified Mission Critical Operator

# Certified Mission Critical Operator

# Certified Mission Critical Operator

Part Number: 099001

Course Edition: 1.0

## Acknowledgements

### PROJECT TEAM

<i>Authors</i>	<i>Media Designer</i>	<i>Contributing Editor</i>	<i>Content Editors</i>	<i>Content Manager</i>
Tony Rossi	Brian Sullivan	Lindsay Bachman	Michelle Farney	Tim Barnosky
Paul Tankel			Tricia Murphy	

## Notices

### DISCLAIMER

Content created for Cleveland Community College by Logical Operations, Inc. While Logical Operations, Inc. takes care to ensure the accuracy and quality of these materials, we cannot guarantee their accuracy, and all materials are provided without any warranty whatsoever, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. We do not believe we have used anyone's name in creating this course, but if we have, please notify us and we will change the name in the next revision of the course. Logical Operations is an independent provider of integrated training solutions for individuals, businesses, educational institutions, and government agencies. The use of screenshots, photographs of another entity's products, or another entity's product name or service in this book is for editorial purposes only. No such use should be construed to imply sponsorship or endorsement of the book by nor any affiliation of such entity with Logical Operations. This courseware may contain links to sites on the Internet that are owned and operated by third parties (the "External Sites"). Logical Operations is not responsible for the availability of, or the content located on or through, any External Site. Please contact Logical Operations if you have any concerns regarding such links or External Sites.

### NOTICES



This workforce product was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The product was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The U.S. Department of Labor makes no guarantee, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites and including, but not limited to, accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability, or ownership.



National Consortium for Mission Critical Operations (NCMCO) Curriculum is licensed under Creative Commons Attribution 3.0 Unported license.

Unless otherwise noted, this work was created by Cleveland Community College and is licensed under Creative Commons Attribution 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by/3.0> or send a letter to Creative Commons, 444 Castro Street, Suite 9.

Any images requiring citation have been attributed accordingly and, where possible, a link to its location on a publicly-accessible repository has been provided. All images without citations have been taken from the public domain or were expressly created for this courseware.

Logical Operations and the Logical Operations logo are trademarks of Logical Operations, Inc. and its affiliates.



# Certified Mission Critical Operator

<b>Lesson 1: Overview of MCOs.....</b>	<b>1</b>
Topic A: Mission Critical Operations.....	2
Topic B: Mission Critical Industries.....	23
Topic C: MCO Careers.....	37
Topic D: Design Parameters and Considerations.....	43
<b>Lesson 2: Mission Critical Infrastructure: Power and Power Sources.....</b>	<b>51</b>
Topic A: Power Fundamentals.....	52
Topic B: Utility–Source Power.....	67
Topic C: Generator–Provided Power.....	73
Topic D: Uninterruptible Power Supplies.....	81
Topic E: Batteries.....	87
Topic F: Alternative Power Sources.....	91
<b>Lesson 3: Mission Critical Infrastructure: Power Distribution.....</b>	<b>101</b>
Topic A: Medium vs. Low Voltage Systems.....	102
Topic B: Redundancy.....	111
Topic C: Power Supply Transfer.....	116

Topic D: Power Distribution Topologies.....	121
Topic E: Electrical Protection.....	125
Topic F: Power Distribution Preventative Maintenance.....	133
<b>Lesson 4: Mission Critical Infrastructure: HVAC.....</b>	<b>139</b>
Topic A: HVAC Fundamentals.....	140
Topic B: Refrigerant-Based Cooling Systems.....	153
Topic C: Water-Based Cooling Systems.....	157
Topic D: Alternative Cooling Systems.....	163
Topic E: Air Circulation.....	168
Topic F: HVAC Preventative Maintenance.....	176
<b>Lesson 5: Mission Critical Infrastructure: Plumbing and Other Mechanical Systems.....</b>	<b>181</b>
Topic A: Water Supply and Drainage.....	182
Topic B: Secondary Systems.....	190
Topic C: Plumbing and Other Mechanical System Preventative Maintenance.....	198
<b>Lesson 6: Mission Critical Infrastructure: Fire Safety, Systems, and Equipment.....</b>	<b>203</b>
Topic A: Fire Detection.....	204
Topic B: Fire Suppression.....	212
Topic C: Building Construction and Fire Prevention.....	220
Topic D: Exit and Emergency Lighting.....	226
Topic E: Emergency Power Off System.....	229
Topic F: Fire Systems Preventative Maintenance.....	232
<b>Lesson 7: Personal Safety and Emergency Response.....</b>	<b>237</b>
Topic A: Common Hazards and Personnel Protection.....	238
Topic B: Emergency Response Procedures.....	253



<b>Lesson 8: Facility Security</b> .....	<b>273</b>
Topic A: Physical Security.....	274
Topic B: Access Control Systems.....	290
Topic C: Security Procedures.....	296
<b>Lesson 9: Critical Production Spaces</b> .....	<b>305</b>
Topic A: Data Center Best Practices.....	306
Topic B: Data Center Air Flow Management Techniques and Strategies.	317
Topic C: Cabling and Cable Management.....	324
Topic D: Manufacturing and Other Critical Spaces.....	333
<b>Lesson 10: Networking</b> .....	<b>337</b>
Topic A: Basic Network Components.....	338
Topic B: Basic Networking Concepts.....	349
Topic C: Network Types.....	362
<b>Lesson 11: Communication Systems</b> .....	<b>373</b>
Topic A: Wired Systems.....	374
Topic B: Wireless Systems.....	377
<b>Lesson 12: Environmental and System Monitoring</b> .....	<b>387</b>
Topic A: Systems and Equipment Parameters.....	388
Topic B: Metering.....	396
Topic C: Monitoring Platforms.....	403
Topic D: Outputs and Reports.....	407
Topic E: Controls.....	417
<b>Lesson 13: Operations and Procedures</b> .....	<b>425</b>
Topic A: Organizational Structure.....	426

Topic B: Operating Procedures.....	430
Topic C: Change Management.....	436
Topic D: Regulations, Standards, Guidelines, and Compliance.....	445
<b>Lesson 14: Facility and System Documentation.....</b>	<b>455</b>
Topic A: Documentation Types.....	456
Topic B: Operating and Maintenance Manuals.....	468
Topic C: Testing Reports.....	473
<b>Appendix A: Certified Mission Critical Operator (CMCO) Certification</b>	
Exam MCO-001 .....	481
<b>Appendix B: Common Engineering Units and Conventions.....</b>	<b>489</b>
<b>Appendix C: Uptime Institute Tier Classifications.....</b>	<b>491</b>
<b>Appendix D: Certified Mission Critical Operator (CMCO) Certification</b>	
Exam Acronym List.....	493
<b>Appendix E: Additional Resources.....</b>	<b>497</b>
<b>Glossary.....</b>	<b>499</b>
<b>Index.....</b>	<b>517</b>

# About This Course

In 2013, President Barack Obama signed Executive Order 13636: *Improving Critical Infrastructure Cybersecurity* and issued Presidential Policy Directive 21: *Critical Infrastructure Security and Resilience*, directing national attention and promising government response to the various threats that pose a risk to critical national infrastructure. While these kinds of cybersecurity threats are a serious issue, they aren't the only concerns related to national security, economic stability, and public safety—organizations, businesses, and even individual people all rely on the mission critical systems that maintain the continuous operation of key telecommunication, financial, medical, production, and emergency response systems. It is therefore equally critical to develop and maintain a workforce trained to ensure the continual operation of such processes and systems.

The *Certified Mission Critical Operator (CMCO)* courseware is an all-encompassing Mission Critical Operations curriculum designed for individuals interested in pursuing a potential career in MCOs. It covers the fundamental skills and concepts required to design, operate, monitor, and maintain the key components, systems, and spaces within a mission critical facility.

## Course Description

### Target Student

This course is designed for first-year students in a Mission Critical Operations degree or certificate program who require the foundational knowledge necessary to understand the systems, design, construction, operation, monitoring, reporting, and emergency response requirements of mission critical facilities.

### Course Prerequisites

As this is an introductory level course, there are no specific prerequisites unless otherwise determined by individual educational institutions.

### Course Objectives

In this course, you will acquire the foundational knowledge and develop the necessary skills to oversee the design, operation, monitoring, and maintenance of mission critical facilities and their associated systems.

You will:

- Identify Mission Critical Operations.
- Identify and describe the power sources relevant to Mission Critical Operations.
- Identify and describe power distribution as it pertains to Mission Critical Operations.
- Identify and describe the heating, ventilation, and air conditioning components within a mission critical facility.

- Identify and describe plumbing and other mechanical systems present in a mission critical facility.
- Identify and describe the fire safety, systems, and equipment integral to a mission critical facility.
- Identify and apply personal safety and emergency response protocols and procedures.
- Identify and apply best practices, strategies, and techniques for establishing and maintaining security for a mission critical facility.
- Identify and apply industry best practices, strategies, and techniques for the proper design and configuration of critical production spaces.
- Identify and apply networking fundamentals as they apply to a mission critical facility.
- Identify and apply communication systems as they apply to a mission critical facility.
- Identify and apply industry best practices and standards for environmental and system monitoring within a mission critical facility.
- Identify and apply industry standards regarding operations and procedures within a mission critical facility.
- Identify and apply industry standards regarding facility and system documentation within a mission critical facility.

## How To Use This Book

### As You Learn

This book is divided into lessons and topics, covering a subject or a set of related subjects. In most cases, lessons are arranged in order of increasing proficiency.

The results-oriented topics include relevant and supporting information you need to master the content. Each topic may contain various types of activities designed to enable you to solidify your understanding of the informational material presented in the course. Information is provided for reference and reflection to facilitate understanding and practice.

At the back of the book, you will find a glossary of the definitions of the terms and concepts used throughout the course. You will also find an index to assist in locating information within the instructional components of the book.

### As You Review





Any method of instruction is only as effective as the time and effort you, the student, are willing to invest in it. In addition, some of the information that you learn in class may not be important to you immediately, but it may become important later. For this reason, we encourage you to spend some time reviewing the content of the course after your time in the classroom.

### As a Reference

The organization and layout of this book make it an easy-to-use resource for future reference. Taking advantage of the glossary, index, and table of contents, you can use this book as a first source of definitions, background information, and summaries.

## Course Icons

Watch throughout the material for the following visual cues.

<i>Icon</i>	<i>Description</i>
	A <b>Note</b> provides additional information, guidance, or hints about a topic or task.
	A <b>Caution</b> note makes you aware of places where you need to be particularly careful with your actions, settings, or decisions so that you can be sure to get the desired results of an activity or task.
	<b>Video</b> notes show you where an associated videos is particularly relevant to the content.
	<b>Social</b> notes remind you to check for opportunities to interact with the online community using social media.



# 1

# Overview of MCOs

## Lesson Objectives

In this lesson, you will identify Mission Critical Operations. You will:

- Identify and describe Mission Critical Operations.
- Identify mission critical industries.
- Identify careers available in the MCO industries.
- Identify the important design parameters and considerations regarding a mission critical facility.

## Lesson Introduction

When you think about the national infrastructure, there are probably quite a few systems or organizations that you consider absolutely crucial for the safety, security, and continued prosperity of the nation. They are imperative for the day-to-day operations of all the different cogs in the machine that is the United States. And they need to work seamlessly together to keep the machine chugging along.

In short, these are all part of Mission Critical Operations (MCOs). As a Mission Critical Operator, you will need to have a strong understanding of all the elements of MCOs, the roles they play, and what to do when anything threatens their continued operations. In this lesson, you will identify those elements of Mission Critical Operations and the possible threats that put those operations at risk.

# TOPIC A

## Mission Critical Operations

Mission Critical Operations are, by definition within their own name, critical. But what exactly are "Mission Critical Operations"? What is unique about these tasks or activities that make them so crucial to the proper functioning of an organization or facility?

As a Mission Critical Operator, you will need to understand numerous complex concepts relating to these critical operations. But, first, it is important to identify what comprises Mission Critical Operations, the role they play, and why they are not just important, but imperative, within an organization. Here, you will identify Mission Critical Operations and why they are, in fact, "critical."

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- MCOs
- Critical infrastructure
- Threat
- Controls
- Networking
- IT
- Security
- Procedures
- Policies
- Documentation
- Crisis
- Crisis management
- Risk management

### What are MCOs?

*Mission Critical Operations (MCOs)* are just that—actions, processes, and systems that enable the execution of the integral functions of a business or organization. Simply put, the litmus test to identify MCOs can be: if this "thing"—a specific task, process, or system—broke or stopped working, would this hinder or cripple the continued ability of the organization to meet its goals?

MCOs are classified as such because of their functions within an integral system, not their standalone characteristics. For instance, the emergency generator at an air traffic control tower is absolutely mission critical, whereas a backup generator for your local sporting goods store is not. The consequences of the same component failing are vastly different: the loss of the former during a power outage poses a tremendous, imminent threat to the safe landing of airplanes, but the loss of the latter during a power outage will probably only result in the store closing early and losing some sales. The two are simply not comparable in the severity of their impact.

There are some systems and processes that are fairly unique to MCOs because they create reliability and safety for the systems and processes crucial to the success of the larger entity. Regardless of how commonplace or unique the component may be, MCOs are united by the fact they are the fundamental building blocks that allow an organization to deliver a service with little or no possibility for error, downtime, or any other type of interruption.

### Critical Infrastructure

*Critical infrastructure* refers to the physical systems that are put together that allow an organization to fulfill its purpose in delivering an important product or service.



Non-physical items such as specific procedures or safety programs might be considered characteristics of the critical infrastructure of MCOs, but in this sense, critical infrastructure focuses on the physical pieces of equipment that make up the mission critical system, including systems networks. Largely speaking, infrastructure is grouped into common categories such as power distribution, mechanical systems, controls, networking, safety, and security—components you are likely to recognize from other, non-MCO industries. However, it's how these systems are designed to be robust and reliable—along with the high level of operational attention to detail—that sets them apart as mission critical.

## Threats

A *threat* is anything that can potentially cause damage or harm to a person or object. A threat can be environmental in nature, the result of faulty equipment, or human-created in the form of accidents, negligence, or nefarious activities.

Considering the possible threats posed to the people, property, or systems within a mission critical facility is an important part of both the design and implementation of MCOs. Within reason, you should always assess the potential threats to MCOs and plan for as many as is practical. This is equally important in design, construction, and day-to-day sustained operations within a facility.



**Figure 1-1:** A hurricane—as evidenced by the damage seen here caused by Hurricane Katrina—can be a potential threat to MCO facilities. (Source: Federal Emergency Management Agency/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Hurricane\\_katrina\\_damage\\_gulfport\\_mississippi.jpg](https://commons.wikimedia.org/wiki/File:Hurricane_katrina_damage_gulfport_mississippi.jpg))

## Mission Critical Systems and Their Roles

In the mission critical world, there is almost never a single piece of equipment—or even one, stand-alone system—that constitutes the whole of MCOs in a given facility. Therefore, it is important to understand the concept of a system as a set of interconnected "things" or components that come together to form a more complex whole. A fundamental building block of MCOs is simply

understanding that these components, in any combination, come together to create a more complicated system that serves a mission critical purpose.

Within MCOs, these various systems work together to perform mission critical functions and are often connected to each other, via design and/or their operators, by various systems of process and procedure. More often than not, MCOs within a mission critical facility include the following systems.

<b>System</b>	<b>Description</b>
Power	<p>Mission Critical Power Systems cover an immense spectrum of designs and components, but really only fulfill two purposes: deliver power to equipment performing mission critical tasks or distribute power from generation sources. In power delivery, this often starts at the utility connection itself, moving through conductors, breakers, backup sources, and more, all the way to the smallest component power supplies. Conversely, in power generation facilities or even local emergency backup sources, Mission Critical Power Systems may begin at a nuclear reactor or solar panel and move through conditioning and distribution gear out to the grid or back through onsite systems.</p> <p>In regards to power as part of MCOs, it is important to remember two things: not all power equipment onsite is part of a Mission Critical Power System and not all components connected to a Mission Critical Power System perform or support MCOs.</p>
Heating, Ventilation, and Air Conditioning	<p>When it comes to MCOs, Heating, Ventilation, and Air Conditioning (HVAC) refers to far more than just the comfort and cooling most commonly associated with the term. There are indeed critical people spaces that require proper heating and cooling, but MCO HVAC systems are critical components themselves or provide temperature control for the primary MCOs.</p> <p>Each of the three sub-components of HVAC are indeed integral to MCOs. Heat itself can be a power source or a means for capturing efficiencies in many other MCO settings. Cooling is of critical importance for MCOs, as it removes heat from increasingly powerful modern technologies. And, the movement and quality of air in spaces may be a primary mission critical system for some specific scenarios, such as ultra-clean manufacturing or research applications.</p>
Plumbing and other Mechanical Systems	<p>Not all the mechanical attention goes to air and cooling systems—there is a wide selection of other mechanical systems that carry out mission critical functions or directly support MCOs. Plumbing itself is an often overlooked mission critical system, whether in regards to drains for cooling tower run-off or collection and pumping of process chemicals and water.</p> <p>Secondary mechanical systems may include compressed air or gas generation equipment, natural gas supplies, and other commonly considered systems. This broad category of systems also includes those with less general public awareness such as radiation (generation or control) systems and large-scale vacuum systems.</p>
Safety and Security	<p>Safety and security work in tandem in most mission critical settings, as security teams tend to be a first line of response to safety issues concerning general site occupants. While an increasing percentage of large, 24/7 MCOs have dedicated safety <i>and</i> security personnel or teams, the operations group always has responsibility in both areas, ensuring the safe operation of and secure access to equipment and systems.</p>

<b>System</b>	<b>Description</b>
Controls	<i>Controls</i> refers to the systems that monitor, report, and manipulate site equipment and networks. Legacy facilities may only have passive controls systems that monitor and record points of data, whereas large modern production facilities may have fully automatic controls systems that operate machinery and correct alarming conditions without human interaction. As the Internet of Everything—the growing network of objects that are digitally connected and able to exchange data—almost anything with electronic components can now interact with expansive networks. With this in mind, a comprehensive discussion of controls within MCOs should include these general components and design theory for the more common controls systems found in MCOs.

Thinking about mission critical systems both as a collection of these various systems and as a single, wholly functioning system is fundamental to mission critical facility design and necessitates operators that are aware of and knowledgeable about each system individually and of the interconnectedness between systems. As more and more critical operations systems become more interconnected and even automated, an emphasis on a systems-centric approach is equally likely to become a prevailing force in the MCO industry.

## Case Study: MCO Failures

Unfortunately, there are a lot of examples of MCO failures throughout history that illustrate just how important it is to maintain the critical operations of MCO facilities and the disastrous consequences that occur when systems fail. One such event was the partial nuclear meltdown at Three Mile Island in late March of 1979.

Three Mile Island, just outside of Harrisburg, Pennsylvania, was home to two working nuclear reactors that provided commercial nuclear energy to hundreds of thousands of American homes. On March 28, 1979, with the first unit powered down for refueling purposes, the second unit experienced a fairly common blockage; but that blockage, in combination with numerous human-related and system-design errors, would eventually result in a full loss of the second unit and a near nuclear meltdown.

The accident started nearly a full 11 hours before the actual nuclear meltdown event in the secondary, non-nuclear system that supports the nuclear reactor itself. There was a blockage in one of the filters that cleans the water used to cool the system, which operators used compressed air in an attempt to unblock. However, they were unaware that a check valve within the system had become stuck open because a key light on the system's control panel falsely indicated that the valve was closed; when the compressed air was used to clear the blockage, the cooling water made its way past the stuck-open valve and into an instrument air line. This would eventually cause the pumps that fed water into the steam generator that fed the cooling system to turn off hours later, which increased heat and pressure in the reactor coolant system and caused the unit to perform an emergency shutdown.

But the problems didn't end there: when the emergency shutdown occurred, control rods were automatically inserted into the nuclear core to halt the chain reaction, but decay heat was still being created and wasn't being removed from the system because of the unknown issues in the water loop. Auxiliary pumps were automatically activated by the process to pump water into the system, but the valves used within the pumps had been closed for routine maintenance—an action that was a flagrant violation of key regulatory rules. The increasing heat and pressure, and the inability for the secondary system to intervene, caused the automatic opening of a relief valve, which should have closed once the heat and pressure had been released. But, of course, the relief valve was experiencing its own mechanical failure and was also stuck open, allowing coolant water to enter the nuclear reactor itself, and resulting in the partial nuclear meltdown of Unit 2.

Once the partial meltdown occurred, it was possible that radioactive materials were released into the environment. While some reactive gases were definitely released, in the initial investigations after the

accident, the plant ownership deemed it unlikely that any dangerous levels of radiation had been allowed to reach the community. However, residents were urged to stay indoors and, as a precaution, the Governor called for a voluntary evacuation of the local population—though all of these emergency efforts took place *days* after the actual event. Unit 2 was subsequently decommissioned and remains permanently shut down to this day, while Unit 1 continues to generate nuclear power.

What was most troubling about the Three Mile Island accident were the system design errors and human errors that allowed such an event to occur in the first place. The light that signaled the stuck-open valve should have indicated the problem. But, beyond that, the operators should have realized that the continuing problems were indicative of a larger problem, rather than going on the assumption that the faulty light was correct and allowing hours to go by before a different shift of operators came on duty and were able to correctly diagnose the problem.

Fortunately, a complete MCO failure of this nature could have resulted in far worse consequences, including major casualties to both the general population and the environment. But what was learned from the Three Mile Island accident was just how important it is to have a complete understanding of the various components of a mission critical system and the need for operators to be aware of the interdependence of these components—and how a failure of one component can have devastating effects on the rest of the system.

# ACTIVITY 1–1

## MCO Failures: Reflective Questions

### Scenario

Based on the previous case study, think about the following questions in regard to how this specific scenario relates to Mission Critical Operations.

1. What does the Three Mile Island accident tell you about the importance of MCOs?
  
  
  
  
  
  
  
  
  
  
2. What kinds of protocols could have been put in place at Three Mile Island to help prevent the disaster in the first place or to mitigate the resulting damages?

## Elements of MCOs

There are five key elements of MCOs that tie together the various systems that make up the mission critical environment. These elements include:

- Networking and IT
- Security
- Policies and procedures
- Documentation
- Crisis management

## Networking and IT

*Networking* refers to the system of computers and other assorted hardware and software components that are connected together to allow for the communication of data and information between devices. It is part of a broader category of *Information Technology (IT)*, which is the broad application of computer devices and other communications equipment that are used to deliver, receive, and store data or other types of information.

There used to be a fairly clear public distinction between networks and IT, but with the regularity of data connections across so much of the developed and developing world now, and so few truly stand-alone information/data systems, modern IT simply doesn't exist without the networks that connect all these digital components. This holds true for MCO environments as well, where the understanding and coordination of the networking and IT components that are part of a mission critical environment are integral to both the proper design and proper operation of a mission critical system.



**Figure 1–2: Server racks in a data center, which is often the heart of IT infrastructure for a facility.** (Source: Global Access Point/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Inside\\_Suite.jpg](https://commons.wikimedia.org/wiki/File:Inside_Suite.jpg))

## The Role of IT in MCOs

Twenty-first century MCOs simply do not exist without a massive amount of IT infrastructure. Even some of the more dated installations still in operation have been retrofitted with newer electronic equipment that needs to communicate with each other and with humans, and needs to be able to store and analyze incredible amounts of data.

At the very least, all MCOs use technology, and therefore rely upon IT systems and networks. Some mission critical facilities exist for the sole purpose of creating and operating these vast IT systems, such as data centers, which are perhaps the most rapidly growing category of mission critical facilities. Additionally, these data processing and storage facilities enable the modern application of other MCOs, which would not exist on their own without access to the scale and power they provide.

For example, consider the vast amount of important patient data that is transmitted and stored on a daily basis in a hospital. This mission critical environment clearly needs vast amounts of IT support to ensure that all of that important information is safely stored, secured, and accessible whether the facility is operating normally or experiencing any kind of interruptive event.

## Case Study: IT Failures

IT failures can have disastrous effects on the day-to-day operations of critical organizations. Take, for instance, the three-hour outage in 2013 that brought the NASDAQ stock exchange to a screeching halt at the height of trading hours.

Trades on the various stock exchanges are conducted primarily via data feeds between the respective exchanges' platforms. A reliable, consistent connection between them is essential for trading to occur; essentially, NASDAQ's day-to-day operations is entirely reliant on the stability of its IT infrastructure. Unfortunately, a number of IT-related issues would be to blame for the hours-long

outage that prevented trading communications between the various platforms that process quotes and trades for the stock exchanges.

It started with a flood of data from the New York Stock Exchange's Arca platform to NASDAQ's Securities Information Processor (SIP), which swamped SIP's capabilities. Unfortunately, this massive data dump uncovered a fatal flaw in SIP's software code: the stream of data overpowered the system, rendering it incapable of triggering its backup system and, as it was unable to failover, there was an outage. Because these two platforms communicate quotes and trade data between one another, trading essentially ground to a halt for the duration of the outage. Without a backup system in place to handle transactions and processing during the outage, trades had to come to a complete stop. While it only took about 30 minutes for the data feeds to be repaired and fully operational, it took more than three hours of testing and evaluation before actual trading could resume.

While it is unknown how many trades the outage affected or prevented, you can do some simple math to estimate its effect. Data taken from a few years before the outage shows that the NASDAQ SIP processed an average of about 6.25 million trades per day; that equates to about 1 million trades per hour during open market hours. So, for the three-plus hours that the system was experiencing its outage, more than three million trades were unable to be processed. In the grand scheme of things, the NASDAQ outage might not have been a catastrophic event in the sense that there were no casualties or major losses, but the disruption of more than three million trades over the span of just three hours is a significant blow to a nationwide financial system that relies heavily on the stability of its IT infrastructure.

## ACTIVITY 1–2

### IT Failures: Reflective Questions

#### Scenario

Based on the previous case study, think about the following questions in regard to how this specific scenario relates to Mission Critical Operations.

---

1. What does the NASDAQ outage tell you about the importance of the IT infrastructure in MCO facilities?
  
  2. What protocols could have been put in place or actions could have been taken to prevent the outage?
- 

#### Security

*Security* refers to the application of devices and procedures to ensure that a valuable asset—whether an object, a person, a facility, or even information—is protected from harm. Obviously, with a name like "mission critical," security is an important component in MCOs. For MCOs, security can be grouped into three main areas of focus: protecting people (safety), protecting equipment (physical design), and protecting information (processes and procedures).





**Figure 1–3: Security personnel monitor a facility after normal operating hours. (Source: Balefire9/iStock/Thinkstock)**

## The Role of Security in MCOs

MCOs really could not serve their mission critical functions if steps were not taken to protect them from failures, catastrophes, or malicious interactions. Much like IT, some mission critical facilities exist for the sole purpose of providing security to information systems, transportation systems, public service systems, etc. However, all MCOs rely upon security services (both physical and digital) and security considerations in their designs.

In this way, security is an integral component in nearly all types of MCOs. For example, financial institutions rely on IT security best practices to protect their customers' important personal information. Large-scale transportation systems rely on security screening devices and procedures to ensure the safety of their passengers by ensuring that dangerous items are not brought on board. A facility like a pharmaceutical research center would rely on both physical and information security to ensure that the building itself is safe from intrusion and the information it houses is safe from accessibility and misuse if it fell into the wrong hands.

## Case Study: Security Breaches

Security breaches today are most often discussed in relation to data security breaches or the unwanted access of secure information. One of the more memorable data breaches of recent memory was the hack of retail store Target's databases in late 2013, during which the debit or credit card information of more than 40 million customers and the personally identifiable information (PII) of more than 70 million customers was accessed.

The breach wasn't particularly innovative or aggressive: in late November of 2013, malware was installed on the company's security and payment systems, which was designed to capture credit card numbers during checkout and then store them on a specific server within the same network that was being controlled and accessed freely by the breaching parties. From there, the data was shuffled to

multiple servers around the country as staging points, and then moved to computers in Russia where the hackers could use the credit card numbers to make unauthorized purchases.

However, Target had already installed malware detection tools on the servers used for the security and payment systems, and the security specialists who monitored them were aware of the suspicious activity almost as soon as it started. They notified the company's security operations center of the potential breach but, unfortunately, these alerts were either not taken seriously or weren't acted upon with immediacy. By mid-December, when the company disclosed the breach to the general public, more than 40 million customer debit and credit card numbers and 70 million customer names, addresses, phone numbers, and email addresses had been stolen.

Since the breach, close to 100 lawsuits have been filed against the company on behalf of both customers and financial institutions, claiming negligence on Target's part and seeking compensation for losses sustained as a result of the breach. Between these lawsuits and its customer response effort, Target has spent millions of dollars in response to the data breach.

## ACTIVITY 1–3

### Security Breaches: Reflective Questions

#### Scenario

Based on the previous case study, think about the following questions in regard to how this specific scenario relates to Mission Critical Operations.

1. What does the Target data breach tell you about the role of security in MCOs?
2. What should the company have done differently to prevent or mitigate the effects of the data breach?

#### Procedures and Policies

The importance of the stable operations of a mission critical facility—they are mission critical, after all—underscores the absolute importance of standardizing the processes followed throughout the facility. These guidelines are captured in the form of procedures and policies. *Procedures* are specifically prescribed means for accomplishing tasks in a reliable and safe manner. *Policies* are guidelines that direct actions or activities, generally needed to ensure similar outcomes are achieved given a wide array of possible inputs and variables. Another way to think of the distinction is that policies govern our thoughts and the boundaries for related actions, while procedures are designed to specific sets or sequences of actions required to assure a predicted result.

#### The Role of Procedures and Policies in MCOs

In high-stakes MCO environments, it is incredibly important to be able to perform common, critical tasks or provide integral services in a reliable, repeatable manner. Having standardized policies and procedures in place ensures that all operations personnel know what to do and how to do it properly, regardless of whether it's their first day or their fifteenth year on the job. And, with the 24/7 nature of most MCOs and today's ever-evolving technology, it is even more important that there is support in place that allows operators to perform the same tasks, in the same safe and reliable manner, regardless of who is on the clock and what time of day it is.

For example, think about O'Hare International Airport, one of the busiest airports in the world based on the number of takeoffs and landings. Can you imagine what would happen if this busy airport didn't have any standardized guidelines to direct common actions or systematic steps for performing critical functions? Mass chaos would ensue: flights wouldn't leave on time, passengers

would be stranded, and the safety of everyone in the facility could easily be at risk. Having policies and procedures in place not only allows for the day-to-day operations to be performed properly and efficiently, but it ensures that they are done with the safety and security of all personnel and passengers in mind.

## Case Study: Failing to Adhere to Procedures or Policies

Policies and procedures exist in any organization for a purpose: to ensure the safe, consistent operations of key systems or devices. So, when they aren't followed or adhered to strictly, things often go wrong—sometimes with devastating consequences. One such case of the disastrous effects of failing to adhere to policies and procedures is the nuclear accident at the Chernobyl power plant in 1986.

The Chernobyl power plant was home to four operating power reactors and a fifth reactor under construction, on a site just north of what is now Kiev, Ukraine (at the time, it was still part of the Soviet Union). The reactors were a Russian design called RBMK, which was fueled by natural uranium, cooled by water, and moderated using graphite construction. However, this design was considered "fundamentally faulty" and "having a built-in instability" by members of the expert community, especially given the fact that, rather than shut itself down in the event that it starts to lose coolant, an RBMK actually would increase in reactivity and begin to run hotter and faster. Additionally, the reactors were not protected by containment structures, which were required of reactors in other countries. From the start, the nuclear reactors on the Chernobyl site were already not in compliance with the standards expected of a safely operating nuclear facility.

Unfortunately, on top of a poorly designed system, the operators at Chernobyl were fundamentally lacking in the knowledge, skills, training, and awareness of the magnitude of their actions needed to safely operate the facility. In fact, it is without a doubt that the accident at Chernobyl was a direct result of actions taken on the part of the operators that failed to adhere to any proper protocol.

The immediate cause of the accident was "mismanaged electrical engineering equipment," but the larger story was that a number of engineers—with no working knowledge of the physics of nuclear reactors—had decided to run an experiment to see if they could use the rotational energy from the steam turbine in the reactor to generate additional backup power for the plant. Before performing the test, they disconnected every important safety system, including the emergency core-cooling system, and disconnected every backup electrical system—all the systems that would be needed in the event of an emergency to help them safely operate the reactor controls.

The experiment went poorly from the start: the operators reduced one reactor's power level to wind up the turbine, but did so far too quickly, which caused a build-up of fission by-products in the reactor core and poisoned the reaction. In an effort to stabilize it, the operators began to remove the control rods from the unit. Despite their efforts, they couldn't increase the power level to more than 30 megawatts, an operating level in which the instability of the reactor is at its potential worst and a level that was specifically forbidden by the plant's own safety rules. They continued to remove more control rods until only 6 of more than 210 rods remained, even though the minimum number of control rods for the proper documented operations of the reactor was 30.

But the engineers pushed on with their experiment, next shutting down the turbine generator, which reduced power to the water pumps and thus reduced the flow of coolant water to the system. This unfortunately increased the chain reaction in the reactive materials, and the power level in the reactor surged. While there is some debate over whether it was an operator decision or an automatic system action, the control rods that had been removed were hurriedly re-inserted into the reactor. Unfortunately, the control rods had a fatal design flaw: their graphite tips increased the reaction, and displaced water from the rod channels increased it further. There was simply too much reactivity, and the reactor exploded.

Between the steam in the initial explosion and the resulting fires, at least five percent of the radioactive materials from the reactor were released into the air and traveled downwind. Two plant workers died in the explosion and another 28 emergency responders died in the following weeks due to acute radiation poisoning. Containment and cleanup of the site took months, involving more than 500,000 workers (many of whom were exposed to dangerous levels of radiation) and costing more

than 18 billion rubles (or more than 3 million U.S. dollars, using the current exchange rate). But the impact of the accident has been felt for decades. Since the accident, more than 230 people have suffered acute radiation sickness, and increased incidences of cancers and other health disorders likely to be related to the accident have been reported.



about the general use and the service and repair history of system equipment and other components allows operators to analyze trends and predict failures before they happen.

Consider this scenario: you have just taken on a key position with a mission critical facility. Chances are, someone else designed and built this facility and its integral systems many years ago. For better or worse, all the decisions that were made during the planning of the facility and its systems and knowledge about all of the various components that have been put into it are in the documentation that was (hopefully) collected and maintained. In your role, it would greatly benefit you to have this information to understand the why and the how about the mission critical systems you are now a part of and to understand them in a proactive sense, rather than having to understand them reactively to fix it when it's broken or—a worst case scenario—in the event of an emergency.

## Case Study: Improper Documentation

As you now know, having access to documentation for the design, proper operation, and even the individual components of MCOs is extremely important for the consistent, safe, and reliable functioning of a facility. And when that documentation is lacking or non-existent, it can be difficult to maintain the systems' optimal functionality. Case in point: the improper documentation for a new data center supporting a large research university.

Typically, the university would build on their own property and construct all facilities to their standards and then maintain and operate the facility after its construction. But this time around, the design and construction of the facility was provided in what is known in the industry as a turn-key approach—it was designed and constructed by a company that specializes in this type of facility, to their own standards and specifications, with input from the university's facilities and IT staff only regarding its specific space and technical needs. The data center was built on a leased site five miles from the center of campus and was operated by staff contracted by the specialty company, not by university IT staff.

On a particularly hot summer day, the temperature in the primary server room in the data center began to rise. Fortunately, the protocol to address this issue was documented in both hard copy and electronic form, so the operators knew where to look. Despite their best efforts to adjust the system according to the documentation, it became clear that the system wasn't responding appropriately. Clearly, they were not addressing the correct issue, but their documentation didn't have any other potential causes or possible solutions. The operators called upon the university's facilities staff to help them, but since they had not been directly involved in the design or construction of the facility, they weren't able to provide the operators with any helpful information.

After some time and exploratory research, it became apparent that the temperature rise was the result of an equipment failure, specifically a malfunctioning relay panel. Unfortunately, the data center operators didn't have any spare components on hand to fix the issue immediately. While the university facilities and IT staff typically had spare parts, the data center used very specific equipment used by the specialty company, and they didn't have a compatible component. Instead, the data center operators had to contact the firm that designed and constructed the building for the necessary parts, which would be accompanied by specific installation instructions. However, the component wouldn't be delivered for another 24 hours, and in the meantime, the temperature in the server room had continued to rise and was getting dangerously close to hazardous levels. Fortunately, the design and build firm was also able to talk the operators through some specific adjustments to the system that would temporarily provide a solution until the component was replaced, and after a few hours of trial and error, the server room was back to safe operating conditions.

## ACTIVITY 1–5

### Improper Documentation: Reflective Questions

#### Scenario

Based on the previous case study, think about the following questions in regard to how this specific scenario relates to Mission Critical Operations.

---

1. **What does this scenario tell you about the importance of having proper documentation available for all of the elements, including the design and construction, of MCOs?**
  
  2. **What could have been done differently to prevent this situation from occurring?**
- 

#### Crises

A *crisis* is any event or occurrence, typically happening abruptly or with little or no warning, that has the potential to result in an unstable or dangerous environment.

Crises can take on many forms and require specific responses, depending upon their nature. A natural disaster and the threat of imminent system failure are of equal concern. For the sake of identification and planning, it is important to categorize the different types of crises and how to address them. The Department of Homeland Security (DHS) identifies the following types:

- A threat is any natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.
- An incident is any occurrence, caused by either human action or natural phenomena, that may cause harm and that may require action.
- An attack is any malicious activity by outside individuals directed at a specific target.





**Figure 1-4:** The damage to the Pentagon was part of the larger terrorist attacks of September 11, 2001. (Source: Stocktrek Images/Thinkstock)

## The Element of Surprise

Although many organizations are actively monitoring threat levels and real-time risk analysis, there is usually little to no warning of an actual crisis. Attacks are certainly more surprising due to their very nature, but other events (consider Three Mile Island or Chernobyl) can catch MCOs off guard as they begin to unfold rapidly. You can't call a time-out in a crisis and have meetings to figure out what to do next—the time for those meetings is before crises occur; hence the focus on planning.

## Crisis Management

Of all the in-depth planning and design that goes into bringing a mission critical installation online, and as skilled as its operators may be, emergency situations still arise—it's inevitable. Hence, the necessity for *crisis management*: the planning and monitoring for and the immediate response to any potential threat to MCOs.

Ordinary mechanical failures in a regular facility don't necessarily interrupt daily operations, but the threat of cascading issues leading to downtime highlight the importance of solid crisis management in MCOs. It is vital to have well-thought-out crisis management plans that operations teams are trained on and comfortable with. Writing scripts for every possible scenario is highly impractical, if not impossible, but consistent plans to respond to situations, to establish a path towards stability, and to connect the right resources will be invaluable in the event of a crisis.

## Accelerated Decision Time frame

With incidents occurring in real time, quick decisions provide windows of opportunity to stop an event or at least mitigate damages from spiraling out of control. Crisis management leaders must think on their feet and be confident enough in prior planning efforts to execute response activities so that they lose as little time as possible.

For instance, if an MCO team notices some initial fatigue in a nuclear reactor's shielding, they may have hours to days to develop a plan to mitigate the risk. But, in the case of an actual breach, they

may only have seconds or minutes before an entire region of the country is potentially in danger of being exposed to hazardous nuclear materials.

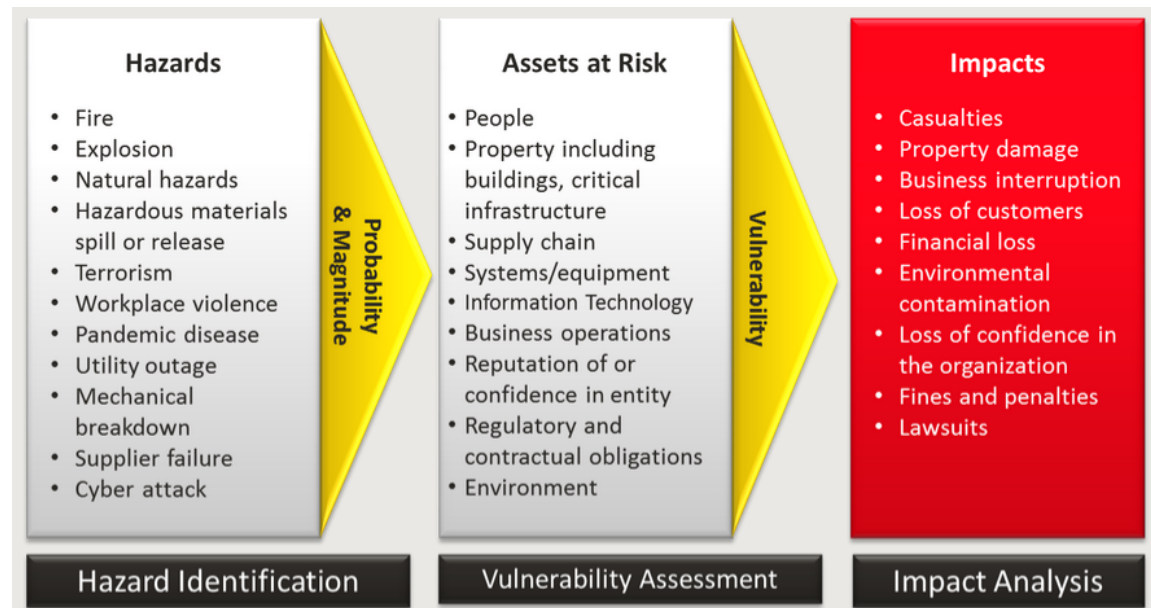
## Risk Management

*Risk management* is the process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level at an acceptable cost.

The primary goal of risk management is to reduce or eliminate risk through mitigation measures (avoiding the risk or reducing the negative effect of the risk), but also includes the concepts of acceptance and/or transfer of responsibility for the risk, as appropriate. Risk management principles acknowledge that, while risk often cannot be eliminated, actions can usually be taken to reduce risk in the first place.

In risk evaluation and planning, the first step is always to assess the situation. Then, *triage* can take place, or sorting the results of a specific risk-related event and determining the priority for addressing each and allocating the appropriate resources to do so. Given a limited time to respond effectively, MCOs need structures in place to sift through the chaos and identify the most serious issues at hand.

Once the state of things has been determined, solutions can be developed to create a safe, stable environment and ready the system for remediation and restoration activities. Outside of extreme situations that require massive, coordinated responses, the aim of the identified solution should always be to place the site or system(s) in a safe condition in which operations teams can take actions to stop further damage or degradation. Solutions need to be clear enough for everyone to quickly be on the same page working together, but broad enough to categorically respond to similar crises without the need for an extensive library of highly specified action plans.



**Figure 1–5: The risk assessment process as described by the DHS on its disaster preparedness website. (Source: <http://www.ready.gov/risk-assessment>)**

### Proactive vs. Reactive Responses

Risk management is more of a preventative measure, used to identify potential events and proactively plan a response. Crisis management is inherently more reactive in nature, as it is the actual actions that are taken, with that plan in mind, when an event takes place.

## Phases of Crisis Management

In the event of a crisis, there are three phases of crisis management that are typically followed:

- 1. Crisis Assessment**—Following a similar thought process to the planning activities, assessing the crisis to get to the heart of the matter is of primary importance. The right problem needs to be addressed and it needs to be fixed. MCO plans and procedures should be followed to determine things like: How did this begin? Are there other conditions (e.g., alarms, faults, etc.) that we're not seeing? What resources are available? And, what is the status of all our systems?
- 2. Crisis Action Plan**—With answers to the preceding questions, the crisis management leader should begin to enact and/or develop action plans. This spans the range from completing triage activities, to incident notification protocols, to marshalling resources for permanent repairs, to establishing the level of sensitivity or urgency under which these actions are to take place. Depending upon the MCO environment, formal crisis response activities may continue on until every single fault or failure is addressed, whereas other MCOs simply want to restore operations, even under temporary conditions, and document the go-forward plan.
- 3. Crisis Termination**—Again, putting a stop to the crisis response varies by industry and application, but generally falls into the two approaches just mentioned: maintain the crisis response posture until all systems, equipment, and operations are fully restored or repaired, or release this posture once the threat to operational availability has been neutralized and the crisis leadership is comfortable with the documented remediation plans.

# ACTIVITY 1–6

## Identifying the Elements of MCOs

### Scenario

In this activity, you will identify the elements of MCOs.

---

**1. MCOs are unique because they allow an organization to deliver its product or service without:**

- Profit
- Integrity
- Interruption
- Procedures

**2. What is critical infrastructure?**

- The collection of physical systems that prevent interruption to an organization's reliable delivery of a product or service.
- The collection of conceptual systems that allow an organization to reliably deliver a product or service.
- The collection of processes and procedures that allow an organization to reliably deliver a product or service.
- The collection of physical systems that allow an organization to reliably deliver a product or service.

**3. What is the difference between policies and procedures?**

- Procedures are guidelines for activities that result in a reliable outcome, while policies are specific actions for accomplishing a task in a safe, reliable manner.
- Policies are specific actions that result in a reliable outcome, while procedures are guidelines for accomplishing a task in a safe, reliable manner.
- Policies are guidelines for activities that result in a reliable outcome, while procedures are specific actions for accomplishing a task in a safe, reliable manner.
- Policies are guidelines for activities that result in a variable outcome, while procedures are specific actions for accomplishing a task in a safe, reliable manner.

**4. What are the phases of crisis management?**

- Crisis Prevention
  - Crisis Assessment
  - Crisis Action Plan
  - Crisis Intervention
  - Crisis Termination
  - Crisis Remediation
-

# TOPIC B

## Mission Critical Industries

With a general knowledge of MCOs and what they are, you now understand how these specific elements and activities are vital to the continued functioning of the absolutely critical components of an organization. But the term "organization" is quite generic. What types of organizations can you classify as critical, and why are they critical to our normal day-to-day functions?

As a Mission Critical Operator, it is imperative that you know all of the organizations that are part of the mission critical infrastructure, especially those that are inherently interconnected. Here, you will identify these mission critical industries and explain why each is an important component of the consistent, reliable functioning of the mission critical infrastructure.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Triage

## DHS

The Department of Homeland Security (DHS) is a department of the United States government that focuses on the safety and security of the American nation, protecting it from a variety of threats to national security. It was created in the wake of the September 11th terrorism attacks, with the primary responsibilities of proactively preparing for, preventing, and reactively responding to any threat to the country or its territories, with a particular focus on terrorism.

## Critical Infrastructure Sectors

According to national policy created to "strengthen and maintain secure, functioning, and resilient critical infrastructure," there are 16 critical infrastructure sectors that DHS oversees. They are:

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector

DHS works closely with organizations and/or corporations within each of the sectors to determine and then oversee the best practices for safety and security for that sector. This includes setting specific goals and objectives, identifying segment assets and assessing segment risks, prioritizing the specific needs of the segment, and then implementing segment-specific protective programs. They also work together to measure the effectiveness of the risk mitigation actions put into place, and

coordinate research and development for future implementations or for updating safety and security measures.

For each of these sectors, DHS also provides standardized resources and training materials aimed at enabling consistency and reliability among the numerous facilities that are part of the sector.

## Chemical Sector

The Chemical Sector consists of five segments based largely on what final products they produce, each of which has unique characteristics, markets, development opportunities and, accordingly, respective areas of issue. These five segments are:

- Basic chemicals
- Speciality chemicals
- Agricultural chemicals
- Pharmaceuticals
- Consumer products

## Commercial Facilities Sector

The Commercial Facilities Sector consists of any facility that operates within the sphere of open public access, which means that the general public can easily enter and move about in the facility's space without the presence of security barriers. Typically, these facilities require unfettered access to the general public because they provide a commercial service or product to them. They fall into one of eight subsectors:

- Public Assembly (such as arenas, stadiums, zoos/aquariums, museums, convention centers, etc.)
- Sports Leagues (such as professional sports leagues or other organizations)
- Gaming (such as casinos)
- Lodging (such as hotels, motels, conference centers, etc.)
- Outdoor Events (such as amusement parks, fairs, campgrounds, parades, etc.)
- Entertainment and Media (such as movie theaters, movie studios, broadcast media centers, etc.)
- Real Estate (such as office buildings, apartment buildings, condominiums, mixed-use facilities, storage facilities, etc.)
- Retail (such as retail centers or districts, shopping malls, etc.)



**Figure 1–6: Paul Brown Stadium in Cincinnati, Ohio is the home venue of the Cincinnati Bengals professional football team. (Source: Derek Jensen/Creative Commons (Public Domain)/<https://commons.wikimedia.org/wiki/File:Cincinnati-paul-brown-stadium.jpg>)**

## Communications Sector

The Communications Sector is an integral part of the entire critical infrastructure of the nation, since so many other sectors rely heavily upon it. As DHS puts it, the Communications Sector provides an "enabling function" to all of the other sectors. This sector in particular has changed significantly over the past two or three decades, as communications technology has quickly evolved: where it used to be primarily concerned with voice services, it now includes terrestrial, satellite, and wireless transmission systems. And, more so, these various transmission types have become interconnected, working together to provide seamless, end-to-end transmissions across different communication media. Today, many providers will share their facilities and technologies to ensure that there is interoperability among the different transmission mediums.



**Figure 1–7:** A cell tower is a critical component of wireless transmission systems, one of the most common communications mediums today. (Source: SvonHalenbach/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Richtfunkantenne\\_Waldeck2\\_Peterskopf.png](https://commons.wikimedia.org/wiki/File:Richtfunkantenne_Waldeck2_Peterskopf.png))

Most facilities within the Communications Sector are privately owned and operated; however, given the critical nature of the sector and the reliance of other critical sectors upon it, the federal government works closely with the privately held organizations to predict, plan for, and respond to any communications outages that could have a wide effect on the safety and security of the nation at large.

## Critical Manufacturing Sector

The Critical Manufacturing Sector is another sector that can be considered crucial to the continued, uninterrupted functioning of some of the other critical infrastructure sectors because the products that they manufacture are directly used—if not essential to—the operations of the others. This sector consists of four broad categories of industries that manufacture critical components:

- Primary Metal Manufacturing—including iron, steel, and ferro alloy manufacturing, alumina/aluminum production and processing, and nonferrous metal production and processing.
- Machinery Manufacturing—including engine, turbine, and power transmission equipment manufacturing.
- Electrical Equipment, Appliance, and Component Manufacturing—including electrical equipment manufacturing.
- Transportation Equipment Manufacturing—including vehicle manufacturing, aviation and aerospace product and parts manufacturing, and railroad rolling stock manufacturing.



## Dams Sector

The Dams Sector is another critical component of the nation's mission critical infrastructure. The Dams Sector consists of a number of different types of dam-related assets, including dams, locks, levees and dikes, hurricane barriers, hydropower generation facilities, and a host of other water containment or control facilities. The facilities or organizations that fall within the Dams Sector provide services with a wide range of benefits to the American public, including water supply and waste management, flood control, waterway navigation, natural wildlife habitats, and even recreation. These services also extend to some of the other critical infrastructure sectors—such as providing a source of water for the Food and Agriculture Sector—creating strong interdependencies between the Dams Sector and these other sectors.

At present, there are more than 87,000 dams or dam-related devices throughout the U.S. With such a high number of critical assets and because of the mutual dependencies that exist between the Dams Sector and some of the other critical infrastructure sectors, DHS involvement in the safety and security of the facilities within such a critical sector is required.



*Figure 1–8: The Willow Creek Dam, just outside of Heppner, Oregon. (Source: U.S. Army Corps of Engineers/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:USACE\\_Willow\\_Creek\\_Dam\\_Oregon.jpg](https://commons.wikimedia.org/wiki/File:USACE_Willow_Creek_Dam_Oregon.jpg))*

## Defense Industrial Base Sector

The Defense Industrial Base Sector is a complex collection of industries that supports the research and development, design, production, delivery, and maintenance of weapons, parts, and other components for the United States military, including products and services that are necessary for mobilizing, deploying, and maintaining military operations. The Defense Industrial Base Sector consists of:

- A number of organizations under the Department of Defense (DOD).
- More than 100,000 companies and subcontractors that provide products or services to the DOD.

- Any government-owned/privately-operated or government-owned/government-operated military-related facilities.

## Emergency Services Sector

The Emergency Services Sector (ESS) serves as the nation's primary defense in regard to the prevention of and remediation of risk resulting from both man-made and natural incidences. In addition to protecting the entire nation in the event of an emergency, it also carries the heavy burden of serving as the first line of defense for the remaining critical infrastructure sectors. This includes a wide array of response functions in an emergency, but primarily it is responsible for protecting people, property, and the environment; providing assistance to those affected by the emergency event; and providing recovery services and aid to those impacted by the event.

These emergency response actions are the responsibility of five broad categories of emergency responders:

- Law enforcement
- Public works
- Fire and emergency services
- Emergency medical services
- Emergency management services



**Figure 1–9: Fire trucks respond to an emergency event. (Source: Jim Parkin/iStock/Thinkstock)**

Within the ESS, there are also a number of specialized organizations that provide specific services in the event of an emergency of various types, including:

- Public Safety Answering Points (such as 911 call center responders)
- Tactical Operations (such as S.W.A.T.)
- Search and Rescue
- Aviation Services (such as police or medical helicopters)
- Hazardous Materials
- Explosive Ordnance Disposal (such as a bomb squad)

## Energy Sector

The Energy Sector has been labeled "uniquely critical" by DHS because the products and services it provides directly support the critical functioning of the other critical infrastructure sectors. The sector is divided into three interconnected segments, including:

- Electricity (which is produced by combusting coal, combusting natural gas, nuclear power plants, hydroelectric plants, or renewable power sources)
- Petroleum
- Natural Gas



**Figure 1-10: The Johnsonville Fossil Plant near Waverly, Tennessee produces enough electricity through coal combustion to supply 800,000 homes. (Source: Tennessee Valley Authority/Creative Commons (Public Domain/[https://commons.wikimedia.org/wiki/File:Johnsonville\\_fossil\\_plant.jpg](https://commons.wikimedia.org/wiki/File:Johnsonville_fossil_plant.jpg)))**

Almost every critical sector relies on some form of energy produced by the Energy Sector industries, making it both incredibly important but also incredibly vulnerable to threats. For example, power or power-related products are distributed across the country via intricate pipeline systems that fall under the Transportation Sector. If something were to happen to these pipelines, energy distribution could be affected with devastating consequences, not just interrupting power to the general public, but to other critical sectors.

## Financial Services Sector

The Financial Services Sector consists of the wide variety of institutions that provide financial products and services to individual consumers, businesses, and the other critical infrastructure sectors. These activities include depositing funds, making payments between parties, providing credit to consumers, investing funds, and transferring financial risk between parties. As technology has become more prevalent in the financial industries, this sector has become more vulnerable to newer security risks including power emergencies, the effects of natural disasters on IT infrastructure, and cybersecurity threats.

## Food and Agriculture Sector

The Food and Agriculture Sector consists of those industries producing and providing food-related products or services to the nation, including:

- Farms
- Restaurants
- Manufacturing, processing, and storage facilities



**Figure 1-11: Grain elevators on a farm in Gordon, Nebraska. (Source: Ammodramus/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Gordon,\\_Nebraska\\_grain\\_elevators\\_1.JPG](https://commons.wikimedia.org/wiki/File:Gordon,_Nebraska_grain_elevators_1.JPG))**

The industries within this sector are of great economic importance to the nation, accounting for nearly one-fifth of the country's economic activity. And, of course, providing sustainable food resources for the nation is of critical importance. Most of these properties are privately owned and operated, but they also have integral interdependencies with many of the other critical infrastructure sectors.

## Government Facilities Sector

The Government Facilities Sector consists of a number of government-owned and operated buildings, some of which are publicly accessible and some that are open to approved personnel only. Those that are open to the public include buildings used for business, commercial, or even recreational purposes; those that are not open to the public typically house sensitive information or materials, including government-used office buildings, courthouses, embassies, laboratories, or any other structure that might be home to critical equipment or systems. The Government Facilities Sector is also responsible for utilizing cybertechnology to protect government assets, including information and personnel, that are critical to government functions.

The sector also oversees two important subsectors:

- The Education Facilities Subsector, which includes both government and privately owned educational institutions such as K-12 grade schools, colleges and universities, and business schools and trade schools.
- The National Monuments and Icons Subsector, which includes a wide array of national landmarks and historic locations.

## Healthcare and Public Health Sector

The Healthcare and Public Health Sector is responsible for protecting the American public from all sorts of risks to their health, including terrorism, outbreaks of infectious diseases, and other natural disasters. These responsibilities are both proactive, in the form of providing preventative healthcare options; and reactive, in the form of providing healthcare response and recovery actions in an emergency event. The healthcare component of these services is typically delivered and managed at the local level via private industries or state-run programs, while the public health component is typically managed across all government levels (national, state, regional, local, and even tribal or territorial).



**Figure 1–12:** *The City of Houston Health Department, as part of the local government, provides public health services to Houston’s residents. (Source: WhisperToMe/Creative Commons (Public Domain)/<https://commons.wikimedia.org/wiki/File:HoustonHealthDepartment.JPG>)*

## Information Technology Sector

The Information Technology Sector has become a key mission critical sector, as more private citizens, businesses, and other large organizations—including the government—rely on the availability and stability of computer-related technology. The functions of the Information Technology Sector are both virtual and distributed in nature, including the production and distribution of hardware, software, IT systems and services, and (in conjunction with industries in the Communications Sector) the Internet. The threats posed to the Information Technology Sector are vast and ever-changing and require that the private entities involved in IT—which are the private owners and operators that maintain key systems and networks, including the Internet—work creatively and collaboratively with the government agencies of the Information Technology Sector to develop plans to protect the safety and security of the sector’s assets.

## Nuclear Reactors, Materials, and Waste Sector

The Nuclear Reactors, Materials, and Waste Sector oversees a variety of industries or services involved in the general use of nuclear reactors, including:

- Nuclear power plants.
- Non-power nuclear reactors (those used for research, testing, or training).
- Manufacturers of nuclear reactors or their components.
- Nuclear fuel-cycle facilities.
- Decommissioned nuclear reactors.
- Entities involved with the transportation, storage, or disposal of nuclear or radioactive waste.

Because of the inherent threat that nuclear reactors can pose to the general population (both within the nation and globally), the environment, and the consistent and reliable functioning of many of the other mission critical sectors, maintaining the safety and security of this sector is of the utmost importance.



**Figure 1–13: The Bellefonte Nuclear Power Plant under construction in Hollywood, Alabama.** (Source: Tennessee Valley Authority/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Bellefonte\\_Nuclear\\_Power\\_Plant.jpg](https://commons.wikimedia.org/wiki/File:Bellefonte_Nuclear_Power_Plant.jpg))

## Transportation Systems Sector

The Transportation Systems Sector consists of all of the industries involved in the movement of people or things from one location to another, within the country and to and from overseas locations. There are seven key subsectors within the Transportation Systems Sector:

- The Aviation subsector consists of all aircraft, air traffic control systems, commercial airports, and privately owned airports, heliports, and landing strips used in the air travel or transportation of people or things within the nation and travelling to or from international locations.
- The Highway Infrastructure and Motor Carrier subsector consists of the millions of miles of roadway, hundreds of thousands of bridges, and hundreds of tunnels across the country that are used by a variety of authorized vehicles, including cars, motorcycles, commercial trucks (including those that carry hazardous materials), buses, and school buses.

- The Maritime Transportation System subsector consists of the millions of square feet of sea waters prescribed by the Exclusive Economic Zone, thousands of miles of coastline and waterways, hundreds of ports, and any other land-and-sea connections within the nation that are used for the transportation of people or things.
- The Mass Transit and Passenger Rail subsector consists of all transportation services carried out by bus, rail transit (including commuter rail; heavy rail, such as subways and metros; and light rail, such as trolleys and streetcars), long-distance rail, or the less common types of mass transit such as cable cars, etc.
- The Pipeline Systems subsector consists of the millions of miles of pipeline that criss-cross the nation, carrying a variety of materials including natural gas, hazardous liquids, and other chemicals. It also includes the natural gas processing and storage facilities that are connected to the pipeline networks for distribution purposes.
- The Freight Rail subsector consists of the seven major freight rail carriers, hundreds of small or privately owned railroads, hundreds of thousands of miles of railroad tracks and their associated structures, millions of freight cars, and thousands of locomotives and trains that are used for the transportation of people or things around the nation. This also includes the thousands of miles of railroad tracks and structures deemed critical by the Department of Defense for the mobilization and transportation of U.S. military forces during times of need.
- The Postal and Shipping subsector consists of the millions of flat mail, publications, small-sized, and medium-sized packages that are handled and delivered between millions of senders and millions of locations throughout the United States, and the facilities that process, sort, and manage these materials.

Because there are so many subsectors and modes of transportation that are moving people and goods within the nation itself and to and from international locations, protecting the safety and security of the Transportation Systems Sector is vitally important to those using its various components and those mission critical sectors that rely on this important sector as well.

## Water and Wastewater Systems Sector

The Water and Wastewater Systems Sector consists of those facilities and associated systems that provide public drinking water and sewage treatment/wastewater treatment services to the American public. These systems are most vulnerable to attacks that could compromise the availability of potable drinking water, including physical attacks such as contamination with toxic agents or the release of other gaseous chemicals, and cyber attacks that target these systems' functions. Attacks of this nature could result in large-scale health concerns, including illness or death, and the interruption of crucial water services to private citizens, industries, and the other critical infrastructure sectors.



*Figure 1-14: A water treatment facility in Ramadi, Iraq. (Source: Jeremy M. Giacomino, United States Marine Corps/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Water\\_treatment\\_plant\\_in\\_Ramadi.jpg](https://commons.wikimedia.org/wiki/File:Water_treatment_plant_in_Ramadi.jpg))*



# ACTIVITY 1–7

## Identifying Mission Critical Industries

### Scenario

In this activity, you will identify the mission critical industries identified by the DHS.

1. **Which of the critical infrastructure sectors is responsible for the oversight of the transportation of natural gas via pipelines that cross the country?**
  - Energy Sector
  - Chemical Sector
  - Transportation Systems Sector
  - Critical Manufacturing Sector
  
2. **Which of the critical infrastructure sectors is responsible for the oversight of buildings that are accessible to the public for business or recreational purposes?**
  - Government Facilities Sector
  - Healthcare and Public Health Sector
  - Transportation Systems Sector
  - Commercial Facilities Sector
  
3. **Which of the critical infrastructure sectors is responsible for the oversight of facilities producing parts and equipment involved in transportation mechanisms like vehicles and airplanes?**
  - Energy Sector
  - Transportation Systems Sector
  - Defense Industrial Base Sector
  - Critical Manufacturing Sector
  
4. **Which of the critical infrastructure sectors is responsible for the oversight of a hydropower generation facility?**
  - Dams Sector
  - Energy Sector
  - Critical Manufacturing Sector
  - Government Facilities Sector
  
5. **Which of the critical infrastructure sectors is responsible for the oversight of the production of pharmaceuticals?**
  - Healthcare and Public Health Sector
  - Food and Agriculture Sector
  - Chemical Sector
  - Critical Manufacturing Sector

6. Which of the critical infrastructure sectors is responsible for the oversight of the transportation, storage, and disposal of the by-products of nuclear energy production?
- Transportation Systems Sector
  - Water and Wastewater Systems Sector
  - Energy Sector
  - Nuclear Reactors, Materials, and Waste Sector
7. Which of the critical infrastructure sectors is responsible for the oversight of the handling of hazardous materials during an emergency event?
- Nuclear Reactors, Materials, and Waste Sector
  - Emergency Services Sector
  - Chemical Sector
  - Healthcare and Public Health Sector
-

# TOPIC C

## MCO Careers

With a better understanding of all of the industries involved in MCOs, you might be thinking: there must be plenty of career opportunities in MCO-related fields. That is an accurate assumption; within MCOs, there is a wide variety of careers available with varying degrees of expertise and skills needed. But there is one similarity among them all: you need to have the right frame of mind to even pursue a career in such a high-stakes system. In this topic, you will identify the different careers available in the MCO industries.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Mission critical mindset

## The Mission Critical Mindset

There exists a special type of person who has what it takes to succeed in mission critical environments. Some people will find the stringent MCO standards impossible to achieve; others just can't handle the stress of the job. To be fair, the role and responsibilities of a facility engineer or a systems operator at a data center or a nuclear power plant is a far cry from a general commercial or industrial location, and it's simply not for everyone. Just because you are a master electrician with years of accumulated knowledge and skills doesn't mean that you will automatically enjoy or be successful in a Mission Critical Operations position.

Beyond the appropriate technical knowledge, though, the secret to success is easily summed up: adopt and maintain a *mission critical mindset*. This means an operator should develop a broad understanding of systems integration and cultivate a constant awareness of how even the smallest action has far-reaching consequences, like the ripples and waves upon a body of water. Even if you don't know every last technical specification about the system you are working on, this mindset greatly increases the probability of operational success because you will be looking for areas of risk and can engage resources or enact plans to manage the risk to an acceptable level. Most importantly, when something (hopefully beyond your control) goes awry, you will have a much better understanding of the current environment and be able to react more promptly to remedy the situation.

To help you create and maintain this mission critical mindset—or at least until it becomes second nature to you—constantly consider the answers to the following questions as you go about your day in a mission critical environment:

- How critical is the work?
- Do I know the systems?
- What else does this affect?
- What are the risks involved?

## Desired Prior Experience

Although the nature of work in mission critical fields is similar, the daily tasks can be quite varied—as seen in the diversity of all of the industries that are part of the mission critical infrastructure. It is difficult to describe the ideal résumé for mission critical candidates, particularly those just getting started or transitioning from some other line of work. The mindset is priority number one.

Second to the mission critical mindset is exposure to the technical aspects of the job, whether direct or indirect. Working as an auto mechanic topped with exposure to MCOs (academic or otherwise) is a fine path towards getting into facilities engineering. Taking some basic computer sciences courses, even at the high school level, or making a habit of working through your own in-home network

setup, with at least a minimal understanding of the MCO principles, at least opens the entry-level door for you in IT.

## Technical Careers

Technical careers in the world of MCOs are the most highly focused professions, as they generally refer to equipment or systems-specific expertise. Think of MCO technicians as the men and women you call to install or repair a system. These individuals most often work for service providers: either the original equipment manufacturer (OEM) factory or a third-party company.

In a technical role, you are not necessarily tied to one specific location or installation, but travel to many customers. Although, with the growing number of billion dollar data centers, research campuses, and manufacturing facilities, it is becoming more common for service providers to assign primary or preferred technicians to one customer, and the scale of those operations may account for most—if not all—of the technicians assigned work. Owners are exhibiting a growing preference for this as the complexity of such installations requires a stronger knowledge of the system-specific design details and site policies.



*Figure 1–15: An Avionics Electronic Technician with the U.S. Navy installs a flight control computer in a fighter jet. (Source: United States Navy/Creative Commons (Public Domain)/ [https://commons.wikimedia.org/wiki/File:US\\_Navy\\_070424-N-9760Z-020\\_Aviation\\_Electronics\\_Technician\\_3rd\\_Class\\_Patrick\\_Beckwith,\\_assigned\\_to\\_the\\_Top\\_hatters\\_of\\_Strike\\_Fighter\\_Squadron\\_\(VFA\)\\_14,\\_works\\_on\\_installing\\_a\\_flight\\_control\\_computer\\_in\\_a\\_F-A-18E\\_Super\\_Hornet.jpg](https://commons.wikimedia.org/wiki/File:US_Navy_070424-N-9760Z-020_Aviation_Electronics_Technician_3rd_Class_Patrick_Beckwith,_assigned_to_the_Top_hatters_of_Strike_Fighter_Squadron_(VFA)_14,_works_on_installing_a_flight_control_computer_in_a_F-A-18E_Super_Hornet.jpg))*

## Operations Careers

Operations is a broad term that means a variety of things depending upon the industry. To simplify the idea, consider operations as those roles that are needed to allow the business to run, but are not necessarily involved in the customer-facing parts of the business. In other words, if you cut out the sales, marketing, administrative, research and development, and executive functions, you are broadly left with operations roles. For example, in a data center, a facility engineer or network technician

would fall under operations; in an emergency call center, a communications technician is part of operations; in a weapons manufacturing facility, a maintenance supervisor or security guard would be considered operations; and in a power grid control center, operations might include an electrician.

Not all operations roles are mission critical, though, even at a fully mission critical location. At a nuclear power plant, for instance, technicians with roles relating to the logistics of fuel delivery are certainly extremely important team members, but don't necessarily have to be performing their job 24/7; in fact, the entire department could probably go on vacation for a few weeks without impacting power production. Or, consider a cutting-edge bio-research facility for the Centers for Disease Control: a supply manager there would likely be considered part of the operations team (just like the logistics technician at the power plant), but she would not have a direct and immediate impact on the ability of scientists to perform real-time analyses during an epidemic.



**Figure 1-16:** An electrician, as part of the operations team for a facility, works on an electric panel. (Source: michaeljung/iStock/Thinkstock)

## Facilities Careers

Facilities Engineers are perhaps the most traditional and more commonplace of the MCO professions. These are the men and women who operate and maintain the mechanical, electrical, Fire-Life-Safety (FLS), and controls systems for mission critical locations. At a first glance, these careers may not seem much different than those in general commercial or industrial settings, but mission critical facility engineers deal with larger, more complex systems with sophisticated designs and a lot at risk in terms of safety and business continuity.

Critical Facility Teams are more regularly taking on 24/7 staffing models, where those employees that aren't manning the building around the clock are almost certainly on call to respond remotely or in person to after-hours incidents. These teams may have dedicated electricians, HVAC technicians, and controls-systems experts, but the growing preference is towards having well-rounded technicians that can operate and maintain all equipment to at least a moderate level, and then be able to work with specific contractors when it comes to major maintenance or repair items. Aside from allowing some flexible and cost-effective staffing models, this approach also allows a greater chance

of success during an emergency response because everyone on a shift understands the fundamental operation of all systems.



**Figure 1-17:** HVAC technicians work on an air conditioning unit for a building. (Source: lisafx/iStock/Thinkstock)

## Data Center Careers

Data centers take on many forms, and these days are more frequently appearing on a small scale in most modern commercial and industrial facilities. In smaller or legacy installations, the facilities team takes care of the data center or server rooms. Data center professionals, as a specialized career field for MCOs, are more specific to the large-scale, enterprise, and/or global service providers. These teams may be as small as 10 people or have a staff of dozens.

Data center professionals specific to MCOs largely fall into facilities, network, and security groups. Facilities engineers at an enterprise-scale data center have very similar roles as in other MCO facility teams, but tend to be more knowledgeable in certain systems due to varying design specifications, such as the use of fuel cells instead of diesel generators. The IT roles specifically include maintaining the network that the data center operates on, and do not include the application engineers that operate the systems responsible for delivering customer-facing services. Security does not always fall into the formal MCO groups at a data center, but increases in likelihood as the level of security increases.



*Figure 1-18: A network technician inspects the server stacks in a data center. (Source: .shock/iStock/Thinkstock)*

# ACTIVITY 1–8

## Exploring MCO Career Options

### Scenario

In this activity, you will explore the available career options in the MCO industries.

---

1. **What is the mission critical mindset?**
    - Having a vast technical knowledge of every single component of a mission critical system.
    - Having a broad understanding of the different components of a mission critical system and how they work individually in the system.
    - Having a broad understanding of how the various components work individually and interact collectively within a mission critical system.
    - Having minimal technical knowledge about the components of a mission critical system, but a good work ethic.
  2. **Which of the following MCO-related career categories is responsible for operating and maintaining the various systems in a facility, such as the mechanical, electrical, or control systems?**
    - Technical
    - Operations
    - Facilities
    - Data Center
  3. **Which of the following MCO-related career categories is responsible for having in-depth knowledge about the equipment or systems within a facility?**
    - Technical
    - Operations
    - Facilities
    - Data Center
  4. **Which of the following MCO-related career categories is responsible for maintaining the network that the facility relies on for general day-to-day operations?**
    - Technical
    - Operations
    - Facilities
    - Data Center
  5. **Which of the following MCO-related career categories is responsible for the day-to-day activities that allow the facility to function properly?**
    - Technical
    - Operations
    - Facilities
    - Data Center
-



# TOPIC D

## Design Parameters and Considerations

With a strong understanding of what exactly MCOs are—including the types of industries and jobs that are part of MCOs—you can then turn your attention to the specifics of MCO implementations. First and foremost, it is important to understand the specifications that should be considered when designing a mission critical system. Here, you will identify the various parameters and considerations necessary for the proper design of mission critical facilities.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Utilities

## Cost/Benefit Analysis

When determining the initial implementation of a mission critical system, the first step will always be to perform a cost/benefit analysis: that is, the systematic approach to making an important business decision where the costs of implementing the decision—both in amount of money and effort spent—are estimated and evaluated against the expected value to be gained from implementing the decision.

It can be hard to put a price on the value provided or protected by mission critical installations. Is it the business value of transactions or services provided each day? Is it the business impact of days or weeks of downtime? Is it the cost to start from scratch and build a new facility or system? Or is it the chance that the organization simply would not survive the loss of the MCOs?

There are certainly other business considerations, such as the amount of available capital or the cost of borrowing the funds needed to bring a mission critical system online. For the purpose of the discussion of a cost/benefit analysis, however, let's assume that the need for the system or facility is, indeed, critical and the organization already has the ability to buy or build its MCOs to at least some scale.

Given that part of the benefit side of the equation is already answered—the organization has a critical need for the MCOs—how else can you evaluate the benefits? If the system or facility generates revenue, that should be an easy dollar figure to project. A power plant makes this analysis easy, but it's not so clear with a research and development facility or an enterprise data center, both of which are clearly vital for continued operations but do not provide clear customer- or public-facing services (and therefore are not directly connected to a revenue stream).

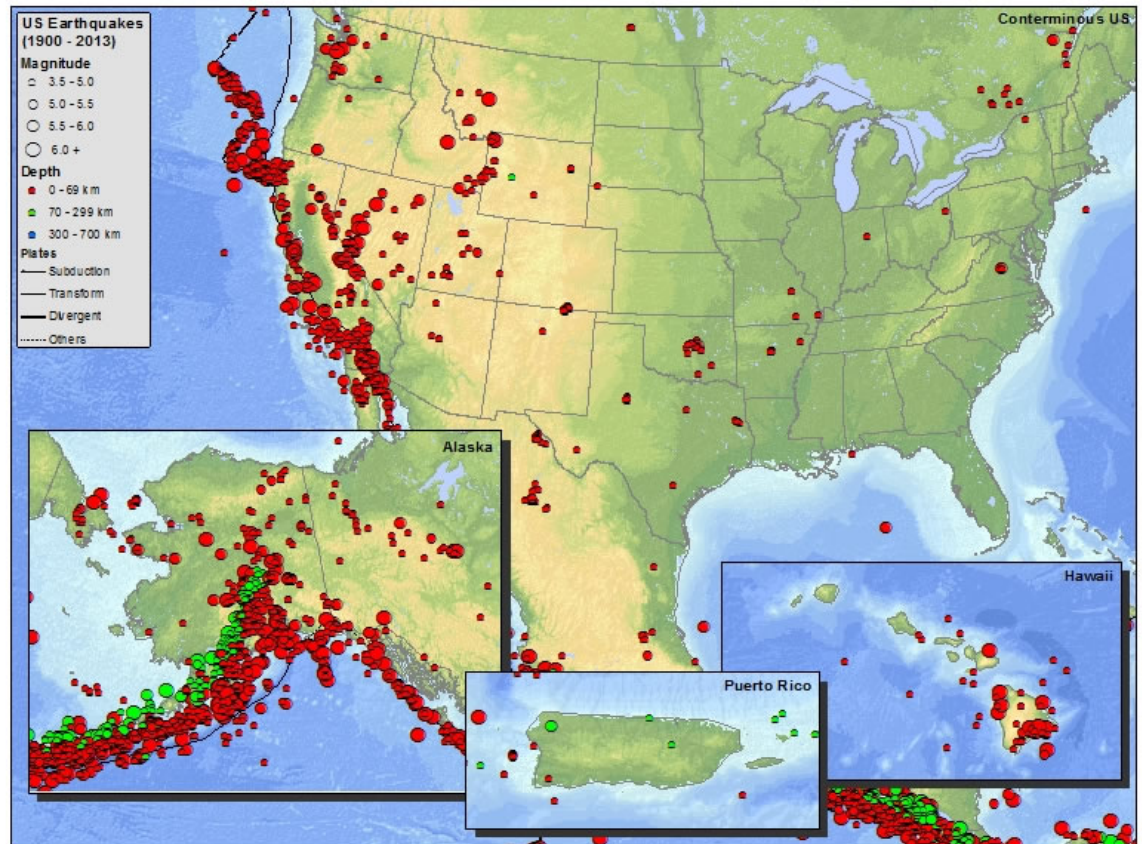
MCOs are not easily duplicated or replaced—certainly not in the sense that they can be mass-produced for easy implementation across facilities or markets—so the cost/benefit analysis of creating, maintaining, and expanding them is never as black and white as a price tag versus sales comparison. Organizations regularly engage consultants to provide this kind of analysis, which often generates hundreds or thousands of pages of reports. While it is not necessary for you as an operator to know all of these details, it is beneficial for you to understand how and why a cost/benefit analysis takes place prior to the system design and implementation.

## Site Survey and Site Selection

If your MCOs require an entire facility, the selection of the location of that facility becomes of the utmost importance. In this case, there are a number of considerations that go into the evaluation of the site to make sure that the location is suitable for the facility and allows for continued proper functioning of the critical operations that will take place within it.

When it comes to selecting a site, geographic location is often the first decision that needs to be made. The most relevant considerations regarding the geographic location is how at-risk it is to

natural or weather-related events that might disrupt its operations. Aside from the obvious threats to human safety and facility damage they can cause, natural disasters are often one of the primary considerations because there is so much data available to help with the decision-making process. For instance, the U.S. Geological Survey (USGS) has troves of free data available to review the seismic activity and risks for any location in the country. The National Oceanic and Atmospheric Administration (NOAA) operates the National Hurricane Center and provides public data on hurricane forecasts and historical events. Flood zone maps have been around for centuries and are currently maintained by the Federal Emergency Management Agency (FEMA). And, as unpredictable as tornadoes are, there is also plenty of information available on past storms and associated damage.



**Figure 1–19:** A map of the United States showing seismic activity from 1900 to 2013. (Source: <https://www.osha.gov/dts/earthquakes/>)



**Note:** For more information regarding the data available for these kinds of natural disasters, visit the respective sites of the organizations that collect and publish this data:

- For earthquake data via the USGS, visit <http://earthquake.usgs.gov/hazards/designmaps/usdesign.php>.
- For hurricane data via the NOAA, visit <http://www.nhc.noaa.gov/>.
- For flood zone data via FEMA, visit <https://www.fema.gov/flood-zones>.
- For tornado data via the NOAA, visit <http://www.ncdc.noaa.gov/climate-information/extreme-events/us-tornado-climatology>.

Transportation access—including proximity to airports, trains, major roads and highways, and even waterways—is another important consideration. While a remote site provides obvious security benefits, it can present significant cost implications for regular transit of personnel and supplies if it involves active and dynamic MCOs. Being close to major transportation hubs, however, heightens security concerns as metropolitan areas pose an increase threat from attack. In the post-9/11 era,

safety is not ensured due to the rise of global and domestic terrorism. The DHS is a great resource for researching the threat of terrorism in an area.

In these more competitive economic times, municipal and government considerations are expanding in scope for site consideration as well. In the past, the evaluation and selection of a mission critical location may have only taken into account local or state regulations, particularly those used to entice an organization to build a multimillion-dollar project in their area. Today, however, even contractors may be able to provide labor rate breaks because of subsidies created to boost local employment opportunities.

In all honesty, the scope of available information to take into consideration when selecting a mission critical location is constantly expanding, as is the existence of highly specialized consulting firms with expertise in the MCO sectors. The level of detail and the growing list of factors being analyzed is beyond the level of knowledge needed for operators, but it is still beneficial for you to understand (to some extent) why the particular location was chosen for a facility where you are working.




**Note:** System design may already be completed (when simply adding a new plant or facility) or may take place in parallel with site evaluation and selection. Keep in mind, however, that utility services, access to support contractors, travel availability, and more may end up influencing what types of equipment and systems will be practical to use.

## Utility Availability, Quality, and Reliability

In industrial terms, *utilities* refer to resources that require connections to public services such as power, water, sewage, and telecommunications. Even in locations where private or semi-private corporations are able to provide power, water, or sewage services, the strict regulatory governance and limited (if any) choice in connections allows these three resources to be considered public utilities for discussion's sake.

At all phases of analysis and design of MCOs, but certainly after the geography has been narrowed down, utility quality and availability quickly jump to the forefront as important considerations. For instance, one metropolitan area may boast incredible ease of connectivity and availability, but may have no history of supplying a single customer at the volume required by MCOs. Let's take a closer look at all of the utilities in terms of the availability, quality, and reliability of each.

<b>Utility</b>	<b>Availability, Quality, and Reliability Considerations</b>
Power Availability, Quality, and Reliability	<p>MCOs are becoming more power hungry every day, often consuming as much power as a small town. It should be no surprise, then, that power quality and availability always top the list of utility concerns during site planning and selection. How stable are the local and regional grids? What is the main source of supply to the grid? Will the site have a dedicated utility feed, or is it shared with other commercial/industrial customers?</p> <p>Power quality is a concept that deserves more detailed discussions in topics pertaining to equipment and system design, but for now, think of it as increases and decreases in the power supply. How consistent are the voltages or current being delivered?</p> <p>Availability of utility power is the most prominent factor for analysis. Availability is generally measured in the number of outages during a given time period and the average or cumulative minutes/hours of downtime during that period. Most of this data is readily available from the utility supplier.</p>

<i>Utility</i>	<i>Availability, Quality, and Reliability Considerations</i>
Water Availability, Quality, and Reliability	<p>The availability of and access to water is a key consideration for MCO facilities. It is nearly impossible for MCOs to operate without water connectivity, requiring access to multiple public water sources; however, there is growing interest in sustainable water practices, such as onsite recycling and rainwater collection to reduce this burden on public utility resources.</p> <p>Potable water is safe to drink and cook with, and is the most common utility supply, so it often ends up being what runs through our sinks, showers, and toilets. Within the facility, people need access to potable water for drinking and there must be some supply of water for sanitation. Depending upon the MCOs, there may be animals or substantial vegetation to consider as well.</p> <p>Often, equipment within MCO facilities need process water for cooling and/or operations. Process water has been more extensively treated to be used for production rather than consumption. It is not often supplied as a utility connection, but does require a supply of at least general potable-cleanliness to cut down on purification system costs and complexities. Process water, in its many forms and for its various production uses, is often made onsite using utility-provided water and the necessary tools or systems.</p>
Sewage Availability, Quality, and Reliability	<p>Wastewater has to go somewhere, and when considering the scale of industrial usage—which could be thousands or even millions of gallons—the importance of sewage as a critical utility becomes obvious.</p> <p>Wastewater from human consumption may be easily handled by onsite or shared-campus septic systems. Septic systems do introduce additional issues such as ground stability in the event of tank leakage, or potential gas buildup. This may be a worthy alternative for remote sites, but there is a practical limit to the volume septic systems can handle.</p> <p>Most commonly, MCOs rely on connections to public sewage systems, which require proper planning for the size of the connection. Anticipating any future growth or increased water usage is vital to the site planning process as repairing or extending sewage systems can be highly invasive and require substantial digging around many other live utility connections.</p> <p>Stormwater runoff systems are another component of sewage considerations for site utility planning. Looking back to flood zone evaluations in the geographic element of site selection, ensuring adequate capacity to handle major storms (10-, 50-, and 100-year flood levels) is of great importance for the location. Keeping parking lots and roadways clear are certainly priorities when striving to maintain free access to and from the site, particularly during times of heightened operational sensitivity, like major storms. In a worst case scenario, significant buildup of standing water can threaten buildings and equipment.</p>
	<p><b>Note:</b> Telecommunications is soon to be non-existent on the list of considerations as landline phones are rarely primary, critical resources anymore. The rise of commercial high-speed fiber and copper data connections, frequently in markets with multiple competitive offerings, has made voice and data transmission with high reliability widely available for use in MCO environments.</p>

## Cost as a Consideration

While some specific utility program prices might be negotiable, costs for connection and use of these utilities are generally fixed based on scale. These costs are similar in geographic regions, so if site selection is already narrowed down to a certain part of the country, this is a point worthy of nominal consideration only. If the whole country is on the table, however, utility costs could become a notable factor; for instance, the dominance of hydroelectric power in the Northern Rockies region may provide electricity costs that are less than half that of the nuclear-dominated Carolinas, which are in turn less than half that of the highly taxed grid in California.

## Backup System Scope

MCO backup systems come in many varieties supporting all types of onsite services, from smaller-scale, battery-operated systems to large-scale, fuel-generated systems. The determination of what backup system should be implemented is very detailed and design-specific, but the major commonality is the need for emergency power. The specific design of a backup system can be very complex, but there are a few general scope factors that most MCOs must take into consideration regarding how long these backup systems need to operate and the level of site stability they need to support.

<b>Factor</b>	<b>Scope Considerations</b>
Duration of Generator-Supplied Power	<p>Modern diesel generators, the most common type of backup generators, have become very reliable and stable during operation. It is fairly easy to calculate how much fuel will be required to support a given site load for a given period of time. With fossil-fuel powered generators being the most prevalent source of backup power, there is plenty of data to work with in designing the scale of these systems.</p> <p>However, you also need to consider the availability of re-fueling options in the site's area. Getting a feel for how long it would take to get a fuel supplier out to the site provides the basis for calculating the volume of onsite fuel storage, plus some safety factors assuming delays in the re-fueling. Keep in mind, most tanker trucks hold somewhere between 5,000 and 8,000 gallons of fuel, so even if the supplier can get out to the site by day two or three of an event, it may take a long time and a long line of trucks to fill up tens of thousands of gallons on onsite storage. It is also important to remember that there are often regulations in place that require fuel suppliers to service hospitals and emergency service centers first during widespread utility outages, as they are the more mission critical of the MCO facilities.</p>

<b>Factor</b>	<b>Scope Considerations</b>
Battery Life	<p>Batteries are the most simple and traditional form of backup power. Large-scale systems can provide enormous amounts of backup power, but they consume a lot of space and are costly to install and maintain. For planning purposes, designers must first answer a simple question: Are the batteries intended to sustain operations during an outage or merely provide a temporary buffer while permanent backup systems (e.g., diesel generators) come online?</p> <p>Given the level of energy used and desired runtime, it is simple to calculate the size of the systems and the number of batteries needed to support it. A particular system can either provide a small amount of power over a long period of time or a large amount of power over a short amount of time. In the first scenario, a system might have days or weeks of battery runtime, perhaps using just enough energy to keep the lights on. In the second scenario, a system might have only a few minutes, such as powering an entire data center just long enough for the generators to fire up and come online.</p>
Temperature Stability During Power Outages	<p>In manufacturing environments, let alone data centers and communications centers, there are so many electric and electronic components that ambient temperature is a great concern during outages. Backup power is at least enough to run the critical production equipment, but may be only sufficient to provide a limited cooling capacity. This is a hotly debated design consideration during site planning. In an optimal design, extremely robust backup power systems could be implemented that could sustain all normal equipment operations; however, in more realistic systems, it is more likely that the less-vital pieces of production equipment may be secured during outages to keep cooling demands lower.</p> <p>On the opposite end of the spectrum, research and development facilities with extremely cold storage requirements face an even stiffer challenge: beyond keeping the facility from getting too hot, certain areas must actually maintain their deep freeze conditions to protect research samples or prevent the damage or release of dangerous substances. Situations like this might call for completely separate backup systems dedicated only to safeguarding these materials and equipment.</p>

# ACTIVITY 1–9

## Identifying Design Parameters and Considerations for MCOs

### Scenario

In this activity, you will identify the various parameters and considerations for the design of MCO implementations.

---

**1. Which of the following are important to consider when determining the necessary scope of the backup system required for a facility?**

- The temperature stability within the facility in the event of a power outage.
- The use of generator-powered backup systems and the amount of time those generators can power the system in the event of an outage.
- The continued safety and security of personnel within the facility in the event of a power outage.
- The use of battery-powered backup systems and the amount of time those batteries can power the system in the event of an outage.

**2. When evaluating and selecting the proper location for a new mission critical facility, what is the first and likely most important decision that needs to be made about the site?**

- The available government subsidies for building the site.
- The possible man-made threats to the site.
- The potential transportation access to the site.
- The geographic location of the site and the resultant natural threats.

**3. Which of the following public utilities do MCO facilities rely on to maintain day-to-day operations of the site?**

- Power
  - Cellular
  - Water
  - Internet
  - Telecommunications
  - Sewage
-

## Summary

In this lesson, you identified MCOs and the potential threats that could interrupt the integral functions they provide or protect. Having a strong understanding of the various elements of MCOs and the important roles they play is essential for a successful career as a Mission Critical Operator.



# 2

# Mission Critical Infrastructure: Power and Power Sources

## Lesson Objectives

In this lesson, you will identify and describe the power sources relevant to Mission Critical Operations. You will:

- Understand the fundamental concepts related to power and power sources.
- Identify utility-based sources of power.
- Identify types of generator-provided power.
- Identify types of uninterruptible power supplies.
- Identify types of battery systems.
- Identify alternative sources of power.

## Lesson Introduction

When it comes to the essentials that are needed to keep a mission critical facility up and running, power is more than likely the top priority. Keeping the lights shining, the air and water appropriately heated or cooled, and all the critical components powered on are all integral to the day-to-day functions of any facility, let alone one in charge of Mission Critical Operations (MCOs). For this reason, it is easy to see why power and power sources are part of the mission critical infrastructure.

As an MCO operator, you will need to have a strong understanding of the fundamentals of power itself and all of the various sources of energy that can provide power to your MCO facility. In this lesson, you will identify and describe the fundamental concepts related to power and the power sources that are relevant to MCOs.

# TOPIC A

## Power Fundamentals

When you think of the term "power," you may think first of the utility lines that provide us with the energy needed to keep the lights and your electronic devices powered on and working. And, as you know, power is one of the utilities necessary for keeping Mission Critical Operations (MCOs) up and running. But what you may not know are the fundamental concepts of power: what power is and how it works.

The fundamental concepts of power is information that you will need to have a strong grasp of as a Mission Critical Operator, since these fundamental concepts come into play when handling the power supplied to and from your mission critical facility, and in troubleshooting or preventing any power problems. In this topic, you will learn about the fundamental concepts related to power and power sources.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Electricity
- Volt
- Voltage
- Low Voltage
- Medium Voltage
- High Voltage
- Current
- Power Factor
- DC (direct current)
- Resistance
- AC (alternating current)
- Frequency
- Single-phase Power
- Three-phase Power
- Transformer
- Rectifier
- Inverter
- Power
- Watt
- Kilowatt
- Kilowatt Hour
- kVA (kilovolt-ampere)
- Grounding
- Power Density

## Electricity

*Electricity* is most simply defined as a form of energy resulting from either the static accumulation of charged particles or the flow of charged particles. The electricity that is most relevant to the discussion of power and power sources is the latter, known as current electricity since it flows between objects or places. A good analogy for this kind of electricity is water in a hose: when the water is turned on, pressure is applied to the water at one end of the hose and pushes it out the other end. Electricity works similarly: electrically charged particles flow from one end—say, a power generator—and come out on the other end—perhaps the lights in your house.

But electricity is also a concept that encompasses all aspects about the accumulation or flow of electric charge, from the quality and volume of energy transferred to the manner in which it reacts with different components. The best way to learn about electricity is from the bottom up: beginning with the characteristics of the flowing electrons (speed & volume); the different means of measuring electric charge; and some of the most common components, or building blocks, or electrical systems.



**Figure 2-1: Power lines provide the type of electricity we are most familiar with: the kind that provides power to our homes and businesses. (Source: Jan Dudik/Creative Commons (Public Domain)/<https://commons.wikimedia.org/wiki/File:Lec06m76.JPG>)**

## Critical Systems That Rely on Constant Availability of Power

There are very few purely mechanical systems in use today that do not require some sort of electrical power. It is therefore possible to state that *all* critical systems in MCOs rely upon electrical power. The degree, however, to which equipment needs constant availability of power, or a certain quality of power is a differentiating factor. Some systems are energy hogs but are not highly sensitive to ebbs and flows in the power supply, while some other systems use only a small amount of electricity but have little or no tolerance for any fluctuation in the quality of power supplied.

One example of a critical system that relies on the constant availability of power would be a computer-based system, like a data center, in which the components are highly sensitive to a constant supply of electricity at a specific voltage. The concern here is that any interruption, no matter how momentary, can cause a hiccup in the function of a delicate high-speed motor component, which would then cause ripple effects throughout other MCOs. Loss of data or continuity of data are both a great concern for all the electronic and digitally controlled systems in place today.

Another example would be the critical components of a disease research and control facility. Imagine a centrifuge in the research center, spinning at tens or hundreds of thousands of

revolutions per minute to analyze disease samples. If power is lost even for one second, let alone minutes, the analysis and sample may be ruined. Or worse yet, the machine is set off-kilter and catastrophic physical damage to the important samples could occur.

The other form of MCO electrical systems particularly concerned with the constant availability of power are those with complex or extended start-up cycle times. Plenty of MCOs have sufficient tolerance or backup plans to handle a system going offline for a few seconds or a minute; for instance, an emergency communications/command center could temporarily allow data to be routed elsewhere and rely upon the most recent information or view information from another location to continue making decisions and move operations forward. But, bringing all of these systems back online, in the proper sequence and with the proper security considerations in place, might actually take hours or days to complete. In this case, those two seconds of power drop begin to cripple MCOs for an extended period of time.

## Case Study: Power Loss and Preparation

Suffering a power loss is one of the worst things that can happen to MCOs, as it will bring down the entire operations of a facility that is critical to keep up and running. One of the most unpredictable events that can lead to widespread power outages are weather-related natural disasters. Case in point: the devastating effects from the havoc that Hurricane Irene wreaked on some of the most critical facilities along the eastern seaboard, including power loss at one major national telecom company's MCOs.

On a Friday in late August 2011, facility managers and MCO personnel across the country shifted into high gear as Hurricane Irene—a massive category 1 storm—was about to make landfall in the Carolinas. While proper preparations were in place to the extent possible, not everyone was ready to handle the \$14 billion in damage Irene would leave behind after driving straight up the eastern seaboard through New England.

One team of Critical Facility Managers running the national telecom company's MCOs started response activities even before the first power lines went down. In the days or hours before a storm like this, they would begin inventorying fuel levels at all the MCO locations and calculate available run times should outages occur. Knowing they were in for a long weekend, the team also began aggregating vendor contact information so other FMs could take over response efforts while eastern regional FMs could catch rest when possible. In this case, as the forecasts sharpened up and it was evident there would be widespread power outages across many states, additional fuel supply vendors were brought on board.

Once power went down at the MCOs, the FMs ran through checklists: contacting client managers to check the status of supported technology, verifying with any onsite personnel that backup equipment had picked up the critical power load and generators were starting, and having site walks done to check the infrastructure. All told, 17 sites lost power, 2 for as long as 4 days. All but one site sailed through fine with no interruptions to MCOs except for some minor equipment failures (backup pumps developing minor leaks, for instance) that could be dealt with after the storm.

The one site that went down did so because the output breaker of the generator failed. It was an older site (the breaker itself was probably at least 15 years old), so the equipment failure was not that shocking. The problem, though, was that the customer had previously refused to follow the team's recommendation to update the building's load transfers as part of the electrical maintenance program. It had been years since that breaker had been cycled, so who knows: perhaps that failure could have been found during a controlled, scheduled maintenance evolution and repaired, instead of coming to light during the height of the storm and causing a critical outage.

## ACTIVITY 2-1

### Power Loss and Preparation: Reflective Questions

#### Scenario

Based on the previous case study, think about the following questions in regard to how this specific scenario relates to Mission Critical Operations.

1. What does this scenario tell you about the effect of a power loss and the importance of being prepared for a potential outage when it comes to MCOs?
2. In this specific situation, what could have been done differently to prevent the power loss at the MCO site?

#### Voltage

*Voltage* is the potential difference in electrical energy (or charge) between two points, which correlates more plainly to the speed that electrons flow through this charge or the amount of pressure pushing or pulling them.

#### Volts

A *volt*, represented by the letter V, is both the unit of measure most commonly used to express voltage, as well as being an aspect of flowing electricity. Think of it this way: conceptually, it is like both the *speed limit* of a roadway and the *actual speed* of the cars travelling on that roadway. The speed limit on Interstate 5 is 70 mph whether or not there are vehicles on the road going 70 mph; in the same manner, a 12V flashlight is still a 12V flashlight whether it is turned on or off.



**Note:** History and science buffs alike may find it interesting that this unit of measure is named after Italian physicist Alessandro Volta, who invented what is considered the first chemical battery in the late 18th century.

Systems are designed to operate at specific voltages, but are not always restricted to that voltage. However, that specific voltage needs to be supplied as consistently as possible to allow the system to operate properly but not running too far outside of optimal operations and potentially causing damage; in the roadway example, this would be establishing a speed limit that allows for the efficient travel of all the commuters on the road, but prevents dangerous speeds that potentially result in loss of control, accidents, or wrecks.

## Low Voltage

*Low voltage* equipment or systems can be loosely categorized as those that operate or are capable of operating below regular residential voltage levels. There are actually many technical definitions of what constitutes a low voltage system that vary by industry and country; however, a consistent standard throughout the MCO industry in the US would be that a low voltage system is one operating at 100V or less.

Some examples of common low voltage systems are included in the following table.

<b>System</b>	<b>Description</b>
Controls circuits	<p>Wiring circuits for building and equipment controls systems run at a multitude of voltages and tend to vary most with the age of the system or facility. In newer installations (within the last decade or two), you will most frequently run across 24V controls systems. Voltage is dictated by the types of components and controllers on the circuits, but the trend is moving towards standardization to increase the commonality of repair parts (wiring harnesses, power modules, backup batteries, etc.).</p> <p>You may also see or hear controls circuits referred to as signal wiring, particularly in international settings.</p>
Voice circuits	<p>Voice circuits, or telephone signals, are becoming less prevalent as voice signals are being carried along data lines or cellular/wireless networks. Telephone wiring most commonly uses RJ11 cables, with 6 small-gauge pin conductors and wires (typically, 22 or 24 gauge), which utilize nominal voltages of less than 10 volts.</p>
Network/data circuits	<p>Most recently, network wiring—Ethernet (RJ45) being the global standard—has become the commonplace low voltage system that MCO operators and technicians are most likely to interact with. Standard Category 5 (Cat-5) Ethernet wiring is made up of 4 twisted pairs of 22 gauge wire. Category 6 (Cat-6) wiring has the same number of conductors, but more stringent specifications in construction and insulation that improve operational frequency ranges and signal clarity.</p> <p>A recent technological innovation is the utilization of Ethernet cabling to power low voltage components like telephones and LED light fixtures, making the presence of RJ45 all the more likely.</p>



**Note:** While some may still consider 120V “house” circuits (general use outlets) as low voltage, operators in MCO roles should be utilizing the safest or more conservative maintenance practice recommendations governed by the National Fire Protection Association (NFPA) and National Electric Code (NEC), under which maintenance and repair of 120V circuits requires more Personal Protective Equipment (PPE) than other common low voltage systems.

## Medium Voltage

*Medium voltage* is the most loosely defined across industry standards, but generally refers to any system operating at equipment voltage levels, which includes everything from 110/120V (the voltage of a typical wall outlet circuit) up to 1 kilovolt (KV).

The following table includes some examples of common voltages falling within the medium voltage range and their common applications.

<b><i>Voltage</i></b>	<b><i>Application</i></b>
110/120	<ul style="list-style-type: none"> <li>• Wall outlets</li> <li>• Corded tools/equipment (i.e., window fans)</li> </ul>
220/240	<ul style="list-style-type: none"> <li>• 3- or 4-wire corded appliances/light equipment (i.e., commercial air compressors)</li> </ul>
277	<ul style="list-style-type: none"> <li>• Commercial/industrial lighting systems</li> <li>• Small hard-wired equipment (i.e., exhaust fans)</li> </ul>
480	<ul style="list-style-type: none"> <li>• Industrial-grade equipment (i.e., HVAC units)</li> </ul>

Operators working in MCOs should be most concerned about the medium voltage systems in their day-to-day MCO tasks, primarily due to the various levels of specified protective equipment and safety regulations required to operate and maintain the power components within a medium voltage system. In this case, dedicated safety and technical training is required, but stops short of needing a full electrical license or advanced preparations.

## High Voltage

Especially in the MCO industry, *high voltage* commonly refers to those systems operating between 1 kilovolt and 15 kilovolts, which is generally limited to the utility supply equipment, such as switchgears, generators, transformers, and main distribution breakers. Some large-scale manufacturing or power generation systems may have high voltage components inside the facility, downstream of the utility supply and backup power systems, but they will be highly specialized to the location.



**Figure 2–2:** The equipment that is part of the utility supply, such as a step voltage regulator, operates using high voltage. (Source: Ebiebi2/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Step\\_Voltage\\_Regulator\\_1.JPG](https://commons.wikimedia.org/wiki/File:Step_Voltage_Regulator_1.JPG))

Live high voltage circuits are incredibly dangerous to work around, since there is no protective gear in existence that can protect an operator from the hazards associated with an electrical fault. MCO operators and technicians rarely perform maintenance on these systems as it is left to utility electricians or specialty contractors due to the infrequency of operation and the levels of knowledge required to do so safely. However, protective gear should be worn even when operating breakers and switches at these voltages with the housings fully closed.

## Current

Electrical *current*, represented by the letter *I* in scientific equations, is the flow of electric charge in a circuit, typically carried by charged electrons moving along a wire. Current takes into account both the volume of electrons in the circuit and the speed in which they are moving, which is the circuit's voltage.

## Amperes

Amperes, represented by the shortened term amps or the letter *A*, is the unit of measure for expressing the flow rate of an electric charge, or current. Scientifically speaking, one ampere is equal to the current flowing in two parallel wires, one meter apart, producing a force of  $2 \times 10^{-7}$  newtons per meter.



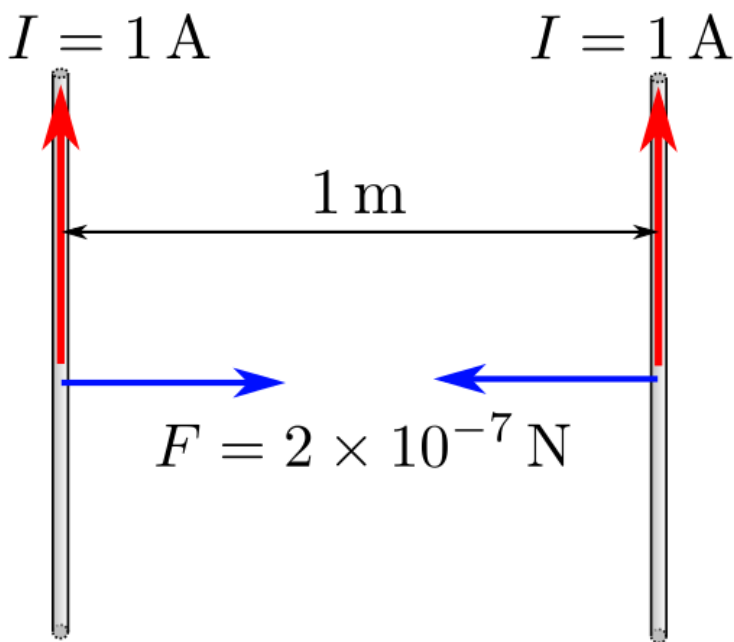


Figure 2-3: An illustration of an ampere. (Source: Danmichaelo/Creative Commons (Public Domain)/<https://commons.wikimedia.org/wiki/File:Ampere-def-en.svg>)



**Note:** A newton is a derived unit of force, represented by the letter N, where one newton is equal to the amount of force needed to accelerate one kilogram of mass at a rate of one meter per second squared.

Current, expressed in amps, is measured by using an instrument called an ammeter.

## Power

*Power* measures the work done (or the potential work that can be done) by electricity. Specifically, power is the rate at which a given amount of energy is transferred through an electrical circuit. The

power of a system can be calculated using the simplified equation  $P = V \cdot I$ , or power = voltage x current.

## Power Factor

In a real, operating electrical system, there are many components that are influenced by their environment that create inefficiencies. So how do you bridge the gap between ideal physics and real-world function? By using the *power factor*, a concept generally calculated indirectly as the ratio of real power (the amount of energy actually available or used) to apparent power (the potential power purely available in an ideal system with no losses). A power factor of 1.0 in a system is referred to as a "unity" and represents perfect conditions.

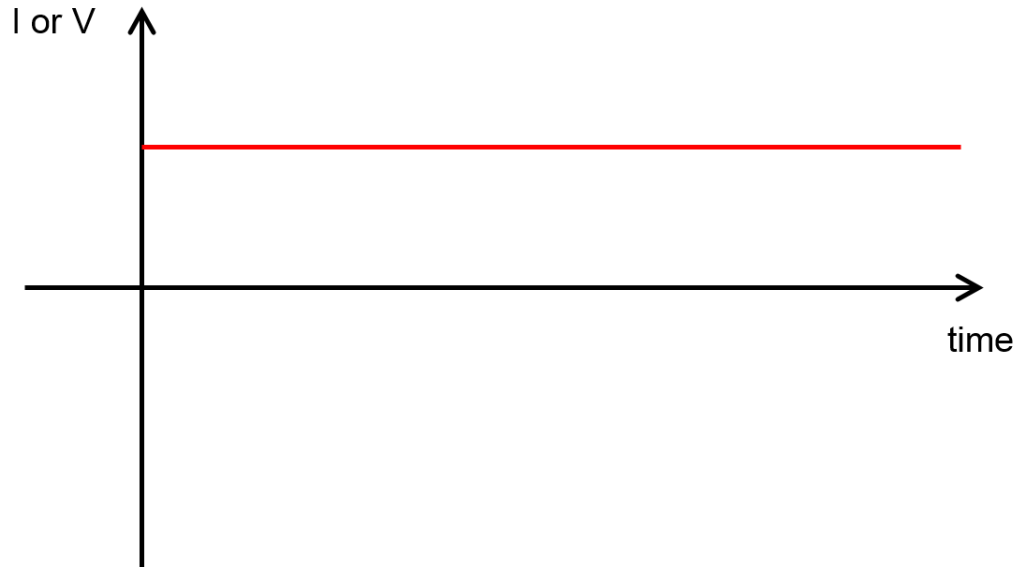
## Direct Current

*Direct current (DC)* is a constant flow of electricity that travels in one direction. It is the "original" type of electrical power, or that which is produced by batteries. In a DC system, both voltage and current are constant, and there is another variable at play: *resistance*, which is the innate property of most conductors that creates opposition to the passage of an electrical current. Resistance is measured in ohms, represented by the symbol  $\Omega$ , named after the German physicist who discovered this property.



**Note:** An ohm is the resistance between two points in a conductor when a constant potential difference of one volt, applied to both points, produces one amp of current.

According to Ohm's Law, current is proportional to the voltage or resistance in a circuit, giving the other being constant. It is expressed as  $I = \frac{V}{R}$  where I is current, in amps; V is voltage, and R is resistance.



**Figure 2-4:** An illustration of direct current (red line), where the vertical axis measures current or voltage and the horizontal axis measures time. (Source: *Logical Operations for NCMCO*)

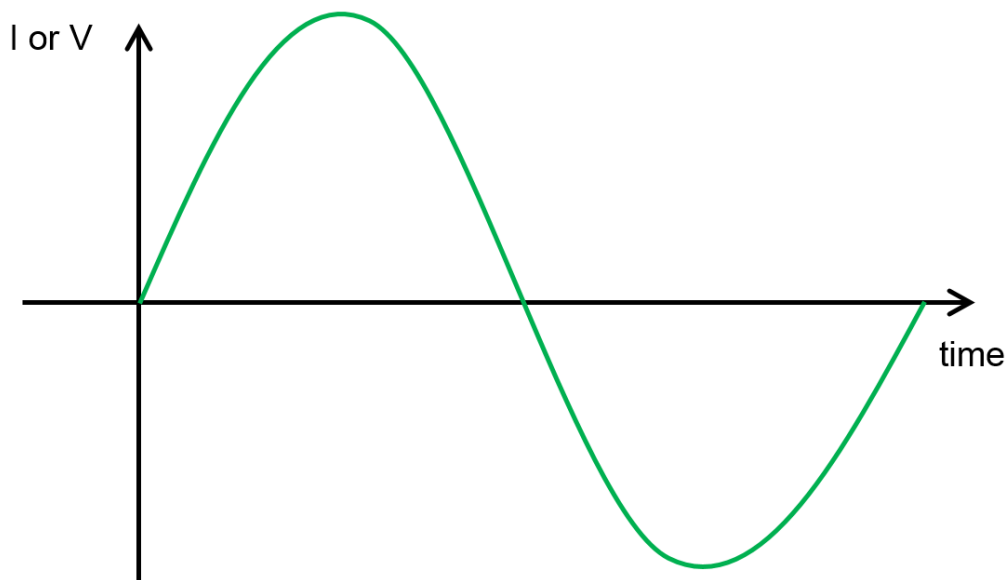
## Alternating Current

*Alternating current (AC)* is one in which the electrical charge periodically reverses the direction in which it flows.

Alternating current first appeared in use in Europe during the mid-19th century via several early versions of an alternator, a device that converts mechanical energy into electrical energy by use of rotating magnetic fields. British scientist Michael Faraday is one of the most well-known of those working with electromagnetism as a source of energy; based on his work, we now know that rotating magnetic fields create energy, which can then be captured by conductors wound around the space in which the magnet is being rotated.

Consider two variables in this scenario—a conductor at a single, fixed position in this space and a magnet, which has two poles of opposite charge—and it is a bit easier to understand how AC occurs: electrons are being pushed away from the negative pole of the magnet in increasing volumes as the pole approaches the fixed point, creating a flow of electrons to that point, which then decreases as that pole rotates away. The same happens, in reverse, with electrons being pulled to the positive pole, creating a flow of electrons away from the fixed point. The result is an alternating current, as the charge periodically reverses its direction of flow in response to the magnetism of the poles.

The rate at which AC voltage cycles from its positive peak, to zero, to its negative peak, and back again is the *frequency* of the AC electricity. Frequency is measured in hertz (Hz), or cycles per second. Because of its peaks and valleys, AC looks like a wave—specifically, what is called a sine wave.



**Figure 2-5:** An illustration of alternating current (green line), where the vertical axis measures current or voltage and the horizontal axis measures time. (Source: *Logical Operations for NCMCO*)

## Single-Phase Power

*Single-phase power* is a specific type of AC power distribution where a single conductor carries one waveform of current, or multiple conductors carry multiple currents with matching waveforms. A single-phase AC power supply does not create a magnetic field in the motor it is connected to, and therefore needs additional circuits to start the motor. For this reason, single-phase power is the most common power distribution scheme for residential and light duty commercial environments, which use few large motors or no motors at all.

## Three-Phase Power

*Three-phase power* is a specific type of AC power distribution where three conductors (or sets of three conductors) reach the peaks of their current waveforms sequentially. When Phase A is at its maximum positive voltage, the waveform for Phase B is crossing through zero volts, and Phase C is at its maximum negative voltage. Therefore, frequency is measured peak to peak for any one of the phases.

Since there is a near-continuous current at its peak-positive voltage available, three-phase power is a common power distribution scheme for grid-level distribution and supply to heavy use commercial or industrial locations.

## Transformers

A *transformer* is an electrical device that changes voltage in an AC circuit—either increasing it or decreasing it—by varying the current flowing through the conductor's internal wires using a process called electromagnetic induction. Basically, it manipulates the characteristics of the rotating electromagnetic fields that create AC power in the first place, in order to “step up” or “step down” the AC voltage supplied. Most commonly, transformers are used to reduce the voltage as it works its way down through the electrical distribution system from high-voltage utility supplies to the end-use equipment.



**Figure 2–6:** A utility lineman replaces the transformer on a utility pole, which decreases the high voltage coming along the power lines to a lower voltage that can be used in a home or business. (Source: Dave Pape/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Lineman\\_changing\\_transformer.jpg](https://commons.wikimedia.org/wiki/File:Lineman_changing_transformer.jpg))

## Rectifiers and Inverters

It is often necessary to convert power from AC to DC or vice versa. This is accomplished by using either a *rectifier* to convert AC to DC, or an *inverter* to convert DC to AC.

Rectification is accomplished by the rectifier chopping up the moving wave of the AC current into pulses of a constant voltage that move in a single direction. This solves the problem of getting to a unidirectional flow of charge at this given voltage, but it is still not a smooth, constant current due to the spaces between the output pulses. For many types of equipment, this is satisfactory, but for highly sensitive components performing functions (often at a rapid rate), filters may be needed to complete the full transition to DC power.

Inverting power is essentially the same, but in reverse. The inverter takes varying voltages within the DC current and slices them into “steps” that cyclically decrease and increase to create the peaks and valleys of an AC sine wave. Much like filters smooth out the new DC output in rectification, the more steps that an inverter adds into the AC output, the closer it comes to natural AC.

## Watts and Kilowatts

A *watt* is the global standard for measuring electrical power and has a value of one joule per second. One watt is not a tremendous amount of energy, so you may often encounter the measurement of a *kilowatt*—or 1,000 watts—more commonly used in the MCO lexicon.



**Note:** A joule is a derived unit of energy, represented by the letter J, where one joule equals the energy of passing one amp of current through 1 ohm of resistance for one second.

## Kilowatt Hours

At times, you may need to measure or calculate the amount of power exerted or consumed by a system over an extended period of time; in short, a means of measuring a cumulative power reading. A *Kilowatt hour (kWh)* is the normal unit for this measurement—you may be familiar with this measurement from your own power bill—and is derived from multiplying Power (P) x time (t).

Aside from the power company wanting to know how much to charge you this month, this is a common means for measuring and comparing equipment efficiencies. For instance, a system may have two motors, and the MCO facilities engineers think they have found a manufacturer whose motors runs 30% more efficiently. To find out if this is accurate, presuming that they each produce the same output, you would measure the actual power consumed over a period of time and see which motor used less kWh.

## kVA

Whereas watts are the units of measurement for real power, *kilovolt-amperes (kVA)* are the units of measurement used for apparent power when taking the power factor into consideration. This is calculated by simply multiplying power (P) x current (I), and is therefore measured in volts x amps—which is more commonly expressed in kVA, or 1,000 volt-amps.

Since this does not discount power from what is actually being generated or delivered, kVA is used for equipment ratings so that a standard baseline exists for comparing gear that could have different power factors when installed in different systems.

## Grounding

*Grounding* is the process of removing excess electrical charge and distributing it to a larger body capable of receiving that charge. Most commonly, that charge is sent down to the earth via a conductor.

The easiest way to think about grounding is lightning itself. The atmosphere and clouds accumulate charged particles due to the changing weather conditions. The charge then finds the earth as a happy receptor for all of that energy. Now consider the use of lightning rods: where the lightning bolt was an uncontrolled discharge of these particles, a lightning rod can be used to accept the excess charge and purposefully move that current through a conductor safely to the ground.



**Figure 2–7: Lightning striking the ground illustrates the concept of grounding: it transfers the excess electrical charge in the lightning to the earth, which is capable of receiving the charge. (Source: Tech. Sgt. Cherie A. Thurlby for the United States Air Force/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Lightning\\_strike\\_near\\_Capitol\\_building.jpg](https://commons.wikimedia.org/wiki/File:Lightning_strike_near_Capitol_building.jpg))**

Grounding is an important safety measure, both for people and equipment. Imagine that the insulation on a piece of equipment has failed; the excess charge that is built up could pose a shock hazard to operators working in the vicinity or could cause arcing between components—resulting in anything from minor damage to sensitive electronic boards, to explosions if near a flammable substance.

## Three–Wire vs. Four–Wire Power Cords

A three-wire power cord has three wires: one hot, one neutral, and one ground. A four-wire power cord has four wires: two hot, one neutral, and one ground. The ground wire serves the same protective purpose in both types. The neutral wire is perhaps even more complex than the concept of grounding, as it can serve multiple purposes. For the sake of comparing power cords, however, it is easiest to consider the neutral conductor as the return path for the electrical circuit. What sets these two applications apart is that having two hot conductors allows delivery of power at two different voltages (to different components in the equipment), both of which can share the neutral path.

## Power Density

*Power density* is a concept most pertinent to design and construction, but is of increasing importance in electrical system fundamentals. Just as the name implies, it refers to the quantity of power consumed in a given infrastructure footprint. This could be a vertical power density, such as in the spaces of a vertical server rack in a data center; or lateral power density, such as the equipment in a manufacturing space. Power density is one of the main bridges between electrical and mechanical cooling design, because it tells us not only how much heat-generating equipment needs to be cooled, but how concentrated the cooling needs to be.

# ACTIVITY 2-2

## Identifying Power Fundamentals

### Scenario

In this activity, you will identify the fundamental concepts of power and power sources.

**1. Which power distribution scheme utilizes conductors carrying currents with matching waveforms?**

- Direct current power
- Alternating current power
- Single-phase power
- Three-phase power

**2. Which power distribution scheme utilizes conductors carrying currents that reach their peaks sequentially?**

- Direct current power
- Alternating current power
- Single-phase power
- Three-phase power

**3. Which type of electrical power utilizes a constant flow of electricity in a single direction?**

- Direct current power
- Alternating current power
- Single-phase power
- Three-phase power

**4. Which type of electrical power utilizes a current that periodically changes the direction of its flow?**

- Direct current power
- Alternating current power
- Single-phase power
- Three-phase power

**5. Which unit of measure is used to express the potential difference in electrical energy between two points?**

- Watts
- Amperes
- Volts
- Kilovolt-amperes

**6. Which unit of measure is used to express the flow of electric charge in a circuit?**

- Watts
- Amperes
- Volts
- Kilovolt-amperes

7. Which unit of measure is used to express the amount of energy actually available or used in an electrical system?
- Watts
  - Amperes
  - Volts
  - Kilovolt-amperes
8. Which unit of measure is used to express the potential power available in an ideal system with no losses?
- Watts
  - Amperes
  - Volts
  - Kilovolt-amperes
-



# TOPIC B

## Utility–Source Power

The next important concept to discuss, once you understand the fundamentals of power, is where power comes from. There are a myriad of energy sources in use today, and that list keeps growing as old sources fall out of fashion and new sources are discovered or developed. Of these sources, utility-source power is one of the most common sources of energy and the one you are probably most familiar with, since you see it and use it on a daily basis.

As an MCO professional, you will need to know where your power comes from and understand the nuances of how and how much power comes into your MCO facility from the source. In this topic, you will identify utility-based sources of power.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Grid
- Microgrid

## Sources

Utility power refers to the electricity that MCOs receive from external sources, typically from a combination of public and privately-owned power plants, as well as public and regulated private/semi-private utility distribution companies that are part of "the grid." Speaking at a high level, the *grid* is the collective system of transmission lines, switching, and substations involved in providing utility power. Generally speaking (with Texas being a notable exception) the national grid is a highly regulated, shared domestic public resource, although it may be operated and maintained by a mix of the organizations listed above.

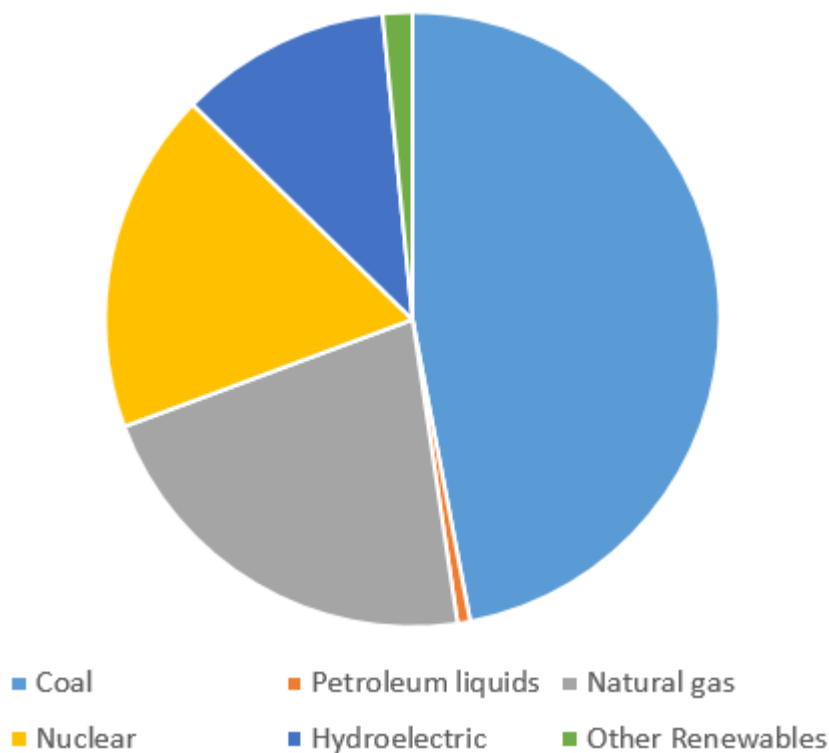
Domestic power is produced from multiple energy sources—the list of which is almost constantly growing due to the advent of various renewable energy sources. However, the following is a list of most common sources that provide utility power.

<i>Utility Source</i>	<i>Description</i>
Coal	<p>Coal-fueled power generation plants supply about half the electricity in the United States. Coal is the original fossil fuel and receives the most press regarding the environmental impact of its use. It is formed over long periods of time as geological processes build up over layers of biological material—mostly plants. Coal is extracted from the earth via mining.</p> <p>The basic concept for creating power from coal is common to most electricity generation plants: create a heat source to turn water into pressurized steam which may then transmit mechanical energy to a turbine. The rotation of the turbine may directly, or indirectly, spin the rotor of a generator set.</p>
Natural Gas	<p>The prevalence of natural gas power plants has doubled in the last decade, now supplying about 20% of the nation's electric power. The jump is partially due to some expansion of the natural gas distribution infrastructure, in the form of more pipes and pipelines, but a large part of natural gas's recent success is accredited to it being viewed as a cleaner alternative to traditional coal-burning plants. In fact, burning natural gas in power plants emits only half the CO<sub>2</sub> that burning coal emits.</p>


<i>Utility Source</i>	<i>Description</i>
Nuclear	<p>Nuclear power plants have been around for more than half a century, but still remain the most controversial. Nuclear has held steady at about 17% of domestic electricity production, largely due to a nearly three-decade ban on further development after the Three Mile Island accident in 1979. Nuclear power plants require a large amount of time and money to build, but are incredibly powerful and efficient in sustained operations.</p> <p>Very similar to most traditional power plants, the nuclear reactor is simply the source of heat to transmit energy to water, making steam. There is nothing being burned, however, so greenhouse gas emissions are not a large concern. Clearly, radioactive waste is a concern, but the biggest impact from nuclear power is heat pollution, beyond the easily recognizable cooling towers exhausting massive clouds of steam. Plants are typically located near a body of water, which is circulated as a cooling medium for many of the plant's systems, so the heat removed from the plant gets put back into the river or lake.</p>
Hydroelectric	<p>Hydroelectric power sits atop most lists in being clean, efficient, and reliable—which could be why it currently provides about 10% of the nation's power. Water wheels at mills along rivers a few centuries ago captured the mechanical energy of flowing water and used it for mechanical work. With hydroelectric, that mechanical energy is simply used to spin a generator and create electricity.</p> <p>There are no notable emissions, no fuels to be consumed, and no supply issues so long as the river keeps moving. Most hydroelectric plants use dams, though, to increase the available mechanical energy when the water has further to fall—thank you, gravity!—which does introduce some environmental impact concerns. Upstream of the dam, areas are flooded as the water level rises (displacing animals and people), and unless "ladders" are built, the dam prevents fish and other river creatures from getting further upstream than the dam itself.</p>
Solar	<p>Solar is the most abundant energy source available; historically, however, it has been difficult to convert it in large enough volumes. Photovoltaic cells work via a complicated mechanical and chemical set of processes to convert sunlight into electricity, a function scientists have known about since the mid-19th century. Solar power can be created on the megawatt scale, but it requires acres and acres of solar panels. Small-scale implementations have readily taken to using solar panels—whether in small-sized "farm" form or installed on individual houses—to supplement non-critical power during daylight hours when electricity costs tend to be at peaks.</p> <p>Night-time is the biggest setback for solar power. Even if a large enough solar installation were constructed and extra energy produced, there simply does not exist a large enough battery or battery-system to store that energy.</p>

Utility Source	Description
Wind	<p>Windmills have been around for centuries, quietly converting the wind's energy to some other usable form of energy; first mechanical, and now electrical. Wind turbines are another very clean source of energy, but have yet to become efficient enough to truly become a widely usable source; recently, however, modern blade designs and low-friction turbines have made significant progress to that end.</p> <p>Wind power remains plagued by reliability. The wind isn't always blowing, at the same speed, or in the same direction. Modern wind turbines are intelligent enough to move their orientation to face the changing wind, but there's still not much to be done when there's nothing but a gentle breeze. Again, if industrial-scale power storage were available, wind power would likely play a larger role in supplying utility power to the masses.</p>

To give you a quick visual of how the nation's energy production is currently broken up amongst these common power providers, take a look at this pie chart displaying the amount of energy produced by each utility source.



**Figure 2-8:** A pie chart of US energy production in 2015, by source. (Source: Logical Operations for NCMCO)



**Note:** Petroleum liquids will be covered under generated-provided power. Additionally, it is important to note that these percentages are based on the data available in 2015. These are subject to change based on the ever-changing energy industry—the energy source that is most prominently used may change over time.

## High vs. Medium Voltage Systems

When discussing utility supply power levels, there is some difficulty in clearly quantifying power levels, particularly the upper and lower boundaries for medium voltage systems. For the purposes of

grid connections, let's just consider the utility supply lines at the point where MCOs take ownership; the voltage at that location will determine what other substation and transformer equipment MCOs need, and perhaps most critically, the backup power source.

Some MCOs take the full 100+ kVA supply from the utility main transmission line and have large substations onsite. Some take power from the utility that's been stepped down once to something closer to 12-15kVA but also have generators that operate at that same level, so the final step-down happens inside the facility, regardless of where the power is being supplied from. Still others take power that's been fully reduced to site operating levels (typically 480V) via a utility reducing station and a "campus" reducing station, and then also run their generators at this voltage.

Determining the appropriate incoming power supply voltage for MCOs is a balancing act either driven by money or end-use (both the equipment being used and operations team using it). At the lowest levels, the operational benefit is not having to deal with large transformers or higher voltage switchgear onsite. However, designing a system with a lower voltage limits, to a certain extent, any further expansion of MCOs; it would be incredibly costly to have to install a step-up transformer or bring a new, higher kVA feed into MCOs if a new piece of machinery needed it.

On the flip side, high voltage distribution is much more energy efficient. There are losses associated with the distance that electricity has to run, and there is always some loss from moving the electricity through the various power equipment in the system (transformers, substation gear, etc.).

Transmission losses increase at lower voltages. So for example, taking a 112kVA or 36kVA feed from the utility, stepping down once to 14kVA, running generators at 14kVA, and then utilizing smaller transformers close to the end-use gear is a more efficient use of power and allows for flexibility and scalability in future MCO use.

## Microgrids

A *microgrid* is a small-scale, localized utility-source system that can disconnect from the larger, more traditional utility-source grid (i.e., the public or privately-owned power plants and distribution centers) either partially or completely. A microgrid can operate autonomously, providing its own generation, storage, and transmission of electrical energy, though typically at a low voltage. In this way, it is an excellent source of both small-scale energy production and a powerful backup option for any interruptions to the power provided by the larger utility-source grid.

With all this in mind, you may think that any MCOs with a backup power source would be considered a microgrid, but that's not entirely accurate. This is particularly relevant in a campus setting, where the backup power will be the supply for multiple loads, both critical and non-critical, and needs to be able to do so for an extended period of time. Additionally, using only a petro-fuel based generator as the sole source of power, without the support of the main utility grid, is limited by how much fuel storage is onsite (and subsequently, how often fuel deliveries would be required). A true microgrid setup is going to have some kind of co-generation plant and/or standalone power plant such as biomass, solar, or wind power.



***Figure 2-9: A solar panel on the grounds of the Marine Corps Air Station in Miramar, California is part of a microgrid providing warm water to the barracks and supporting backup power for a nearby landfill. (Source: Lance Cpl. Christopher Johns for the United States Marine Corps/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Energy\\_assurance\\_only\\_a\\_microgrid\\_away\\_140113-M-OB827-007.jpg](https://commons.wikimedia.org/wiki/File:Energy_assurance_only_a_microgrid_away_140113-M-OB827-007.jpg))***

## ACTIVITY 2–3

### Identifying Utility–Based Power Sources

#### Scenario

In this activity, you will identify the sources of utility-based power.

---

- 1. What is the collective system of buildings, devices, and equipment involved in the production and distribution of power called?**
    - Utility-source
    - Framework
    - Grid
    - Microgrid
  - 2. What is a small-scale, localized utility-source system that can operate autonomously to generate, store, and transmit power called?**
    - Utility-source
    - Framework
    - Grid
    - Microgrid
  - 3. Based on the data presented in this book, which utility-source provides about half of the electricity for the United States?**
    - Nuclear
    - Coal
    - Natural gas
    - Hydroelectric
  - 4. Based on the data presented in this book, which utility-source provides about one-fifth of the electricity for the United States?**
    - Nuclear
    - Coal
    - Natural gas
    - Hydroelectric
  - 5. For a brand-new MCO system that is likely to expand and need to scale-up in the future, which power distribution scheme would be the best fit?**
    - A low voltage system
    - A medium voltage system
    - A high voltage system
    - None of these
-

# TOPIC C

## Generator–Provided Power

While utility-based power is the optimal source of electrical power for MCOs, there will always be a need for a backup power supply. For this, generator-provided power is the most common source of backup energy. But, of course, there are many types of backup generators and fuels that can be used to power them, and different types of system components to safely switch between the two sources of power.

As an MCO operator, it will be vitally important for you to have a strong working knowledge of generator-provided power and how to integrate this source of backup power into your MCOs. In this topic, you will identify the different types of generator-provided power and the system components used to implement them safely.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Generator
- Prime mover
- ATS (automatic transfer switch)
- Throw-over switch
- Paralleling switchgear

## Generators

Generators are by far the most recognizable and widely implemented source of backup electrical power for MCOs. A *generator* is a machine used to convert mechanical energy of some kind into electrical energy. By industry standards, the terms "generator" and "generator set" are often used interchangeably, but in fairness, the generator itself is the part of the system making electricity and the generator set is the engine attached to the generator that provides the mechanical energy.

Another term that you may find used to refer to any machine providing electricity is *prime mover*, since there are a few MCO designs that use something other than an engine to turn a rotor and generate electricity.



**Figure 2-10: Construction electricians with the US Navy move a portable backup generator, which will be used to provide power to residents affected by an earthquake. (Source: United States Navy/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:US\\_Navy\\_070719-N-2560Y-001\\_Construction\\_Electrician\\_2nd\\_Class\\_Ryan\\_Nichols\\_and\\_Senior\\_Chief\\_Construction\\_Electrician\\_Alejandro\\_Bautista\\_of\\_Naval\\_Air\\_Facility\\_Atsumi\\_Public\\_Works\\_Department\\_load\\_a\\_portable\\_generator\\_to.jpg](https://commons.wikimedia.org/wiki/File:US_Navy_070719-N-2560Y-001_Construction_Electrician_2nd_Class_Ryan_Nichols_and_Senior_Chief_Construction_Electrician_Alejandro_Bautista_of_Naval_Air_Facility_Atsumi_Public_Works_Department_load_a_portable_generator_to.jpg))**

## Generator Types and Ratings

There are different types of generators that are rated for use in certain situations, based on their size and function. The intended use within MCOs typically guides which type of generator is the best fit for a system. The following lists the various types of generator-sets.

<b>Generator Type</b>	<b>Description</b>
Stand-By	Stand-by generator sets are exactly as the name implies: purely backup systems. These engines are off, in a normal state, but fully operational and waiting on a start command to fire up and power MCOs. Stand-by generators may be required to operate for extended periods of time in large emergencies, but ideally only need to run for a few hours during a utility outage. Typically, a stand-by generator will have some more rugged components installed, such as heavy-duty starters and starting batteries, pre-lubrication pumps, and jacket water heaters, so as to be able to start immediately during any condition.



<b>Generator Type</b>	<b>Description</b>
Continuous	Continuous-designed generator sets are intended to run all of the time, with a relatively constant load. Typically, a continuous-run generator is sized to carry all of the critical load for MCOs and will supplement something near that amount of power during normal operations. This design is often chosen in more remote locations where power may be limited or unreliable. This design is also generally accompanied with larger, more complex fuel storage, cleaning, and delivery subsystems.
Prime Power	<p>A prime power generator set is the primary (and potentially <i>only</i>) source of power to MCOs. A prime power generator is intended to run 24/7, but since it will generally supply power for an entire facility, the load it's supporting may fluctuate—so it needs to be an engine that can operate efficiently across a much broader range of demands.</p> <p>A subset of prime power generators would be those that only supply power to critical loads for MCOs. If the power distribution for the critical spaces is sufficiently separated from the rest of an MCO system, and the generator is running all the time to power the critical loads with some other backup system available, the system setup would fall under the prime power category.</p>

## Fuel Types

Traditionally, the prime mover for a generator set is an internal combustion engine. An internal combustion engine can run on a variety of fuel types, with diesel, fuel oil, gasoline, and natural gas being the most common engine fuels in use. However, there are some pros and cons to evaluate when considering what type of engine/fuel type is best for MCOs.

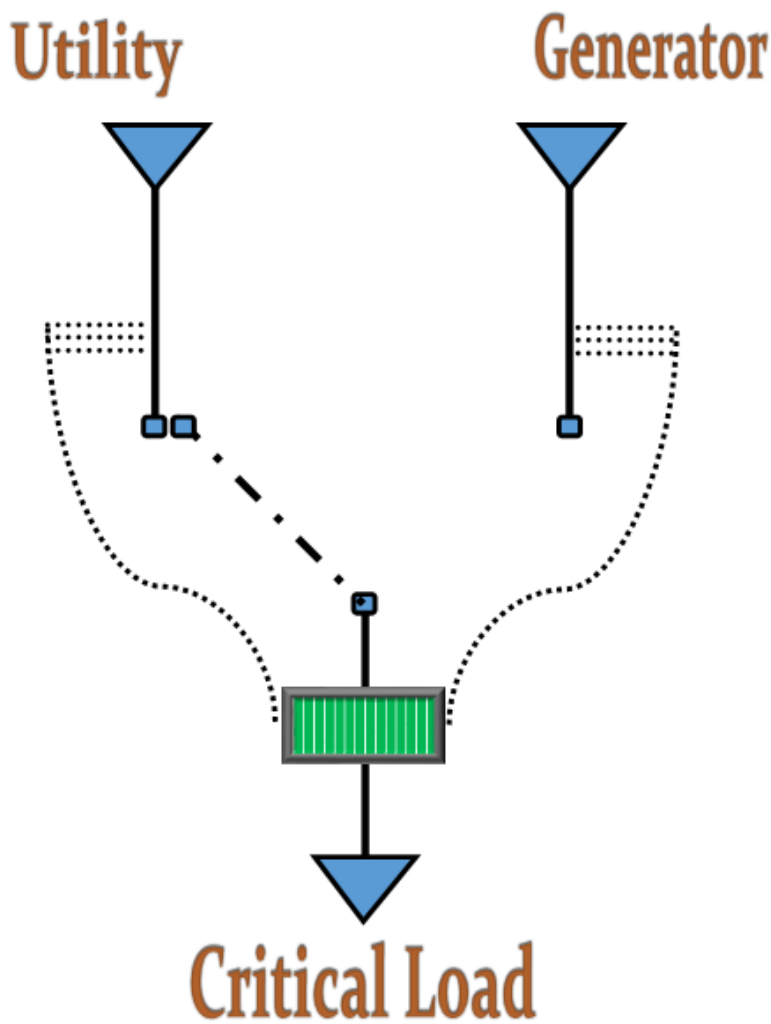
<b>Fuel Type</b>	<b>Description</b>	<b>Pros and Cons</b>
Diesel	The term "diesel fuel" is the commonly accepted shorthand for off-road diesel #2, a particular type of petroleum-based fuel that is not the same as the "highway use" diesel you might fill up your truck with. Diesel #2 is a particular grade of refinement that would not meet the emissions requirements for use on roadways in most states. It is also usually colored with a red dye to denote its off-road use. Utilizes the heat and pressure created by compression as its means of starting.	<p>Pros:</p> <ul style="list-style-type: none"> <li>• Most common and reliable engine type, and is therefore widely available.</li> </ul> <p>Cons:</p> <ul style="list-style-type: none"> <li>• Larger minimum engine size.</li> <li>• Concerns regarding emissions.</li> <li>• Potential issues with cold-starts.</li> </ul>

<b>Fuel Type</b>	<b>Description</b>	<b>Pros and Cons</b>
Fuel Oil	Fuel oil, otherwise known as heating oil or home heating oil, is very similar to diesel #2 without some additives to prevent gelling (the material breakdown of the fuel at low ambient temperatures) or control exhaust gasses. Utilizes the heat and pressure created by compression as its means of starting.	<p>Pros:</p> <ul style="list-style-type: none"> <li>• Same fuel used for heating, and is therefore widely available.</li> </ul> <p>Cons:</p> <ul style="list-style-type: none"> <li>• Less common engine type, and is therefore less widely available.</li> <li>• Potential issues with cold-starts.</li> </ul>
Gasoline	Gasoline generators have perhaps the widest range in acceptable fuel types/grades, much like you have a selection of octane ratings at the gas station for your car. The majority of gasoline refinement is geared towards on-road vehicle use, so most generator engines will utilize one of the commonly available grades. Utilizes the ignition of compressed air and fuel as its means of starting.	<p>Pros:</p> <ul style="list-style-type: none"> <li>• Flexibility in usable fuel grades.</li> <li>• Easier to start in cold weather.</li> </ul> <p>Cons:</p> <ul style="list-style-type: none"> <li>• Smaller generator size.</li> <li>• Concerns regarding fuel storage.</li> </ul>
Natural Gas	Natural Gas (NG) refers to a hydrocarbon gas mixture made up mostly of methane. NG generators are similar to gasoline engines in design, but with different combustion properties due to fuel differences. Liquid Propane (LP) is a variant of the natural gas engine, and some models have the flexibility to run on either fuel source due to their similarity. Utilizes the ignition of compressed air and fuel as its means of starting.	<p>Pros:</p> <ul style="list-style-type: none"> <li>• Available as a utility-supplied fuel, and is therefore widely available and reduces the need for fuel storage.</li> <li>• Easier to start in cold weather.</li> </ul> <p>Cons:</p> <ul style="list-style-type: none"> <li>• Smaller generator size.</li> </ul>

## Automatic Transfer Switches

An *automatic transfer switch (ATS)* is a particularly helpful component that acts as an independent traffic director of sorts, to ensure that power is being supplied from the most optimal source available. While ATSs exist in many places throughout MCO installations, ATSs at the main utility input are of unique importance since they perform a few extra duties.

Think of an ATS as a “Y” gate, with the top of the Y connecting to two different power sources; in this case, the utility-source and the generator. The bottom of the Y heads off to whatever load is being supported. The ATS has two main parts: a control panel and the switch. The control panel is always monitoring power quality signals from both sources and is programmed to have a primary and alternate source.



**Figure 2–11:** A diagram of an automatic transfer switch. (Source: *Logical Operations for NCMCO*)

In a very simplified view, the ATS will switch over from the primary source (the utility power) to the alternate source (the generator) when it senses a drop in voltage that is outside of the acceptable levels of tolerance frequency or other programmable parameters, and senses that the alternate source is providing a quality power signal. In many cases, the ATS is set to flip back to the primary source when it senses that the primary power has been restored to an acceptable quality for a specified period of time. This is often a feature that MCO technicians can override and force a manual transfer back to the primary source.

Additionally, some ATSs—especially those serving a generator output—can actually control the generator itself. In this scenario, upon a fault in the primary power supply, the ATS can send a start signal to the generator and wait for it to come online before transferring over.



**Note:** Some smaller, less complex variations of ATS design are often used throughout MCO facilities further down the power distribution path. For instance, an ATS may be tied to a redundant electrical lineup if certain sets of equipment need to be operated independently.

## Throw–Over Switches

A *throw-over switch*, or manual transfer switch, serves the same purpose as an ATS, but without the automatic control features. Some switches still have control panels that will provide an alert or alarm when conditions reach set thresholds, although they will require an operator to physically make the transfer.

## Paralleling Switchgear

*Paralleling switchgear* are large devices comprised of electrical disconnects, fuses, circuit breakers, and other electrical instruments used to transfer the electrical load from the utility-source to the generators (and vice versa) and then appropriately distribute the electrical power throughout the system. Specifically, they are used to switch the power source for the load, provide load sharing capabilities, operate the generator, meter the output, and protect the generator from any potential malfunctions.



**Figure 2–12: A paralleling switchgear in an MCO facility. (Source: P199/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Electrical\\_switchgear.JPG](https://commons.wikimedia.org/wiki/File:Electrical_switchgear.JPG))**

Paralleling switchgear is an especially vital component for MCOs with multiple backup generators, specifically because of its multiple moving parts. Think of it this way: generators are rotating machines, providing an AC output of a certain frequency, voltage, and waveform. Since it is constantly in flux—say, 60 Hz, or 60 cycles of the waveform every second—you can imagine how difficult it could be to match two "moving" AC sources from multiple power supplies. Closing the AC output from the generator to transfer it to the facility bus with AC power still running through it will have disastrous consequences if the two AC signals are not closely matched: most likely, an explosion!

Modern paralleling switchgear is controlled electronically by logic boards to remove the need for operators to be standing at the switchgear, manually closing the breakers. Until the generator output breaker has closed to support the MCO load, it is the variable source, and the control boards in the switchgear will usually make minor tweaks to the speed of the engine in order to align the AC waveforms.

## ACTIVITY 2-4

### Identifying Generator Types and Components

#### Scenario

In this activity, you will identify types of generators and the components that make up generator-set systems.

1. **Which type of generator typically has its engines off in its default state, waiting to become fully operational once a start command is run?**
  - Prime power
  - Stand-by
  - Continuous
  - Automatic
2. **Which type of generator runs all the time, but with a load that may fluctuate?**
  - Prime power
  - Stand-by
  - Continuous
  - Automatic
3. **Which type of generator runs all the time, with a relatively constant load?**
  - Prime power
  - Stand-by
  - Continuous
  - Automatic
4. **Which of the following MCO components is used to automatically shift between the primary and alternate power sources to maintain optimal power conditions?**
  - Throw-over switch
  - Paralleling switchgear
  - Double-pole switch
  - Automatic transfer switch
5. **Which of the following MCO components is used to transfer the electrical load from the utility-source to the generator (or from the generator to the utility-source) and distribute the power appropriately throughout the system?**
  - Throw-over switch
  - Paralleling switchgear
  - Double-pole switch
  - Automatic transfer switch

6. Which of the following MCO components is used to manually shift between the primary and alternate power sources to maintain optimal power conditions?
- Throw-over switch
  - Paralleling switchgear
  - Double-pole switch
  - Automatic transfer switch
-

# TOPIC D

## Uninterruptible Power Supplies

By now, you have a strong understanding of the two main types of power that can be provided to your MCOs: the consistent power supplied from the utility-source and the backup power supplied from a generator. These are likely the two sources you are most familiar with, just from day-to-day use; you may have even used a generator before to supply power to your own home. But, there is another source of backup power that is a commonly-used, critical component of any MCOs: an uninterruptible power supply.

As an MCO operator, it is imperative that you understand the purpose of an uninterruptible power supply and be able to choose between the different types that are available in order to best serve your MCOs. In this topic, you will identify the types of uninterruptible power supplies.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- UPS (uninterruptible power supply)
- Flywheel
- Line interactive UPS
- Double conversion UPS
- Delta conversion UPS
- Rotary UPS
- Diesel rotary UPS
- LBS (Load Bus Synchronization)

### UPS

An *uninterruptible power supply (UPS)* is a device or machine that provides immediate emergency power when the primary power source fails, using electrical energy stored within the device itself. UPSs are a critical component of an MCO power system because they are designed to provide clean and continuous power to MCOs during power interruptions and eliminate abnormal fluctuations from the power source as delivered.

Electricity delivered from the utility power source is never “clean power,” often experiencing spikes, sags, and occasional interruptions. These power abnormalities can wreak havoc on the IT load and other critical equipment serving MCOs and even severely damage them. UPSs protect these systems by providing temporary backup power for brief outages and absorbing those spikes and sags, ensuring the power delivered is within acceptable tolerances and specification for critical consumption. UPSs are not designed to sustain power supply for long periods of time, but rather long enough to engage another alternative source of power, such as a power generator, to accept the electrical load.

UPSs vary in design and method of application, but the basic function of a UPS follows the same principle. A UPS accepts AC power from the provided source, stores a portion of the energy in a backup battery system, and delivers the remaining to the critical connected equipment. In order to perform this vital function, the UPS requires three key components: a charger/rectifier, a battery or other storage mechanism (typically, a flywheel), and an inverter. The charger/rectifier converts the input AC power to DC power for battery charging, and the inverter converts the battery power to AC power during a power interruption.



**Figure 2–13: A UPS on server racks in a small-scale data center. (Source: Logical Operations for NCMCO)**

## Flywheels

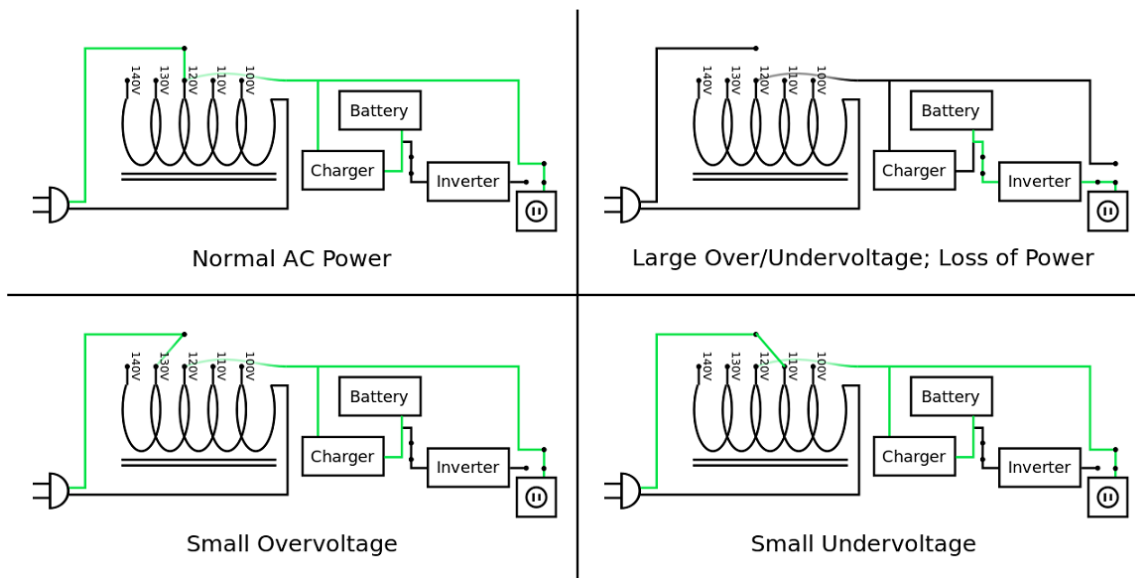
As an alternative to a battery system, flywheels can be used with a UPS to support continuous power requirements. A *flywheel* is a mechanical-type storage device that stores energy kinetically by rotating a mass around an axis. The electrical input spins the flywheel rotor up to speed where it remains fully charged in stand-by mode, 24/7, until a power interruption requires its activation. When this occurs, the flywheel provides back-up power immediately, while the system monitors for proper electrical input. If this condition persists for a specified time frame measured in seconds, the system transfers to a more permanent power source such as the backup generator system.

This technology is relatively cost-effective and environmentally friendly as opposed to the traditional lead acid battery system. Although the initial cost of batteries is relatively low, the cost of maintaining, replacing, and disposing of batteries over the long term must be taken into consideration. Flywheel technology can also work alongside a battery system if desired, and is highly effective at absorbing the abnormal electrical inputs as the first line of defense, thus prolonging the life of the storage batteries.

## Line Interactive UPS

A *line interactive UPS* combines the inverter and charger in the power supply line to supply both the AC power and the backup battery power and is capable of regulating its output voltage by utilizing a transformer or "buck-boost" circuit. This system limits transient voltages when switching and increases the speed of the changeover from main power to backup battery power. Because of this design, a line inverter UPS does not have to resort to batteries as often as other systems; instead, it utilizes some of its battery power only to support the transition from normal mode to voltage regulation mode.





**Figure 2-14:** A schematic of a line interactive UPS, showing how it operates (or doesn't operate) at various levels of voltage. (Source: Own work/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Line-Interactive\\_UPS\\_Diagram\\_SVG.svg](https://commons.wikimedia.org/wiki/File:Line-Interactive_UPS_Diagram_SVG.svg))

## Double Conversion UPS

A *double conversion UPS* converts all AC power to DC power, some of which is utilized for battery charging, while the rest is simply converted back to AC power to provide power to the critical load. The double conversion aims to prevent any possibility of an abnormal power event reaching the equipment downstream. Although the double conversion method is highly successful in providing continuous power from outages and power quality anomalies, it is also less efficient due to the power loss during the conversion process and the generation of additional heat, which creates a higher demand on the cooling systems.

## Delta Conversion UPS

The *delta conversion UPS* was designed to address some of the issues of a double conversion UPS, and therefore has a few similarities. Like the double conversion UPS, the inverter in a delta conversion UPS is always supplying the load voltage; however, it also uses a special transformer configuration to interface between the utility supplied power and the electrical load. A “delta” converter in the transformer regulates the input current and power and also delivers power to the inverter output. During normal conditions, the delta converter allows the UPS to deliver power to the load with greater efficiency than that of the double conversion UPS.

## Rotary UPS

In a *rotary UPS*, a motor generator or some variation of rotating components are utilized to transfer power to the load via rotating generation. Whenever power is supplied within an acceptable range of frequency and voltage, the motor mechanism is driven directly from the utility power source as delivered, and therefore also supports the critical load. At this point the rectifier/inverter remain in a stand-by mode while acceptable power is monitored.

If and when the supplied utility power parameters fall outside of specifications, the rectifier/inverter begin to supply power to the motor and thus to the generator portion of the UPS to support the load. The energy stored in the stand-by batteries provide sufficient power momentarily until an alternate source, such as stand-by generators, can come up to speed and incur the electrical load.

## Diesel Rotary UPS

A *diesel rotary UPS* combines a battery-powered or flywheel-powered UPS with a diesel generator to supply backup power for the load. It actually consists of five key components: a motor generator, flywheel, choke, mechanical clutch, and a diesel engine.

Under normal and uninterrupted conditions, the local utility power is fed to the critical equipment load via the choke and motor sub-system, otherwise known as the filter. This same source of power also feeds the flywheel to retain kinetic energy storage capability in the event of a power interruption. When utility supplied power is interrupted, alternate power is supplied by the rotating flywheel to the motor generator unit, which provides adequate power for a few seconds until the diesel engine can start and accelerate to full speed. At this point the clutch is engaged, enabling mechanical power to be supplied to the motor generator to sustain continuous electricity to the critical load.

In most cases, diesel rotary UPSs are a fixed asset and are rarely modular. Future growth relating to power requirements must be considered upon the initial engineering calculations to ensure capabilities are somewhat oversized. Since these are diesel powered, special ventilation and purging equipment for fumes may be required, as well as potentially constructing a separate building or enclosures to support these systems.

## Load Bus Synchronization

*Load Bus Synchronization (LBS)* is an engineering method to keep the output of two independent UPSs in sync, even if they are operating from two different sources of supplied power. In general, a UPS in a multiple-UPS system will automatically sync to its own bypass source, as long as all of the UPSs are tied to the same input source. However, imagine if these UPSs were operating off of different back-up generators, batteries, or another bypass source. In these scenarios, their outputs will always tend to drift out of sync and cause problems within the electrical load.

The LBS system functions by continuously monitoring the sync reference signals of two UPS modules. It remains in a dormant state until the output of the UPS modules drift out of predetermined operational parameters—or out of sync—at which point the LBS activates and manipulates the output of each UPS module until they once again fall in sync with each other. Once completed, the LBS once again returns to its dormant state of operation.

# ACTIVITY 2–5

## Identifying UPS Types

### Scenario

In this activity, you will identify the various types of uninterruptible power supplies (UPSs).

1. **Load Bus Synchronization is an engineering method that aims to maintain which of the following conditions within the power system of your MCOs?**
  - Keep the output of two independent UPSs operating from a single power source in sync.
  - Keep the input of two independent UPSs in sync in order to maintain a stable output.
  - Keep the output of two independent UPSs operating from multiple power sources in sync.
  - Keep the input of two independent UPSs outputting to two separate locations in sync.
2. **Which type of uninterruptible power supply uses some sort of spinning components to transfer power to the load?**
  - Line interactive UPS
  - Delta conversion UPS
  - Diesel rotary UPS
  - Rotary UPS
  - Double conversion UPS
3. **Which type of uninterruptible power supply converts all the AC power to DC power, and then stores some of it as battery charge and converts the rest back to AC power to carry the power load?**
  - Line interactive UPS
  - Delta conversion UPS
  - Diesel rotary UPS
  - Rotary UPS
  - Double conversion UPS
4. **Which type of uninterruptible power supply combines an inverter and charger in the power supply line to supply both the AC power and the backup battery power, and regulates its output voltage using a transformer?**
  - Line interactive UPS
  - Delta conversion UPS
  - Diesel rotary UPS
  - Rotary UPS
  - Double conversion UPS

5. Which type of uninterruptible power supply uses an inverter in the supply line to provide power for the load and a converter in the transformer to regulate the input and deliver power to the inverter output?
- Line interactive UPS
  - Delta conversion UPS
  - Diesel rotary UPS
  - Rotary UPS
  - Double conversion UPS
6. Which type of uninterruptible power supply uses rotating components to produce immediate emergency power while an engine starts up to maintain the backup power to the critical load?
- Line interactive UPS
  - Delta conversion UPS
  - Diesel rotary UPS
  - Rotary UPS
  - Double conversion UPS
7. Why is an uninterruptible power supply a critical component of an MCO power system?
- The electrical equipment used in MCO design and construction is notoriously flaky, and there needs to be a reliable source of emergency power when it inevitably stops working properly.
  - Electricity from the utility-source is not strong enough, and extra power is needed to help "boost" the voltage to a level strong enough to support the critical load.
  - Electricity from the utility-source is riddled with potential disruptions that need to be mitigated with backup devices to ensure that power is always supplied to the critical load.
  - The electrical equipment used in MCO design and construction uses various voltages, and some sort of device is needed to break up and distribute power to the various critical components.
-

# TOPIC E

## Batteries

So far, the sources of power you have learned about are typically used on a larger scale, providing power to a whole system or the large components within it. When it comes to providing power to smaller devices or equipment (or, sometimes, even a secondary source of power), batteries are a familiar and typical solution; however, not all batteries are best suited for use in an MCO environment.

As an MCO operator, you will need to be able to differentiate between the different types of batteries and select the one that is best for your particular MCOs' needs. In this topic, you will identify types of battery systems and their characteristics.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Battery
- Battery system
- Primary battery
- Secondary battery
- Lead acid battery
- Lithium-ion battery
- Nickel cadmium battery

## Battery Systems

A *battery* is a device that converts stored chemical energy into electricity via a process in which free electrons move between a positively charged terminal (called a cathode) and a negatively charged terminal (called an anode) through a solution favorable to this process (called the electrolyte). All of these things together, within a container, is called a jar or cell (although some battery designs include multiple sets of terminals such that one jar may have several cells within it). There are numerous types of batteries which are differentiated based on the materials used for the cathode, anode, and the electrolyte (as well as a few other secondary variables).

A *battery system* is simply a set, or sets, of individual battery cells wired together in strings in order to achieve higher voltages, capacities, or redundancies.



**Note:** A quick refresher on basic DC power laws: when connected in a series, current remains constant while voltages are accumulative (think of the cells in a string); when connected in parallel, voltage remains constant but current is accumulative (think of multiple strings in a system).

Important MCO battery systems include:

- UPS battery strings
- Switchgear batteries
- Control panels
- Fire system panels/detectors

For much of history, the type of batteries that were being used were what would be considered *primary batteries*, meaning they were really only useful for one full discharge before having to be scrapped or have at least one component replaced. With the advent of rechargeable, or *secondary batteries*, a charge could be applied to the battery which would convert the electricity back to chemical energy to store for future use. In MCOs, only the latter type of battery system is typically used, and therefore these types of batteries will be focused on here.

## Lead Acid Batteries

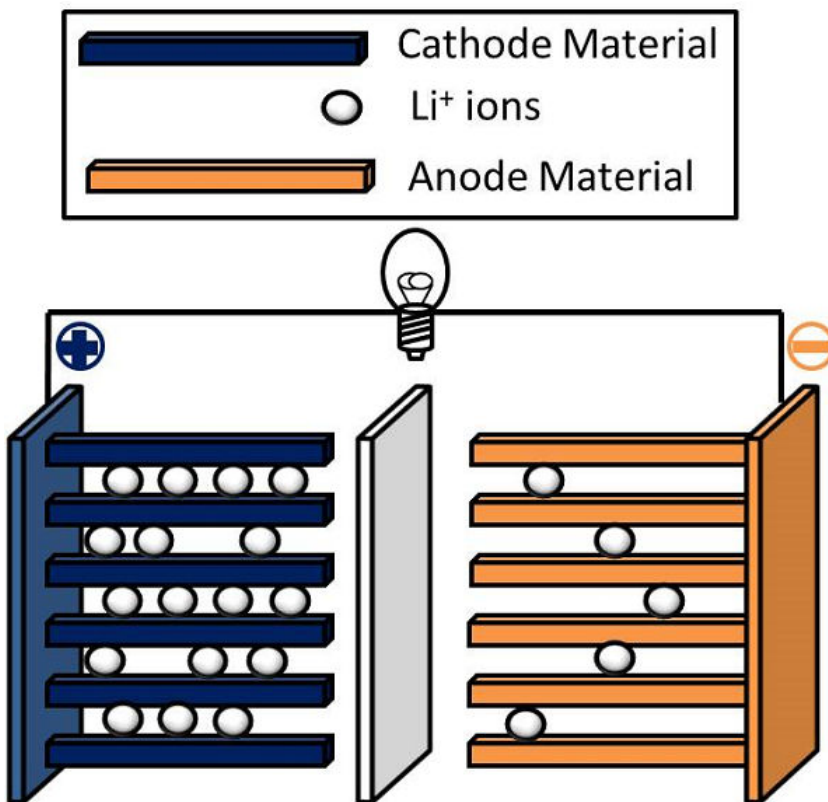
Lead acid batteries are widely prevalent and come in many options available for commercial/ industrial scale usage in MCOs. In a *lead acid battery*, the positive terminal is made of lead-oxide ( $\text{PbO}_2$ ), the negative terminal is made of lead ( $\text{Pb}$ ), and the electrolyte solution that fills the container is some concentration of sulfuric-acid ( $\text{H}_2\text{SO}_4$ ). The chemical reaction amongst the three components produces the voltage for the battery.

Flooded wet cell batteries are the original form of lead acid batteries and simply have the cathode and anode fully submerged in the electrolyte solution. The top of the battery is covered, with the terminals protruding for connection, and two ports: a vent and a fill port. As part of the chemical reaction releasing and storing energy in the battery, the acid (in this case,  $\text{H}_2\text{SO}_4$ ) and some water ( $\text{H}_2\text{O}$ ) molecules are broken apart, releasing hydrogen ( $\text{H}_2$ ) and oxygen ( $\text{O}_2$ ) gasses. This gas needs to be vented in order to prevent over-pressurization of the battery, hence the need for the vent. Some of the solution can also evaporate over time, so to maintain the cathode and anode fully submerged, de-ionized water may need to be added to the jar from time to time.

Valve Regulated Lead Acid batteries (VRLA) are an advancement of lead-acid battery technology and have been in wide use for decades now. This battery design utilizes a specialized one-way pressure release valve, only releasing gasses when pressure is actually beginning to rise to certain levels (whereas the flooded wet cell tends to release most all gas produced). By forcing the gasses to stay within the jar, they become re-absorbed by the solution, attach to the cathode and/or anode, and through ionic exchange reactions, form water again. This is a process commonly referred to as recombinant technology and delivers two main benefits: increased safety protection from over-pressurization and/or dangerous gas release, as well as virtually eliminating the need to ever refill a jar.

## Lithium-Ion Batteries

Lithium-ion batteries are relative newcomers to the world of battery technologies, bringing many benefits along with them. In a *lithium-ion battery*, the cathode is a lithium oxide material, the anode is typically a carbon-based material, and the electrolyte is a liquid consisting of lithium salts and an organic solvent. The basic operation is still the same: a chemical reaction causes ion exchange with is then converted, stored, and used as electricity. In this case, positively charged lithium ions ( $\text{Li}^+$ ) are shared back and forth between the two terminals, creating the voltage for the battery.



**Figure 2–15:** A schematic of a lithium-ion battery. (Source: Materialsgrp/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Schematic\\_of\\_a\\_Li-ion\\_battery.jpg](https://commons.wikimedia.org/wiki/File:Schematic_of_a_Li-ion_battery.jpg))

There are certainly many advantages to using lithium-ion batteries, including the higher voltages that can be produced, a more compact design, a longer lifespan and recharging efficiency, and little to no maintenance; however, they also have their disadvantages, including high temperature concerns and more expensive production.

## Nickel Cadmium Batteries

Nickel Cadmium (NiCd or NiCad) batteries are another style of popular modern batteries. In a *nickel cadmium battery*, the cathode is a cadmium material, the anode is a nickel oxide material, and the electrolyte is an alkaline. Principles of operation remain the same as other types of batteries, although in this case it is the chemical reaction between the two terminals that creates the voltage for the battery. NiCd batteries tend to be smaller—generally, between the scale of lithium-ion batteries and other lead acid batteries—but do not have the higher voltage characteristics of lithium-ion. They are, however, extremely robust and durable, having both impressive recharge lifetimes and the ability to handle a wide range of electrical activity. Typically, in MCOs, NiCd batteries will be used to operate switchgear or machinery but not to the scale of full-system (i.e., UPS) support.

# ACTIVITY 2–6

## Identifying Battery Types

### Scenario

In this activity, you will identify batteries and the different types of secondary batteries suited for use in MCOs.

---

1. **What is the difference between a primary and secondary battery?**
    - A primary battery is the main source of power, while a secondary battery acts as the backup.
    - A primary battery uses the utility-source power, while a secondary battery uses backup-generated power.
    - A primary battery can only be used once, while a secondary battery can be recharged.
    - A primary battery is discharged first in the power supply, while a secondary is discharged second, after the primary has been used.
  2. **Which type of battery system is typically used in MCOs?**
    - Backup battery
    - Reserve battery
    - Primary battery
    - Secondary battery
  3. **Which type of battery uses a chemical reaction between the cathode, anode, and electrolyte solution to create an electrical charge?**
    - Lead acid battery
    - Lithium-ion battery
    - Nickel cadmium battery
  4. **Which type of battery uses a chemical reaction between just the cathode and the anode to create an electrical charge?**
    - Lead acid battery
    - Lithium-ion battery
    - Nickel cadmium battery
  5. **Which type of battery uses an exchange of ions between the cathode and anode to create an electrical charge?**
    - Lead acid battery
    - Lithium-ion battery
    - Nickel cadmium battery
-



# TOPIC F

## Alternative Power Sources

Most of the power sources you are familiar with are the more traditional types, such as utility-supplied or battery-supplied. These days, there are more alternative energy sources available as we look to find clean, renewable options for power. As the technology improves, these alternative power sources are becoming more available and prevalent in both residential and commercial implementations—including MCOs.

As an MCO operator, it will benefit you to be aware of these alternative power sources and be prepared to potentially interact with them in an MCO facility. In this topic, you will identify alternative sources of power.

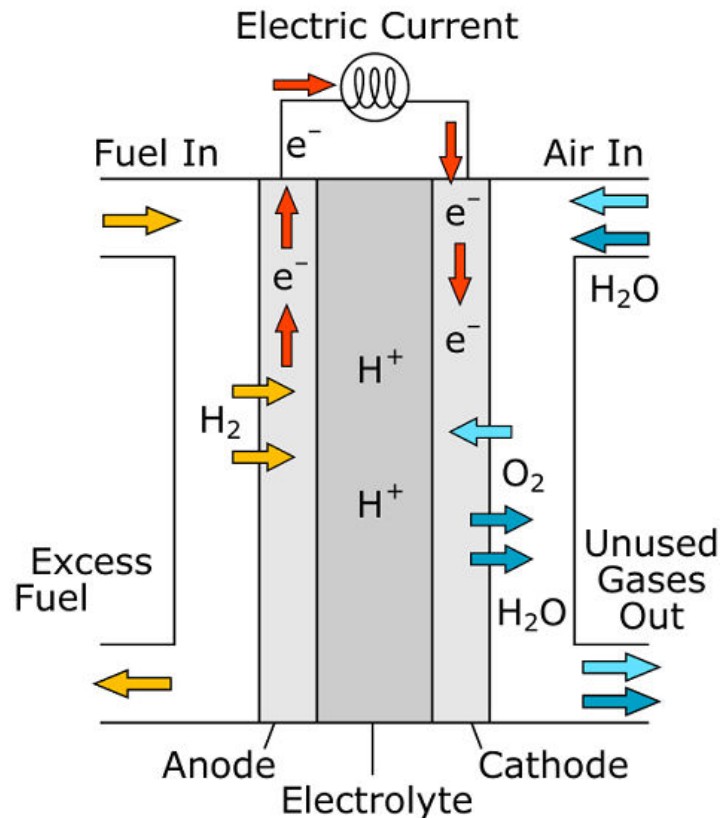
The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Fuel cell
- Biomass
- Capacitor
- Capacitance
- Supercapacitor
- Co-generated power
- Geothermal power

## Fuel Cells

A *fuel cell* converts stored chemical energy into electricity using a chemical reaction between positively charged ions and an oxidizing agent. Like batteries, they are made up of three segments: the anode, the cathode, and the electrolyte; unlike batteries, however, fuel cells require a continuous source of fuel and air to operate. In a fuel cell, the chemical reaction occurs where the three segments interface, such that the fuel is consumed, water or other gases are created as a waste product, and an electric current is produced. As long as the sources are supplied, the fuel cell will continue to produce electrical energy.

The most common and familiar type of fuel cell is likely the hydrogen fuel cell, which requires hydrogen ( $H_2$ ) fuel and air ( $O_2$ ) as the sources. During the chemical reaction at the segments, some  $O_2$  molecules are stripped from the air and some are stripped from the water ( $H_2O$ ) molecules, leaving more  $H_2$  to act as fuel. In the end, the remaining broken-apart, ionized hydrogen ( $H^+$ ) and oxygen molecules re-combine to form water as the waste product (which is, unfortunately, non-potable).



**Figure 2-16:** A schematic of a hydrogen fuel cell shows how energy is created from the chemical reactions between hydrogen and oxygen. (Source: R.Dervisoglu/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Solid\\_oxide\\_fuel\\_cell\\_protonic.svg](https://commons.wikimedia.org/wiki/File:Solid_oxide_fuel_cell_protonic.svg))

Fuel cells have been making inroads in several industries—notably, transportation and propulsion, in addition to power generation—due to their capability to make renewable, mostly clean energy (wastewater being the one downfall). For large-scale implementations, fuel cells can be an expensive capital investment but have relatively low cost of operation. Power density is approaching that of traditional diesel/gas generators, so MCOs of any size would still require a small array of fuel cells, but they can provide continuous power more indefinitely than generators.

## Solar Power

One of the cleanest alternative energy sources available is right above you: the sun. To understand the potential alternative energy source that is solar power, consider this: on average, the Earth receives enough solar radiation each day to equal about seven times the amount of total global consumption. The photovoltaic (PV) cells on solar panels can capture the sun's energy and provide a clean, renewable source of electric power and yet—unfortunately—current commercially available solar panels are only about 20% efficient, making it a widely available but underutilized source of energy.



**Figure 2–17: Long rows of solar panels on a solar farm in Sharon, Vermont. (Source: SayCheeeeeese/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:SunGen\\_Sharon\\_Solar\\_7.jpg](https://commons.wikimedia.org/wiki/File:SunGen_Sharon_Solar_7.jpg))**

Aside from the lack of efficiency, the current limiting factor for solar power production and usage is real estate. Panels simply take up a lot of linear space, so their viability as an alternative energy source depends largely upon how deep the owner or developer's pockets are. Whether you are deciding between implementing solar panels as input to a local grid or as onsite supplemental power, the decision factors are largely the same. PV manufacturing technology has improved sufficiently enough in the last decade that construction and labor costs are the major variables that may provide economies of scale; the PV cells/panels themselves have become quite affordable in relation to the overall investment.

However, much like microprocessors changed the face of electronics and computing, the next breakthrough in solar technology will certainly bring it to the forefront of most power planning discussions. If solar technology can reach a point where it is capable of generating two to four times the amount of power on the same amount of land (or the same power in a fraction of the footprint), solar power could rival hydroelectric power as a leader in renewable energy production. For MCOs in particular, it is important to keep in mind that—even without a solution to grid-scale power storage limitations—creating solar power is nearly free (minus the initial capital investment) to generate during daylight hours when strains on the utility grid and electricity prices are highest.

## Wind Power

Wind power also ranks very highly as a clean, sustainable alternative energy source. Wind turbines are simply large fans that convert the mechanical energy of the wind to electricity by turning the rotor of a standard generator. These are highly efficient machines as virtually the only source of energy loss is overcoming friction in turning the rotor.



**Figure 2–18: Wind turbines on a wind farm in Idaho. In 2011, wind power generated 8% of the state's total electricity. (Source: Executive Office of the President of the United States/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Power\\_County\\_Wind\\_Farm\\_002.jpg](https://commons.wikimedia.org/wiki/File:Power_County_Wind_Farm_002.jpg))**

Although not nearly as predictable as solar availability, wind power suffers the same fate in widespread adoption because it is not constant. Wind is always changing (or sometimes not blowing at all) which makes it difficult to rely upon to provide a given amount of power. However, there have been a few recent advancements to combat some of these reliability concerns, including turbines that track the direction of the wind and automatically adjust to face it and variable gears in the generator that produce different levels of power based on the current wind speeds.

Wind does have a leg up on solar in that it mostly requires vertical real estate, so installation location possibilities have a much wider range. Some utility-scale wind farms have many thousands of wind turbines installed across vast acreage...even at sea! When it comes to using wind power for your MCOs, it is easy enough to install a few turbines onsite to provide supplemental power to a facility.

## Biomass

*Biomass* is a broad term encompassing virtually all renewable, organic materials—from old wood pallets, to discarded crops, to “municipal waste” as the dictionary gently puts it—that can be treated in some manner (shredded, compressed, composted, etc.) and burned for fuel. Then, just like most other power plants, the heat is generally used to drive steam or gas turbines to create electricity. In short: is it related to paper, plants, or poo? Then, it is probably a biomass fuel source.

While the by-products of biomass are not quite as bad as coal or other fossil fuel plants, burning is still burning; in this regard, biomass should be considered a cleaner alternative energy than some of the others, speaking strictly from the energy production process. However, if you take into account the fact that much of the biomass fuel sources are often headed for landfills, or require additional energy to recycle or treat, removing these items from the waste chain does actually have a notably positive effect on the environment.

Currently, the largest hurdle for biomass power plants is the fuel supply chain. There is certainly no shortage of fuel products, but industries have not been fully established to process these sources in a manner desirable for a particular plant design. Plant designs can be easily modified for any primary source, or combination of fuels, but once it's built, it's committed. While many large-scale biomass power plants also process their own fuel onsite, it is simply not practical to build processing capabilities for all types of biomass sources; as a result, most biomass plants usually stick to producing the one or two sources that are the most heavily used in the serviceable area.



**Figure 2–19: The biomass plant at the Savannah River Site in South Carolina burns forest residue to provide power to the rest of the campus, which produces nuclear materials for the U.S. Department of Energy. (Source: United States Department of Energy/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Biomass\\_being\\_processed\\_at\\_the\\_Savannah\\_River\\_Site\\_\(7609895484\).jpg](https://commons.wikimedia.org/wiki/File:Biomass_being_processed_at_the_Savannah_River_Site_(7609895484).jpg))**

## Supercapacitors

*Capacitors*, specifically electrochemical capacitors, are another category of energy storage devices, typically used on smaller scales than batteries. They can store very small amounts of electric potential. For example, think about the minuscule amount of charge it takes for an electronic device to keep track of time. The battery on your phone may have died, or your computer may have been unplugged for weeks, and yet when you connect to a primary power source and boot it up; it still knows what time it is. *Capacitance*—the ability to store some amount of charge—is measured in a unit called the farad (named for the acclaimed 19th century English scientist Michael Faraday).

*Supercapacitors* are capacitors on a much grander scale, with capacitance on the order of tens of thousands of farads and the ability to charge or discharge all of their energy very quickly. While current technology has provided these higher capacitances, physical construction limitations cause supercapacitors to be many times larger than a battery for a given charge.

Supercapacitors won't become a replacement for primary or backup power anytime soon, but there are still many advantages in this design. Most commonly, you might run into capacitors as part of the mechanical equipment of your MCOs. Since most motors require a rather large amount of power—many times higher than running power—to start, capacitors can act as a buffer to minimize

the surge in demand on connected power distribution systems, or mitigate an extreme drain on batteries if the motor ends up starting on backup power.

## Co-Generated Power

In a *co-generated power* system, some fuel source (nuclear, coal, gas, biomass, etc.) is used to create steam for turbine generators, and then the leftover heat is extracted from the exhausted waste steam (or condensate) and is used to provide power for other central services (such as space heating or water heating). Co-generation plants are an economical, if not thrifty, alternative power source that is primarily found in campus settings because of the ability to utilize the co-generated energy to power a central service for multiple buildings on the site, if not the entire campus.

While it is still not common for most MCO facilities to be generating their own primary power onsite (with a few large-scale exceptions), the co-generation concept is one that MCO technicians and operators are finding great success in implementing after the fact. Anything that generates heat can be considered a candidate for co-generation. For instance, a communications center that finally decides to install a solar array on the roof could then install a bypass loop to its hot water heater and run tubes within or behind the array to collect its heat. Or machinery with compressors or motors in a manufacturing plant could be hooded in some manner, and ductwork could be put in place to pump the hot air back into people spaces during colder months to augment installed electric heaters.

## Geothermal Power

*Geothermal power* uses the natural thermal energy—in short, heat—generated and stored in the earth to act as either a nascent heat source or a power source. Geothermal power is a dual-faceted alternative energy source: these underground heat sources can either be utilized directly in heat exchangers that create hot air or hot water (mostly for comfort uses, like office areas) or provide the supply power to heat engines that in turn generate moderate amounts of electricity.



**Note:** Heat engines are systems that convert heat energy into mechanical energy, taking on many forms, but rely upon complex thermodynamic principles that are necessarily pertinent to the fundamentals of MCOs.



*Figure 2–20: Steam rises from the stacks of a geothermal power plant in Iceland. (Source: Gretar Ivarsson/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:NesjavellirPowerPlant\\_edit2.jpg](https://commons.wikimedia.org/wiki/File:NesjavellirPowerPlant_edit2.jpg))*

# ACTIVITY 2–7

## Identifying Alternative Power Sources

### Scenario

In this activity, you will identify the various types of alternative power sources.

---

- 1. Which type of alternative power source converts stored chemical energy into electricity using a chemical reaction between positively charged ions and an oxidizing agent?**
  - Biomass
  - Supercapacitor
  - Fuel cell
  - Co-generated
- 2. Which type of alternative power source uses a typical fuel source to create steam for turbine generators and extracts the leftover heat from the exhausted waste steam to provide power for heat or hot water services?**
  - Supercapacitor
  - Co-generated
  - Geothermal
  - Fuel cell
- 3. Which type of alternative power source uses the heat derived from burning treated organic materials to drive steam or gas turbines in order to create electricity?**
  - Biomass
  - Supercapacitor
  - Wind
  - Fuel cell
- 4. Which type of alternative power source uses the heat generated by the earth to warm air or water, or power heat engines that generate moderate amounts of electricity?**
  - Supercapacitor
  - Solar
  - Co-generated
  - Geothermal
- 5. Which type of alternative power source uses an energy storage device that always maintains a large amount of stand-by charge to minimize surges in demand on the power distribution system or mitigate the drain on backup battery power?**
  - Co-generated
  - Supercapacitor
  - Fuel cell
  - Biomass



6. Which type of alternative power source uses large fans called turbines, rotated by the force of moving air, to turn the rotor of a standard generator and produce electricity?

- Wind
- Solar
- Co-generated
- Biomass

7. Which type of alternative power source uses photovoltaic cells to capture the radiation energy from the sun and convert it into electricity?

- Geothermal
  - Supercapacitor
  - Solar
  - Biomass
-

## Summary

In this lesson, you identified and described the fundamental concepts of power and the power sources that are relevant to Mission Critical Operations. Having a strong understanding of what power is, how power works, and what sources of power are available and best suited to your MCOs will help ensure that you are a successful MCO operator.

# 3

# Mission Critical Infrastructure: Power Distribution

## Lesson Objectives

In this lesson, you will identify and describe power distribution as it pertains to Mission Critical Operations. You will:

- Compare and contrast medium and low voltage systems for power distribution.
- Identify redundancy levels.
- Identify the elements of power supply transfer.
- Identify power distribution topologies.
- Identify and apply electrical protection techniques.
- Identify preventative maintenance procedures for power distribution components.

## Lesson Introduction

From the simple components—like the lights and heat in its people spaces—to the more complex, critical components—like the cooling equipment in a data center—nearly every component within an MCO facility relies on a steady source of power or is directly affected by one that does. For this reason, supplying and managing electricity to all critical equipment is the primary focus of Mission Critical Operations (MCOs).

As a Mission Critical Operator, you will need to have a strong understanding of the fundamental concepts of power distribution and the various components that are involved in distributing power throughout your MCO facility. In this lesson, you will identify and describe power distribution as it pertains to Mission Critical Operations.

# TOPIC A

## Medium vs. Low Voltage Systems

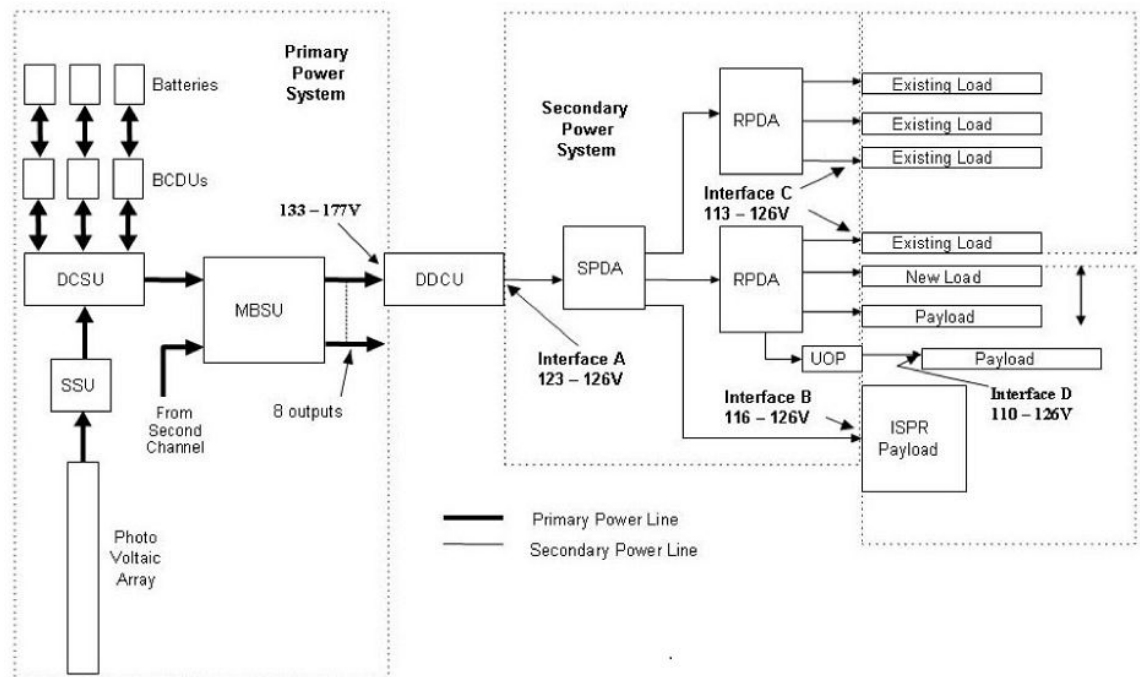
As you already know, there are different voltage levels at which a power system can operate. But how do you know which is the right system for your MCOs? As an Mission Critical Operator, you will need to be able to understand the basic concepts of power distribution, differentiate between the types of voltage systems available to distribute power, and choose the one that best applies to your own MCO facility's needs. In this topic, you will compare and contrast medium and low voltage systems for power distribution.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Power distribution
- PDU (power distribution unit)
- Efficiency

## Power Distribution

*Power distribution* is the set of electrical transmission systems that receive power from a primary source—either externally from the utility or internally from generators—and then divide it up, pass it through any protective features, and deliver it to the connected equipment load. In a Mission Critical Infrastructure, power is generally supplied via the local utility substation to the facility at a predetermined and fixed voltage. From there, the power must be harnessed, distributed, and stepped down to various voltages suitable for the customer's critical load, and that's where the various components of the power distribution come in—components including uninterruptible power supplies (UPSs), substations, power distribution units (PDUs), electrical switchgear, transformers, circuit breakers, power supply cables, and other equipment that you'll learn more about.



**Figure 3-1: A schematic of power distribution for a site. (Source: NASA/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Electrical\\_Power\\_Distribution.png](https://commons.wikimedia.org/wiki/File:Electrical_Power_Distribution.png))**

## PDU

A *power distribution unit (PDU)* is a piece of electrical equipment consisting of multiple outputs—typically in the form of outlets—designed to distribute electrical power to multiple devices. Generally a PDU in an A/C circuit is engineered with a power transformer to step down 480VAC to 120/208VAC to provide conditioned power from a centralized UPS or generator to racks and computers of network equipment. A PDU may have the capability to accommodate power supply to multiple equipment racks or server cabinets. PDUs vary in design and use, and may be as simple as inexpensive rack-mounted power strips to much larger and expensive floor-mounted machines with complex functions.



**Figure 3–2:** A cabinet PDU, shown with its door open, is designed to support a much larger-scale power distribution system. (Source: Robert.Harker/Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:UPS\\_PDU\\_Open.jpg](https://commons.wikimedia.org/wiki/File:UPS_PDU_Open.jpg))

## Low Voltage Systems

In the context of critical environments, specifically in the United States, low voltage electrical systems are generally categorized as those systems operating at voltages up to 1000 volts (or 1kV). Power coming from the utility-source is delivered at a much higher voltage (typically closer to that of a medium voltage system) so it must be stepped down to low voltage, which can be done via a three phase transformer in the low voltage system. The low voltage bus (a device in the power system that evaluates the voltage, current, or flow of energy within the system) then distributes this stepped down electrical power to the various loads in the facility, such as IT equipment loads, PDU converters, lighting, and cooling systems.



**Note:** Attempting to define low voltage, medium voltage, and high voltage can be tricky because these levels vary depending on specific application guidelines, the context of the application, and sometimes even the electrical parameters that have been determined by the authority having jurisdiction.

## Medium Voltage Systems

In the context of MCO systems, medium voltage electrical systems are generally defined as those operating between 1000 volts (1kV) to 36kV. In large critical environments, which typically have over 1 megawatt (or 1,000 kilowatts) of loads, medium voltage switchgear may be utilized. Medium voltage distribution can minimize electrical losses, since a higher voltage decreases the current that is required for the same power level requirements. In very large critical environments, this can be of a significant value by reducing the amount of low voltage equipment and increasing potential valuable floor space. Additionally, many design options are possible to include enabling the UPS to perform at medium voltage, thus distributing medium voltage to individual areas of the facility.



**Note:** It is important to recognize that the terms "low voltage" and "medium voltage" can mean different things based upon the context in which they are being used. In previous lessons, "low voltage" and "medium voltage" and their typical voltage levels were introduced in reference to the types of equipment that plug into power sources. In this context, the voltages of each system are slightly different than in previous usage, because they are being used in reference to the voltage levels for the power distribution system, which operates at much higher voltage levels.

## Multiple-Source and Multiple-Feed Power

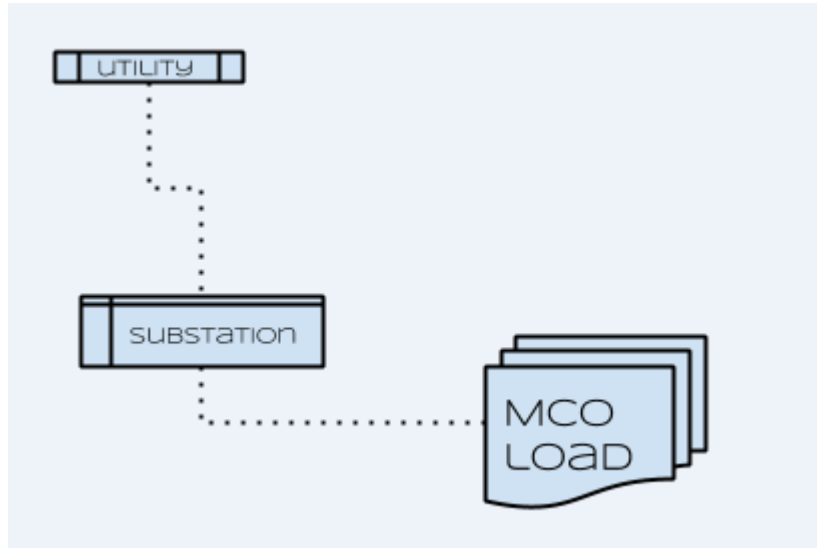
In the ideal situation, the critical facility will be fed from multiple power sources—maybe even more than one power plant. Additionally, the substations, switches, transformers and UPSs within a specific system will influence how electrical power is transferred to and throughout the facility. Dependent upon the design, quantity, placement, and redundancy capabilities of each will define the true meaning of multiple-source or multiple-feed power.



**Note:** Redundancy refers to the "extra" components of a system that are typically used solely for backup during critical times, like an outage or failure. It will be covered in greater detail in the next topic.

There are four types of multiple-source/multiple-feed power configurations, each with their own distinguishing characteristics.

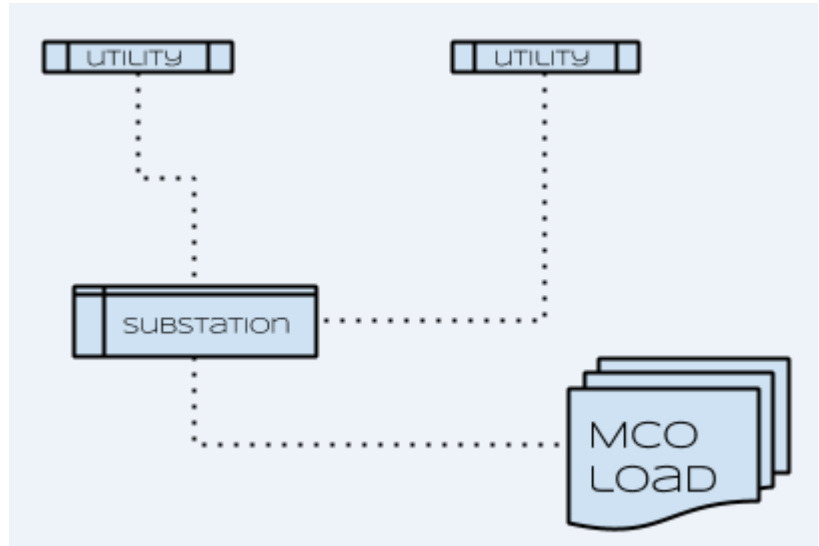
<b>Configuration</b>	<b>Description</b>
Single feed/single substation	In this configuration, a facility is supported by one substation with a single power line and a single input feed to the utility transformer(s).



(Source: Logical Operations for NCMCO)

Facilities that are supplied power in this manner can be vulnerable to a high risk of failure and critical operations interruption. While it might be supported by multiple transformers (giving it the appearance of backup redundancy), if this single substation and single feed failed to provide power, all equipment downstream would fail as well.

Configuration	Description
Multiple feed/single substation	In this configuration, there is a single power line with a manual or automatic throw-over switch from the one substation and a single input feed to the utility transformer(s). The throw-over switch will manually or automatically transfer to the second feed if power is interrupted from the main feed.

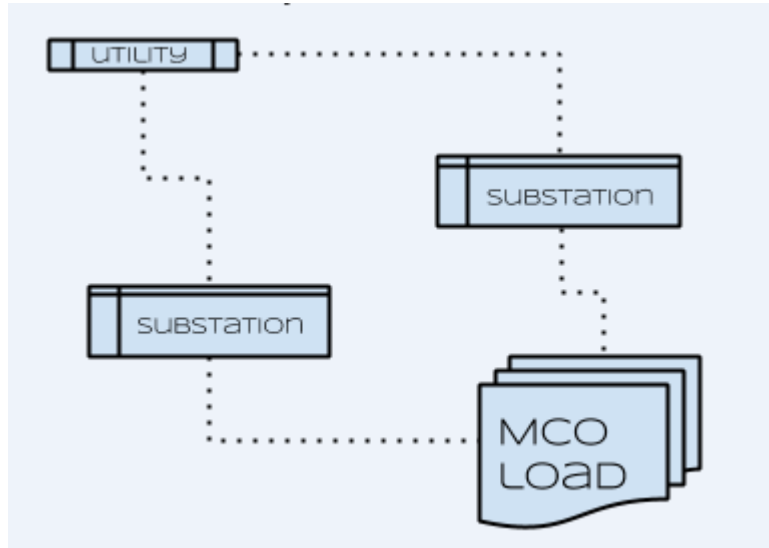


(Source: Logical Operations for NCMCO)

Facilities supported by a single substation with a multiple feed from that substation are at a somewhat reduced risk of failure when compared to a single feed and single substation; however, this configuration still poses a significant failure risk as the facility is relying on one substation for power supply.



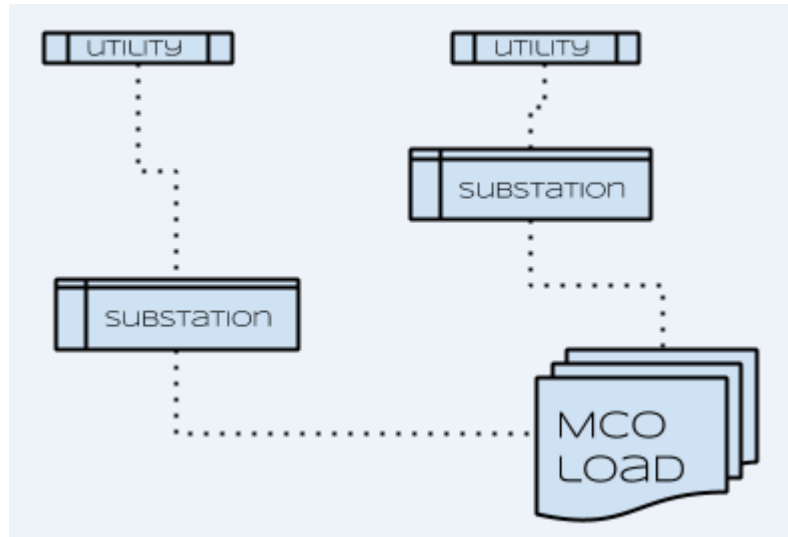
Configuration	Description
Multiple substation	In this configuration, there are two power lines (one from each substation), single input feeds to each transformer, and one throw-over switch connecting the two substation outputs. Upon a substation failure, the throw-over switch will manually or automatically transfer to connect to the other substation.



(Source: Logical Operations for NCMCO)

Facilities supported by multiple substations gain the advantage of increased redundancy with limited single point failure opportunities. In this case, the throw-over switch is the most prominent single failure source. Failing to transfer after a substation power interruption will create the necessity for the facility to rotate to an alternative source of electrical generation to maintain the critical load.

Configuration	Description
True dual/multiple feed	In this configuration, the facility is supported by two separate substations with a single and independent feed from each to the transformer(s). There isn't a need for a throw-over switch, as dual inputs are fed directly into each transformer located within the facility.



(Source: Logical Operations for NCMCO)

Facilities supported by the true dual/multiple configuration gain the advantage of a significantly lower risk to the critical operations of the facility with the most backup redundancy possible, because the system is designed to eliminate single points of failure and to enable electrical loads within the facility to be shared.

## Efficiencies

Specific to MCOs, *efficiency* refers to the ability to deliver the same desired critical operations while using less energy, incurring lower costs (namely, utility costs), and/or requiring less involvement or maintenance by specialized technicians.

Reducing costs and improving efficiency are elements that are under the microscope at every opportunity. From initial construction, operations, and repair, it is always a balancing act of ensuring continuous operations of the facility at a cost that is acceptable to the business. To do so, many design engineers are increasingly choosing medium-voltage power distribution over low-voltage power distribution within their Mission Critical facilities.

In any power system, the larger the load current and the larger the conductor resistance, the larger the voltage drop between the utility-source and the distribution system. A medium voltage distribution system helps to reduce drops in voltage from the utility service to the load, therefore increasing the overall effectiveness of the distribution system. Low voltage distribution systems generally have much longer feeder runs and must be designed to be oversized in an effort to compensate for the resistance of the conductor; since medium voltage systems have a smaller load current and reduced voltage drop, the necessity for oversized conductors can be eliminated.

Utilizing medium voltage power distribution can also reduce the upfront cost of copper conductors and installation as well as the long term operating costs. This method provides the opportunity to move the transformation of load power closer to the load itself to take advantage of the reduced current at higher voltages. Lower current equates to smaller and fewer copper conductors, thus reducing overall costs.

# ACTIVITY 3-1

## Differentiating Low and Medium Voltage Systems

### Scenario

In this activity, you will differentiate between low voltage and medium voltage systems.

1. **The set of electrical transmission systems that receive power from a primary source and then divide it up, pass it through any protective features, and deliver it to the connected equipment load is known as?**
  - A power distribution unit
  - An uninterruptible power supply
  - Power distribution
  - Utility-source power
2. **A rack-mounted power strip is an example of which of the following critical components?**
  - An automatic transfer switch
  - An uninterruptible power supply
  - A dual-supply power cord
  - A power distribution unit
3. **Which of the following types of power sources are supported by only one substation and feed but potentially multiple transformers?**
  - Single feed–single substation
  - Multiple feed–single substation
  - Multiple substation
  - True dual/multiple feed
4. **Which of the following types of power sources are supported by only one substation with a single throw-over switch at the input feed to the utility transformer?**
  - Single feed–single substation
  - Multiple feed–single substation
  - Multiple substation
  - True dual/multiple feed
5. **Which of the following types of power sources are supported by multiple power lines with single input feeds and a single throw-over switch connecting the substation outputs in the event of a failure?**
  - Single feed– single substation
  - Multiple feed– single substation
  - Multiple substation
  - True dual/multiple feed

6. Which of the following types of power sources are supported by single, independent feeds from multiple substations?
- Single feed–single substation
  - Multiple feed–single substation
  - Multiple substation
  - True dual/multiple feed
-

# TOPIC B

## Redundancy

When it comes to providing power to your MCO system, one of the most important things you need to consider is how to ensure that power is always being consistently supplied. As a Mission Critical Operator, you will need to understand the concept of redundancy as a method for maintaining stable power and distributing it appropriately throughout your power system and selecting the appropriate scheme for your facility's needs. In this topic, you will identify redundancy levels.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Redundancy
- Dual-cord supply


## Redundancy

*Redundancy* refers to the inclusion of extra systems, equipment, or components that may or may not be in service all the time, but provide additional capacity or function to support critical operations in the event of critical equipment failure.

In the world of MCOs, however, the concept of redundancy is much more multi-faceted than the word “extra” implies. How many components of a system have redundancy? Is it just extra capacity or really extra equipment? Does the extra equipment sit idle in standby, or can it be used for non-critical functions until called upon in the event of a failure? To what extent can a single fault take out the primary component *and* the redundant component?

## Redundancy Levels

Most of the MCO industries are converging towards a common language regarding redundancy and the different variations, or levels, of redundancy. This means an MCO technician can walk from a power plant to a data center to a critical manufacturing facility and understand very quickly what equipment is actually being used out on the floor when the operations manager describes the designed redundancy.

	<b>Note:</b> Redundancy levels in regard to mechanical and controls systems have essentially the same meaning as they are described here, in terms of power distribution systems.
---	---

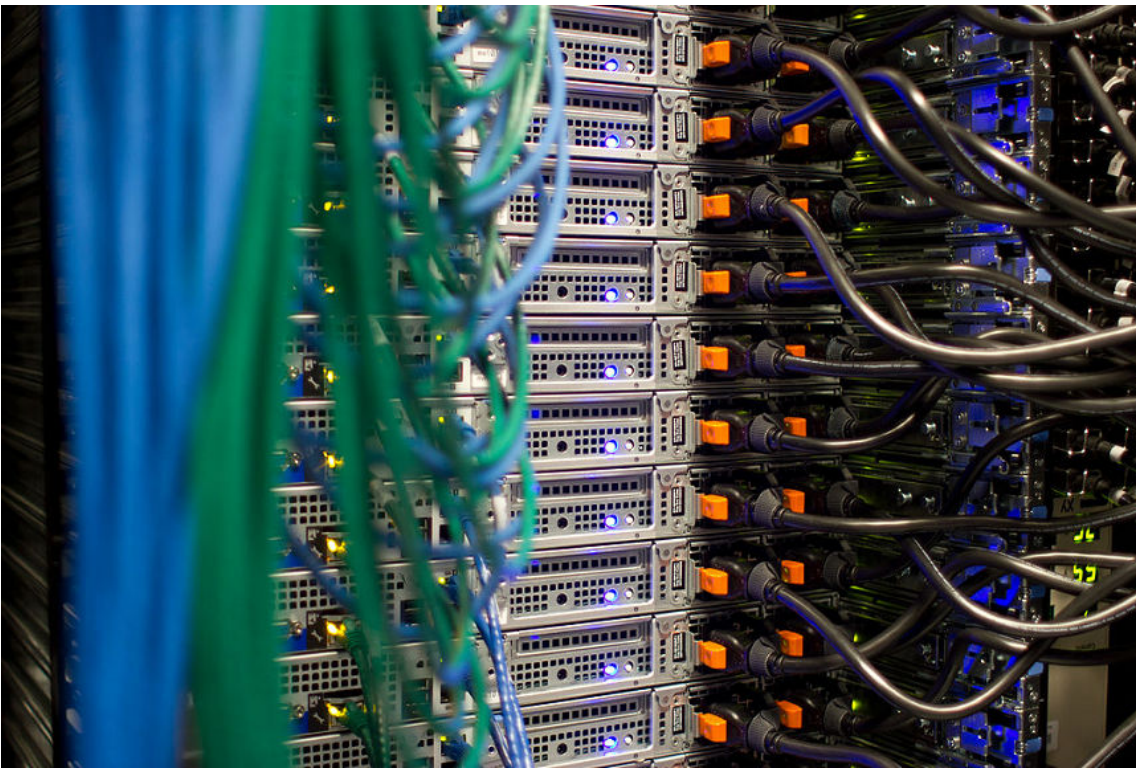
These various levels of redundancy include the following.

<i>Redundancy Level</i>	<i>Description</i>
N	<p>N is to redundancy discussions as the variable “x” is to mathematics: a given or basic number of some thing(s). <i>N redundancy</i> means just that: the basic number of some type of device or equipment (be it generators, UPSs, chillers, etc.) required to support and operate the critical infrastructure.</p> <p>In this case, the number of items is more limiting than capacity. For instance, an MCO facility that requires 2 MW of power for its critical infrastructure with a single 5 MW generator is only operating at N redundancy; that same facility is still operating at N redundancy if it uses two 1.5 MW generators because while it has an extra piece of equipment, it is not supporting two times the critical load.</p>

<b>Redundancy Level</b>	<b>Description</b>
N+1	<p><i>N + 1 redundancy</i> means all of the components needed to continuously support MCOs are present, plus one extra piece of equipment.</p> <p>In this case, the same 2 MW facility with three 1.5 MW generators is <math>N + 1</math>. Regardless of how large a number <math>N</math> actually is, the <math>+ 1</math> is really still just one more unit. Hence, a 10 MW installation with six 2 MW generators is <math>N + 1</math>.</p>
2N	<p><i>2N redundancy</i> follows the math function implication in that there is (at least) twice the number of components or systems that are needed to support critical operations. These units may or may not be grouped in distinct sets and may or may not be interconnected.</p> <p>In the case of a 10 MW facility with 2 MW generators, ten generators would be needed for it to be considered operating at <math>2N</math> redundancy. However, this could be two sets of five 2 MW generators that independently connect to the power distribution system; two sets of five 2 MW generators that only operate in those groupings, but share a common connection to the power distribution; ten 2 MW generators that all come online together, but any number of them (up to five) could drop off and the remaining units split the load; or any other combination that utilizes the ten generators.</p>
2(N+1)	<p><i>2(N+1) redundancy</i> means that there is twice the components needed to continuously support MCOs, plus one extra piece of equipment. It is a very robust design according to the math, but does have a fairly strict implication in that each <math>(N + 1)</math> component does need to be a separate set. The benefit derived from <math>2(N + 1)</math> design is that the facility could lose a full system or component and still have equipment or component level redundancy.</p> <p>In the case of a facility with three 1.5 MW generators for a 2 MW facility, the better application of <math>2(N + 1)</math> design is more detailed than just having six generators. Each set of three generators should be at least partially segregated to operate as distinct groups; even better, if the MCOs can afford it, each distinct group would tie into the power distribution system in separate locations for full redundancy.</p>

## Dual-Cord Supply

When you get down to the level of an individual piece of equipment, redundancy can get a bit tricky. Utilizing a *dual-cord supply* scheme is the most common approach for high-technology equipment and literally refers to plugging that piece of equipment in twice.



**Figure 3-3: Rack-mounted servers in a data center utilize dual-cord supplies to provide power redundancy. (Source: Victorgrigas/Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:Wikimedia\\_Foundation\\_Servers-8055\\_24.jpg](https://commons.wikimedia.org/wiki/File:Wikimedia_Foundation_Servers-8055_24.jpg))**

When utilizing dual-cord supply, there is a basic method and a preferred method. In almost any piece of equipment, there is usually an internal power supply of some sort behind the power cord connection that takes the supplied power and converts it to what the machine needs to run on (AC vs. DC, a particular voltage, wattage, etc.). The machine will therefore need two of these. The basic method to establish redundancy is to have this configuration and plug both cords into the same supply circuit. The preferred method is for each of these cords to be connected to separate power circuits, so that there is redundancy if the machine's power supply component fails, but also if one of the circuits in an MCO system goes down.

There are two situations where dual-cord supply is important and therefore often implemented: with medical equipment and data center equipment. Medical equipment tops the list of candidates for dual-cord supply, simply because there may be one or more lives at risk. Not all medical equipment is highly sensitive to losing power for fractions of a second, but if a life-support system or surgical device went offline for even a few seconds or minutes, the results could be deadly. Additionally, when it comes to complex modern medical technologies, it's not just about how long power is lost, but whether or not the start-up cycle time for that equipment is lengthy enough to have equally terrible consequences.

When it comes to data center equipment, dual-cord supply is equally important. Computers operate at incredibly high speeds and, in most cases, all outages are therefore equal: it doesn't matter if power was lost for one second or milliseconds. Lost data, lost transactions, the risk of fail-over systems not picking up the load are all examples of how millions of dollars can be lost all for the sake of not installing an additional \$50 power cord.

# ACTIVITY 3–2

## Identifying Redundancy Levels

### Scenario

In this activity, you will identify the various redundancy levels that can be implemented in a power distribution system.

---

#### 1. What does the term *redundancy* mean?

- The extra systems, equipment, or components that are always in service, all the time, in order to provide additional capacity or function to support critical operations in the event of critical equipment failure.
- The critical systems, equipment, or components that only come online in order to provide additional capacity or function to support critical operations in the event of critical equipment failure.
- The extra systems, equipment, or components that may or may not be in service all the time, in order to provide additional capacity or function to support critical operations in the event of critical equipment failure.
- The critical systems, equipment, or components that are always in service, all the time, in order to provide additional capacity or function to support critical operations in the event of critical equipment failure.

#### 2. Which redundancy level requires only the number of components necessary to support and operate the critical infrastructure?

- N
- N + 1
- 2N
- 2(N + 1)

#### 3. Which redundancy level requires all of the components necessary to support and operate the critical infrastructure, plus one extra component?

- N
- N + 1
- 2N
- 2(N + 1)

#### 4. Which redundancy level requires twice the number of components necessary to support and operate the critical infrastructure?

- N
- N + 1
- 2N
- 2(N + 1)



5. Which redundancy level requires twice the number of components necessary to support and operate the critical infrastructure, plus one extra component?

- N
  - N + 1
  - 2N
  - 2(N + 1)
-

# TOPIC C

## Power Supply Transfer

With a strong understanding of the fundamentals of power distribution and redundancy, you can then begin to explore what to do if there is any interruption to the stable power being delivered through the system. In the event of some sort of power outage, having the ability to easily switch between the primary power source and the backup power source is of the utmost importance.

As a Mission Critical Operator, you will need to understand the basics of power supply transfer, including the various components that can be used to perform this important function. In this topic, you will identify the elements of power supply transfer.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- CTTS (closed transition transfer switch)
- Open transition transfer switch
- SLTS (soft loading transfer switch)
- STS (static transfer switch)
- Soft loading closed transfer switch
- Interlock
- Trapped key interlock

### Closed Transition Transfer Switch

Closed transition is a method of switching between two power sources utilizing the “make before break” method of transfer. A *closed transition transfer switch (CTTS)* utilizes switch logic technology to determine if the subject sources to be connected meet the same criteria for voltage, frequency, and phase relationship between each source of power. If these conditions are met within tolerances, the switch contacts close or “make” with a slight overlap for transfer to prevent any interruption of supplied service.

### Open Transition Transfer Switch

The opposite of closed transition, open transition is known as the “break before make” method of transfer; in this design, an *open transition transfer switch* completely breaks its connection to one power source before making connection to the next. During this time frame, neither the primary power source nor the secondary power source is providing electricity to a load downstream.

### Soft Loading Transfer Switch

Soft loading is a method of switching between two power sources where a *soft loading transfer switch* synchronizes and parallels the two independent power sources without the interruption of power, and then transfers the load between the two as it minimizes the momentary variations in the voltage and frequency. In this manner, the load is slowly modulated to the new source, such as an emergency generator, upon transfer.

### Static Transfer Switch

A *static transfer switch (STS)* utilizes solid state power electronics and silicone controlled rectifiers to transfer power very rapidly without utilizing slower electromechanical means to transfer the power supply. This type of switch is very effective at protecting critical systems from short duration power disturbances and interruptions. The STS simply monitors two sources of power and automatically

transfers to the source that is within proper operating parameters upon any interruption or degradation of the primary (or previous) power source.

## Soft Loading Closed Transition Switch

A *soft loading closed transition switch* is often utilized to support an automatic transfer of power while enabling an emergency generator to synchronize with a utility service. This transfer system closes the generator to the utility and then transfers the facility load gradually to synchronize the emergency generator set without interruption of service. Upon transitioning back to utility, the system allows the emergency generator load to be gradually reduced before being removed from the electrical bus.

## Automatic Transfer Switch

As you may recall, an automatic transfer switch (ATS) automatically transfers electrical power from the primary source (via electromechanical means) to an alternate source such as an emergency generator set. Once the control panel of the ATS senses a power failure, it signals the emergency generator to start, which continues to accelerate to an optimum level in preparation to accept the electrical load. Once this level is achieved or pre-set amount of delay time has passed, the ATS will transfer the load to this alternate source of power. Once normal power is restored, the ATS senses proper power is once again supplied and transfers back to primary power after a specific time delay is achieved.



**Figure 3–4:** An automatic transfer switch connected to the main breaker box. (Source: Logical Operations for NCMCO)

## Critical Power Interlocks

An *interlock* is a device or controls function used to prevent a component from causing damage to itself or the system by stopping during a power outage. This is achieved by utilizing two circuit breakers that are interlocked so that only one can close at a time. In this manner, an interlock system

maintains the critical load during a power outage, while prohibiting the circuit breakers from being powered by two different sources at the same time while connecting to the load.

In the case of an electrical transfer from utility power to generator, the interlock system will enable a safe disconnect from the utility feed to the emergency generator power without the two sources connecting to each other. This separation eliminates the possibility of electrical back feed which can be extremely dangerous to personnel and cause catastrophic damage to critical equipment.

## Trapped Key Interlocks

Trapped Key Interlocks are almost universal in their use as a physical layer of breaker pair controls. Just as the name implies, in a *Trapped Key Interlock* a key is actually trapped inside a cylinder that is part of the breaker itself. In one key position, the breaker is free to operate; in the alternate position, some sort of physical obstruction (typically, a bar) is inserted through the breaker operator mechanism, locking it in that position.



**Figure 3–5: A Trapped Key Interlock.** (Source: Wtshymanski/Creative Commons (CC BY-SA 4.0)/ [https://commons.wikimedia.org/wiki/File:Trapped\\_key\\_interlock\\_transfer\\_block.JPG](https://commons.wikimedia.org/wiki/File:Trapped_key_interlock_transfer_block.JPG))

Specific pairs of breakers that are highly sensitive to each other's operation are keyed with the same cylinder and labeled with a letter or number. There is, however, only one key between the two. For example, one breaker may be open with the key removed. In order to close that breaker, its paired breaker must be opened first, allowing that key to be removed, placed into the lock on the first breaker, and turned to a position allowing operation.



**Note:** Trapped Key Interlocks are commonly referred to as Kirk Keys. Kirk Keys are a specific brand of trapped key interlocking systems, but having been around for over a century, many MCO personnel have gotten into the habit of referring to all trapped key interlock systems, regardless of manufacturer, as Kirk Keys.

# ACTIVITY 3–3

## Identifying the Elements of Power Supply Transfer

### Scenario

In this activity, you will identify the various components used in power supply transfer.

1. **Which power supply transfer component first synchronizes the two independent power sources and then transfers the load between the two as it minimizes the momentary variations in the voltage and frequency?**
  - Soft loading closed transition switch
  - Open transition transfer switch
  - Soft loading transfer switch
  - Static transfer switch
  
2. **Which power supply transfer component first determines if the sources meet the same criteria for voltage, frequency, and phase relationship and then closes the contacts with a slight overlap to prevent any interruption to the power?**
  - Automatic transfer switch
  - Closed transition transfer switch
  - Static transfer switch
  - Soft loading closed transition switch
  
3. **Which power supply transfer component monitors the two sources of power and automatically transfers to the source that is within proper operating parameters upon any interruption to the primary power source?**
  - Automatic transfer switch
  - Open transition transfer switch
  - Interlock
  - Static transfer switch
  
4. **Which power supply transfer component automatically transfers electrical power from the primary source to an alternate source such as an emergency generator?**
  - Static transfer switch
  - Soft loading closed transition switch
  - Automatic transfer switch
  - Open transition transfer switch
  
5. **Which power supply transfer component completely breaks its connection to one power source before making connection to the other?**
  - Closed transition transfer switch
  - Interlock
  - Soft loading transfer switch
  - Open transition transfer switch

6. Which power supply transfer component automatically transfers power between the utility source and a generator, without interruption of service, by closing the connection between the generator and the utility and then transferring the load gradually?
- Interlock
  - Automatic transfer switch
  - Soft loading closed transition switch
  - Closed transition transfer switch
7. Which power supply transfer component utilizes a pair of interconnected circuit breakers to enable a safe transfer from the utility source to a generator, without the two sources connecting to each other?
- Static transfer switch
  - Interlock
  - Closed transition transfer switch
  - Soft loading transfer switch
-

# TOPIC D

## Power Distribution Topologies

Now that you know about the concepts of redundancy and the components of power distribution and transfer, it's time to think about how all these components go together to provide the necessary redundancy for your MCO system. As an MCO operator, it is important for you to understand the concept of a topology and select the appropriate schema that will successfully support your facility in the event of an emergency. In this topic, you will identify the various power distribution topologies.

### Power Distribution Topology

The topology of systems refers to more than just what is in a system: it focuses on how and why things are laid out and connected the way they are. Specific to power distribution, then, this refers to the specific design of the power distribution system, made in such a manner that it offers the most optimal operations. With this in mind, an MCO design may include the best equipment available and extra components for redundancy, but the next step in mitigating risk and ensuring reliability is a well-defined topology that takes into consideration more than just a piece of equipment breaking down.

Redundancy is only one part of topology reliability designs—we do want extra equipment, after all. Taking steps to protect parts of systems, or other systems, from nearby faults is how we take steps toward higher and higher levels of reliability. In this vein, there are four different topologies or "tiers" of design that are commonly used in power distribution (and that are applicable to other system designs): basic, redundant, concurrent maintainability, and fault tolerant. For simplicity's sake, we'll look at each of these topologies using a single MCO example utilizing generators and associated generator switchgear for distribution, with a desired  $N + 1$  level of redundancy for a 5MW load.



**Note:** The Uptime Institute—a consortium of companies that oversee the education and certification of enterprise data center professionals—has perhaps the most well-defined and widely recognized system for design topology analysis. The Tier System they have developed has four levels corresponding to the major levels of reliability: Tier I—Basic, Tier II—Redundant, Tier III—Concurrently Maintainable, and Tier IV—Fault Tolerant. A full description of the tier classification system, the tier classifications, and the process for site certification analysis is included in an appendix, reprinted with permission from the Uptime Institute.

### Basic Topology

Basic topology for the example facility (generators, associated switchgear, and a desired  $N + 1$  level of redundancy for a 5MW load) gives us just enough to keep things running—perhaps two 2.5 MW generators connected to a single generator switchgear. During a loss of power—while, hopefully, a UPS system is carrying the load—the generators fire up and supply the whole power distribution system from a single connection. While this is better than no back up, for sure, a basic topology is just barely an acceptable option.

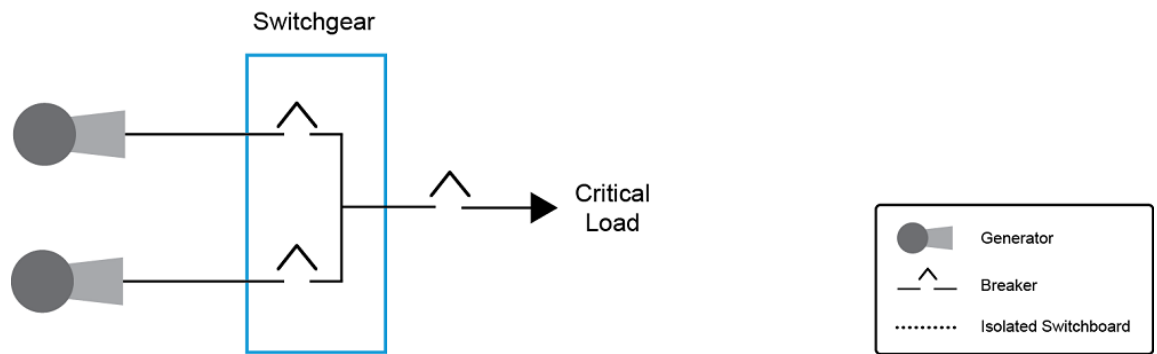


Figure 3-6: A basic topology. (Source: Logical Operations for NCMCO)

### Redundant Topology

Given the desired level of  $N + 1$  redundancy when the design allows for it at the example MCO facility, you would need at least one extra unit beyond  $N$ . Redundant topology for this facility would be three 2.5 MW generators sharing a common connection to the generator switchgear. Upon a loss of power, all three generators would come online to power the facility (most likely, but the logic could call for just two, keeping one in ready standby), but a fault on one unit will still leave sufficient capacity to carry all the critical load. In this manner of thinking, a redundant topology is a good option.

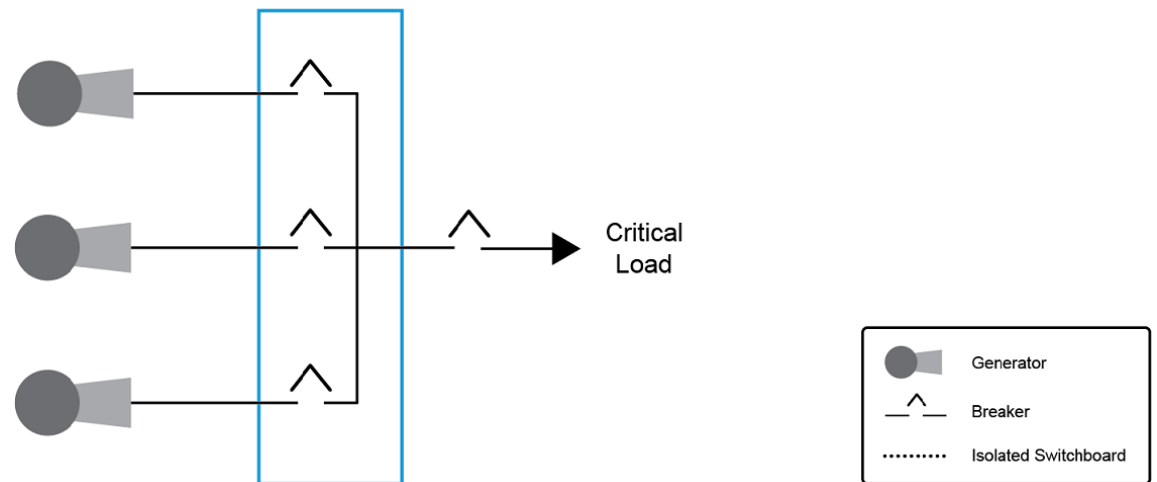


Figure 3-7: A redundant topology. (Source: Logical Operations for NCMCO)

### Concurrently Maintainable Topology

Concurrently maintainable topology takes it one step further by adding isolation points around the pieces of equipment in a system with redundancy. As the name implies, this allows for maintenance or repair of equipment without taking the entire system out of service. In the MCO example, each of the three generators would certainly have output isolation breakers, but would also have an additional means of separation at the generator switchgear—perhaps additional breaker cubicles that isolate each conductor connection from the switchgear. By opening both of those breakers, MCO technicians could safely work on a single unit without compromising the system's ability to fully support its design function (although, redundancy may be affected). Acknowledging notable additional cost, some MCOs might push a very rigid view of concurrent maintainability such that taking one unit offline still leaves the desired redundancy level—think of this as  $N + 1 + 1$  or  $N + 2$ . In this manner of thinking, a concurrently maintainable topology is a better option.



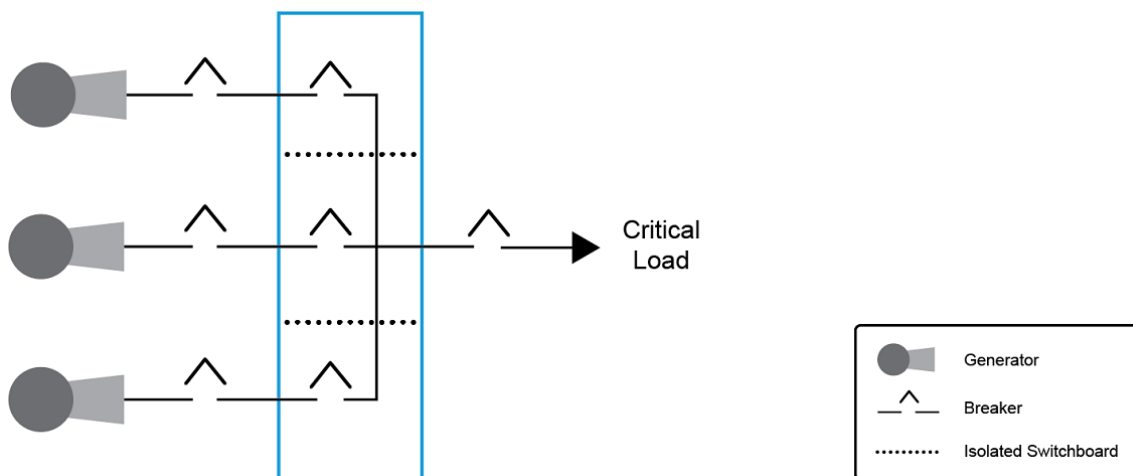


Figure 3-8: A concurrently maintainable topology. (Source: Logical Operations for NCMCO)

### Fault Tolerant Topology

A fault tolerant topology has the most strenuous design considerations put into place; basically referring to a design in which a single fault would not take out an entire system. From a redundancy perspective, we would see  $2(N + 1)$  for all equipment and components in the system. In the MCO example, there would be two sets of three 2.5 MW generators (for a total of six units), with each set having its own separate generator switchgear. The two units would most likely be connected by a normally closed “tie-breaker” between them, with the ability to supply the power distribution system from either end. Not only does the MCO team benefit from the aspects of concurrent maintainability, any fault (generator failure, switchgear breaker failure, fault on the switchgear, etc.) only takes out one half of the system, leaving it with a full  $N + 1$  set of equipment available. In this manner of thinking, the fault tolerant topology is the best option.

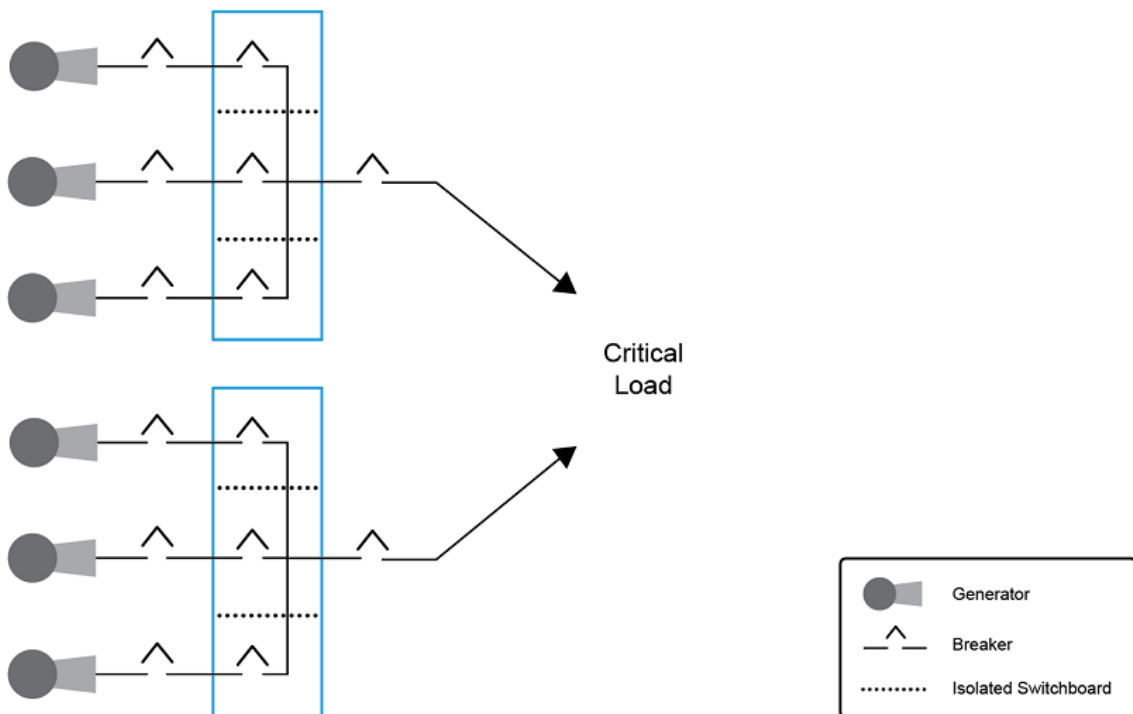


Figure 3-9: A fault tolerant topology. (Source: Logical Operations for NCMCO)

# ACTIVITY 3–4

## Identifying Power Distribution Topologies

### Scenario

In this activity, you will identify power distribution topologies.

---

1. In regard to power distribution specifically, what does the term *topology* mean?
    - The number and type of components in the system.
    - The ways in which the components interact.
    - The ways in which the components are arranged.
    - The ways in which the components are arranged and interact.
  2. Which type of topology utilizes additional isolation points at the key redundant components to make it possible to repair a component without taking the entire system down?
    - Basic
    - Redundant
    - Concurrently maintainable
    - Fault tolerant
  3. Which type of topology utilizes just enough backup components that can provide power to the system in the event of an outage?
    - Basic
    - Redundant
    - Concurrently maintainable
    - Fault tolerant
  4. Which type of topology utilizes a redundant counterpart for all components to prevent any single issue from taking out the system?
    - Basic
    - Redundant
    - Concurrently maintainable
    - Fault tolerant
  5. Which type of topology utilizes the baseline of backup components plus one additional backup component that could provide power to the system in the event of an outage?
    - Basic
    - Redundant
    - Concurrently maintainable
    - Fault tolerant
-

# TOPIC E

## Electrical Protection

As you start to get further into the design of a system's power distribution scheme—including which critical components will be implemented and how they will be implemented—you need to make sure that you have put the proper protections in place to ensure that every component in the electrical system is operating safely. Any amount of electrical voltage could be hazardous to the people or parts in any given facility, but the voltage in an MCO facility is exponentially more dangerous.

As an MCO operator, you will need to know what techniques and devices are available to protect your facility's personnel and critical components from dangerous electrical events. In this topic, you will identify and apply electrical protection techniques.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Over-current protection
- Protective relay
- TVSS (Transient Voltage Surge Suppressor)
- Arc flash
- Arc fault potential
- Zone selective interlock

## Grounding Electrical Equipment

As you may recall, grounding is the process of removing excess electrical charge from a component or system and distributing it to a larger body capable of receiving that charge. When it comes to your power distribution system, grounding is an extremely important concept, especially due to the higher voltages that you may interact with at this level of the distribution chain.

In addition to grounding measures in place throughout power distribution systems as a whole, individual electrical equipment should have grounding connections whenever possible to mitigate the risk of damage to the equipment during faults and to disperse any excess charge for personnel safety. In many cases, individual pieces of equipment may be connected directly to those larger facility grounding systems. In this situation, it is imperative that these connections are well-documented and well-designed, so that the pathways of lower electrical potential lead to the ground termination and not back to smaller equipment.

Equipment may also be grounded locally if need be. For example, a PDU may be located in a hall or closet somewhere between the switchgear and the critical load, but not near the installed grounding system. In this case, the PDU may be grounded to a piece of structural building steel, or just a single copper rod sunk into the subfloor.

## Over-Current Protection

*Over-current protection* is likely the type of electrical protection that you are familiar with: it's just a means of interrupting the power flow when it exceeds safe levels. This is most often achieved by a breaker tripping or fuse blowing—the exact same thing you've probably experienced in your own home if you overloaded an outlet. A surge of current through the device triggers the interruption, which likely requires a manual reset.



**Figure 3–10:** In over-current protection, a breaker automatically switches to the off position when the power exceeds the level it can support. (Source: Logical Operations for NCMCO)

Over-current protections can be instantaneous or over a pre-determined, measured period of time. For example, most motors have a notably higher starting current than running current, so we don't want equipment tripping a breaker just because there are twice as many amps as usual if the motor equipment is shifting. So, on a PDU that is feeding mechanical equipment, the design may call for the PDU to trip breakers instantaneously at one hundred times the running current, or at twenty-five times the running current and sustain it for three seconds.

Some advanced logic controls may be able to analyze the occurrence and determine if it is safe to close the breaker and rejoin back in to the load, but the majority of MCO operations personnel prefer to stick with manual resets so that a technician has the chance to troubleshoot the occurrence and make the determination whether or not a dangerous condition still exists.

## Protective Relays

*Protective relays* are electromagnetically or electronically operated devices that sense conditions and/or receive logic inputs to remotely accomplish protective actions. More simply, these are the mechanical devices that open and close breakers in response to undesirable conditions. This is generally the means by which breakers are tripped open during protective features such as over-current. Protective relays may also be controlled by logic as part of a response sequence, closing breakers for alternate source after a primary source is tripped due to a fault condition.



**Figure 3-11: Protective relays used to provide over-current protection at a power generating station. (Source: Wtshymanski/Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:Protective\\_Relays\\_Hydroelectric\\_Station.JPG](https://commons.wikimedia.org/wiki/File:Protective_Relays_Hydroelectric_Station.JPG))**

## Surge Protection

Just like you might have a surge protector at home to protect your electronic devices from harmful spikes in the power supply (typically in the form of a surge-protected power strip), MCOs need a form of surge protection to do the same for their critical components. A *Transient Voltage Surge Suppressor (TVSS)* is the industrial equivalent to the surge protector power strip your home electronics are plugged into, and provides electrical protection to connected equipment by buffering and absorbing voltage spikes. There are many variants of TVSS systems available to MCO designers, with a wide range of proprietary technologies (usually to protect specific types of equipment or to mitigate specific types of transients (i.e., momentary changes in the voltage)).

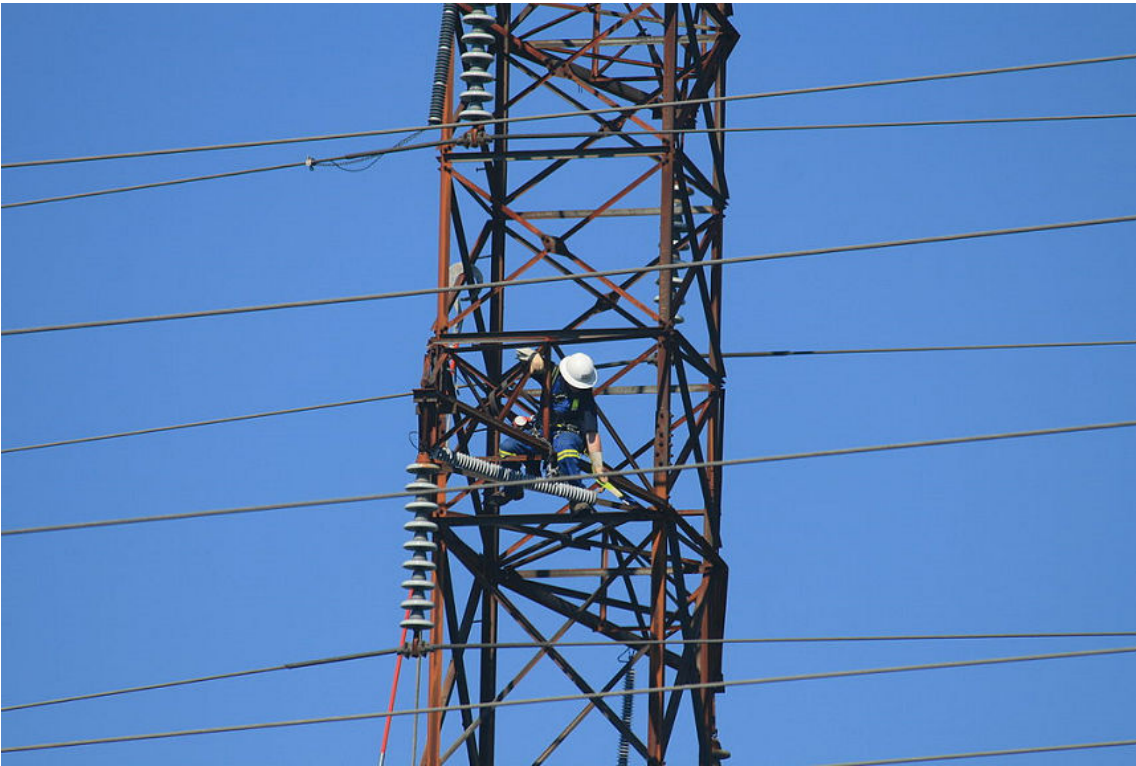
The basic concept of surge protection—in addition to the specific protections that individual equipment may have—is to have inline devices throughout the power distribution system that act as energy diverters. When a TVSS module senses a condition for which it is configured, it uses some form of switch to quickly divert part or all of the excess voltage away from the connected load, generally to a ground connection.



*Figure 3–12: A TVSS surge protector in a printing and distribution space. (Source: Logical Operations for NCMCO)*

## Lightning Protection

Since MCO facilities have a tendency to be very large, often remotely located, they are clearly at higher than average risk for lightning strikes. Lightning protection comes in many forms and is simply a safeguard to MCOs from lightning strikes. It can be as simple as a single tower located away from the main facility, or a series of small lightning rods (similar to those found in residential applications) connected to a ground conductor.

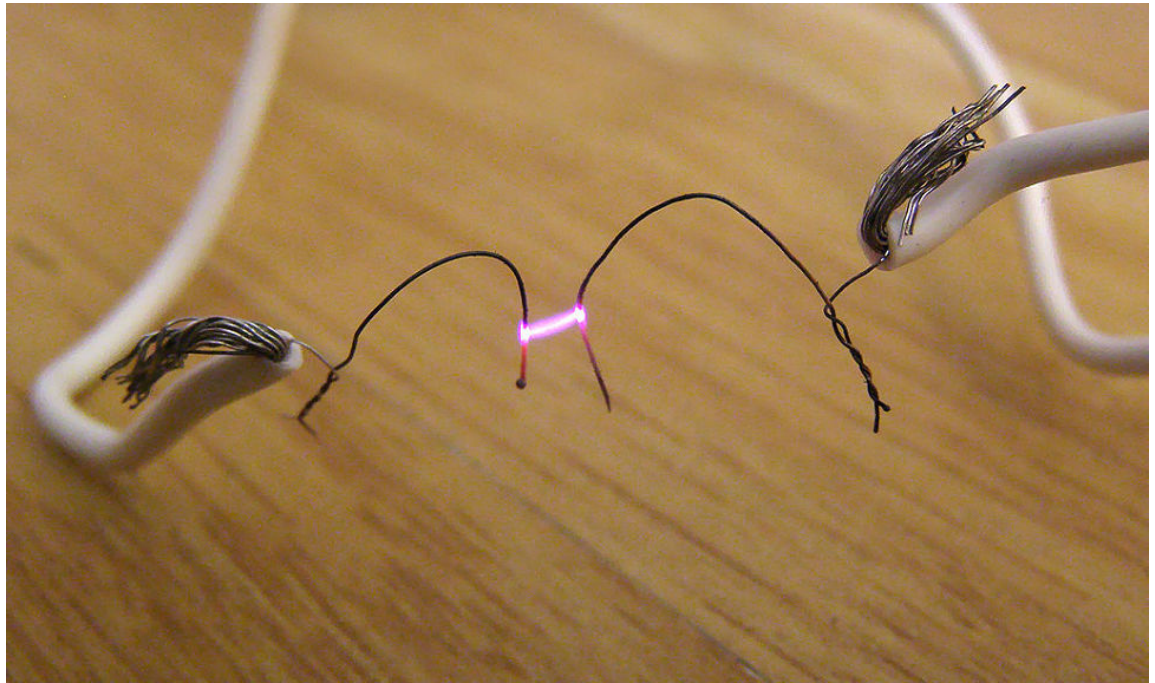


**Figure 3–13:** A worker performs maintenance on a lighting protection device on an electrical transmission tower. (Source: Tew3/Creative Commons (CC BY 3.0)/<https://commons.wikimedia.org/wiki/File:NBPowerTransmissionTowerMaintenance.JPG>)

TVSS setups are also a form of lightning protection to handle the immense voltages associated with a strike. For MCO installations that may share utility connections with non-critical spaces or other customers (namely, not having their own substation and switchgear with a full set of other protective trips, relays, and interlocks), TVSS should be an important part of the design in regard to lightning protection, as the MCO installation may not have full control of the incoming utility.

## Arc Flash Protection

An *arc flash* is an explosion of heat, light, molten metal, and plasma that results when an electrical connection is made with very little resistance. Most commonly, an arc is the result of a short between phases and or ground connections (imagine what happens when a conductive material falls across two power lines running along the street). You may have experienced a small spark when removing a plug from a power outlet—this is a minor arc. In MCOs, however, you are exposed to much higher electrical energies than in your home, so these arcs become exponentially more powerful and dangerous. Operators and technicians are most exposed to arc flash risks when operating and maintaining switchgear and breakers.



**Figure 3-14: An arc flash between two live wires.** (Source: Khimich Alex/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Electric\\_arc.jpg](https://commons.wikimedia.org/wiki/File:Electric_arc.jpg))

Arc flash protection is the method and means for determining safe working boundaries in the event of arc flash situations. Determining the proper arc flash protection relies a lot on the system's *arc fault potential*: the calculated maximum amount of energy that may be released by a fault in a particular piece of equipment, taking into consideration any protective features in place. Categories of this risk then determine safe working distances and minimum levels of protective gear required to be worn by MCO operators.

For example, a large breaker cabinet may require minimal protective gear and not have a distance threshold during normal operation due to the strength of the enclosure. If the front or back panel of the cabinet is opened for maintenance, and the breakers are live, the arc flash guidance may require full protective gear within 36 inches and allow no immediate contact while energized (or until verified de-energized).

## Zone Selective Interlocks

Keeping in mind that electrical energy does not exist as a stationary point in a system but is always moving in some direction (ignoring energy storage devices for the moment), a *zone selective interlock* is an intelligent control feature that can be added to a protective system in order to prevent the entire system from responding to a fault.

For example, a ground fault may be sensed on an entire circuit, from the output of a UPS down to a specific piece of equipment; however, the logic-controlled zone selective interlocks will observe the condition and only perform the protective response at the point closest to the fault (furthest downstream, in most cases). This will ideally only trip the breakers nearest the condition—it wouldn't make sense to shut down the entire electrical lineup if only a single PDU has a fault.

This particular protection scheme could be designed in a very complex manner depending upon the scale of the MCO power distribution system and criticality of connected load, but the underlying principle remains the same: impact the least amount of equipment possible.



# ACTIVITY 3–5

## Applying Electrical Protection

### Scenario

In this activity, you will identify the techniques for applying electrical protection to your system.

- 1. Which type of electrical protection technique uses a component that buffers and absorbs voltage variations in the power supplied to the system?**
  - Over-current protection
  - Zone selective interlocking
  - Surge protection
  - Arc flash protection
- 2. Which type of electrical protection device automatically senses or receives input about the system's current power conditions, and then opens and closes breakers if undesirable conditions are detected?**
  - Zone selective interlock
  - Protective relays
  - Surge protectors
  - Arc flash protector
- 3. Which type of electrical protection technique interrupts the flow of power when it exceeds levels that are safe for the system or its components?**
  - Over-current protection
  - Surge protection
  - Arc flash protection
  - Zone selective interlocking
- 4. Which type of electrical protection device uses logic and intelligence to monitor the conditions of the system and, when a fault is observed, triggers a protective response at the point closest to the fault?**
  - Protective relays
  - Surge protectors
  - Arc flash protector
  - Zone selective interlock
- 5. What is the explosion of light and heat that occurs when an electrical connection is made with very little resistance called?**
  - Lightning
  - Arc flash
  - Over-current
  - Power surge

6. What is the calculated maximum amount of energy that could be released by a fault in a particular piece of equipment (even with protective gear in place) called?
- An over-current
  - A power surge
  - Arc flash potential
  - An arc flash
-

# TOPIC F

## Power Distribution Preventative Maintenance

Now that you can identify all of the various components of the power distribution system and how to protect them reactively in an emergency event, it is equally important to think about how you can protect them proactively. Preventative maintenance can help ensure that all your critical components are operating safely and effectively, even without the threat of an outage.

As an MCO operator, it is highly likely that your responsibilities will include completing these types of tasks. In this topic, you will identify the preventative maintenance procedures for power distribution components.

## Switchgear Maintenance

Switchgear maintenance involves removing all sources of electrical input to a gear lineup, exercising all moving parts, cleaning, tightening lugs, database maintenance on logic systems, and more, depending upon the particular equipment installed. It is generally the most complex, comprehensive, and risk-sensitive preventative maintenance procedures that most MCO facilities will experience on their support infrastructure (aside from the more complex maintenance of specialized components such as nuclear reactor refueling, bringing down a satellite tower, moving cryogenic R&D equipment, etc.). As it is difficult, and often dangerous, to methodically work through fully de-energizing switchgear for personnel safety, this maintenance is typically only done once every few years. MCO managers will take advantage of this rare condition to maintain as many components of this critical component as possible on a tight timeline.



**Figure 3–15:** The switchgear for an electrical main and its associated distribution should be maintained every few years. (Source: Zaereth/Creative Commons (CC BY-SA 4.0)/[https://commons.wikimedia.org/wiki/File:Electrical\\_Main\\_and\\_distribution\\_panel\\_for\\_480\\_volt.JPG](https://commons.wikimedia.org/wiki/File:Electrical_Main_and_distribution_panel_for_480_volt.JPG))

## Breaker Testing

Breaker testing involves physically inspecting a circuit breaker and subjecting it to as many functional checks as possible. This is often accomplished during switchgear maintenance schedules because it is much easier and quicker to remove breakers from de-energized cabinets. One sub-process of breaker testing is injection testing, in which varying levels of voltage, current, and/or resistance are applied to the breaker in order to check that its protective features respond appropriately.

## Coordination Studies

Breaker coordination studies refer to the analysis of installed breakers, their connected loads, and validating or setting their protective features to operate in proper sequencing. For example, breakers that are further down a lineup, and therefore closer to connected load, should generally have lower thresholds or tighter tolerances than those upstream. Similar to selective interlock functions, this allows for isolation of faults closest to the condition, affecting fewer adjacent components. Coordination studies should be performed during construction, but are unfortunately not regularly updated with the addition of new equipment. Many MCOs, therefore, prefer periodic reviews of the power distribution systems to identify any changes and then adjust settings appropriately.

## Exercising Generators

Exercising generators refers to a variety of maintenance activities from short weekly run starts, to load bank tests, to full transfer of connected critical load. It is general best practice to exercise

generators to at least a nominal extent on a monthly basis. This is a hotly debated topic amongst MCO personnel as there is always some risk. An engine could break during an otherwise innocuous test and inadvertently take a backup power supply away from the facility, or the switchgear could hang up during a full load transfer and force the UPSs to carry the load or cause an outage altogether. With proper equipment-level maintenance, these risks can be minimized, but never prevented. The other side of the argument is: if there is going to be a failure, why not have it during a controlled environment, with competent personnel around, and primary power sources still available?



**Figure 3-16:** Any generator sets onsite, whether backup or primary, should be exercised on a monthly basis. (Source: StcudorPrewoP/Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:Caterpillar\\_3512C\\_Generator\\_Set.JPG](https://commons.wikimedia.org/wiki/File:Caterpillar_3512C_Generator_Set.JPG))

## ACTIVITY 3–6

### Identifying Power Distribution Preventative Maintenance Procedures

#### Scenario

In this activity, you will identify the appropriate preventative maintenance procedures for power distribution components.

---

1. **Which type of preventative maintenance for power distribution systems involves the analysis of installed breakers, their connected loads, and validating or setting their protective features to operate in proper sequencing?**
    - Exercising generators
    - Coordination studies
    - Breaker testing
    - Switchgear maintenance
  
  2. **Which type of preventative maintenance for power distribution systems involves removing all sources of electrical input to a gear lineup, exercising all moving parts, cleaning, tightening lugs, and performing database maintenance on logic systems, and so forth?**
    - Coordination studies
    - Breaker testing
    - Switchgear maintenance
    - Exercising generators
  
  3. **Which type of preventative maintenance for power distribution systems involves a variety of activities including short weekly run starts, load bank tests, full transfers of connected critical load, and so forth?**
    - Exercising generators
    - Breaker testing
    - Switchgear maintenance
    - Coordination studies
  
  4. **Which type of preventative maintenance for power distribution systems involves physically inspecting the system's circuits and subjecting them to as many functional checks as possible?**
    - Switchgear maintenance
    - Coordination studies
    - Exercising generators
    - Breaker testing
-

## Summary

In this lesson, you identified and described the fundamental concepts of power distribution and the critical components of a power distribution system, particularly as it pertains to Mission Critical Operations. Having a strong understanding of power distribution, redundancy, and power distribution topologies, as well as the components that are used in supply transfer and electrical protection, will help you properly manage the power supplied to and throughout your MCO facility.





# 4

# Mission Critical Infrastructure: HVAC

## Lesson Objectives

In this lesson, you will identify and describe the HVAC components within a mission critical facility. You will:

- Understand the fundamental concepts related to heating, ventilation, and air conditioning.
- Identify refrigerant-based cooling systems.
- Identify water-based cooling systems.
- Identify alternative cooling systems.
- Identify air circulation systems and components.
- Identify preventative maintenance procedures for HVAC systems and their components.

## Lesson Introduction

While the critical components of an MCO facility might vary based on the product or services it provides, there is one critical system that applies to all Mission Critical Operations (MCOs)—the heating, ventilation, and air conditioning (HVAC) system. Regardless of the facility's use, the controlled and consistent ambient conditions of a facility are of the utmost importance, whether it is for people spaces or critical equipment spaces.

As an MCO operator, you will need to have a strong understanding of the fundamental concepts of HVAC; the various components and systems that provide the necessary heating, cooling, and air circulation services for a facility; and how to properly maintain those components for continued operations. In this lesson, you will identify and describe the heating, ventilation, and air conditioning components within a mission critical facility.

# TOPIC A

## HVAC Fundamentals

When you think of the types of critical equipment that span all kinds of mission critical facilities, HVAC equipment is probably some of the first that comes to mind. As a Mission Critical Operator, you will need to know not only what this critical equipment is and how it functions, but the basic scientific ideas behind the critical functions they provide. In this topic, you will learn about the fundamental concepts related to heating, ventilation, and air conditioning.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- HVAC (heating, ventilation, and air conditioning)
- Conditioned space
- Heat
- Entropy
- Heating
- Ventilation
- Air conditioning
- Refrigerant
- Temperature
- Sensible heat
- Latent heat
- VAV (variable air volume)
- Humidity
- Dew point
- Dry-bulb temperature
- Wet-bulb temperature
- Fluid
- Pressure
- PSI (pounds per square inch)
- Inch of water column
- Flow

## HVAC

*HVAC* is the term used to refer to the set (or sets) of systems and equipment that provide the heating, ventilation, and air conditioning services for a facility. This term and these services are common to all *conditioned spaces*, whether they are commercial offices, industrial settings, or the most modern MCO installation packed with technology. A conditioned space is any (at least partially) segregated space that has requirements for controlling atmospheric conditions—which is to say, any space where some or all air qualities are maintained to certain design parameters, including heating, cooling, adding or removing humidity, maintaining positive or negative pressures, and so forth. Similarly, air that has been conditioned has had its qualities changed to meet one (or sometimes more than one) of these parameters.

## Heating

*Heat* is a technical term referring to the energy transfer between substances, objects, systems, etc., that is not otherwise defined as work. In short, it's adding energy to or taking energy from the

material makeup of something. As a process, heat is closely tied to *entropy*, or the molecular disorder or randomness of matter.



**Note:** Take water, for example. You may recall from a Physics class that the changes of state for water are tied to the movement of the water molecules. Ice has molecules that are locked in place and are almost completely stationary. As heat is applied, the molecules begin to go crazy, bouncing around to the point that they can no longer exist in liquid form and need lots of space between them—creating steam. Throughout the process of transformation from ice to water to steam, the entropy of the substance is increased.

The British Thermal Unit (BTU) is a common unit of heat measurement (used in the English system of units, in English-speaking countries such as the United States and Canada). As a standard unit, it represents the amount of energy required to heat (or cool) one pound of water by one degree Fahrenheit. Converting this to an SI unit, 1 BTU = 1055 joules.

In general, *heating* in the context of HVAC refers to the warming of air or water for either people comfort or for maintaining the necessary conditions for the proper operation of critical equipment or systems. However, it is important to know that, in the context of MCOs, heat serves functions beyond just providing warmth and is used in other critical capacities.



**Figure 4-1:** A boiler provides heating for a facility. (Source: hxdyl/iStock/Thinkstock)

## Heat Sources

A heat source refers to anything that can produce or release heat in some form. In MCO facilities, heat sources generally provide heat energy for some combination of three main functions: space conditioning, primary energy source for power generation, and/or process work. Space conditioning includes functions such as moderating air or water temperature either for people comfort or for sustaining satisfactory conditions for equipment (especially if the MCO installation is in a cold climate). Heat can also be the primary source for power generation, such as in a boiler system that creates steam for use in turbines. Lastly, some highly specialized MCOs may call for specific heating

capabilities (in the form of air, water, or steam) for use in process work, such as manufacturing or R&D.

Common sources of primary or secondary heat provided for MCOs include:

- Natural gas
- Electric
- Oil
- Steam
- Coal
- Geothermal



**Note:** Depending upon the application, a source such as steam could be delivered to critical spaces as either a primary or a secondary source. Primary refers to steam being delivered from external to the MCO systems via a central service (e.g., a steam system provided for an entire campus where only one building is mission critical), while secondary means the steam could be generated local to the critical space (e.g., a gas-fired boiler).

## Heat Delivery Systems

Regardless of the heat source, MCO infrastructure still requires a means to deliver heat energy to the facility. Hot water and steam are carried throughout the installation via pipes, generally relying upon source pressure as the motive force, although some hot water systems may require booster pumps if spanning long distances or heights. Warm air for comfort often travels through the same ductwork as cool air, but doesn't necessarily have to.

A few examples of common heating systems include:

- Package or Rooftop Units (RTUs), where the heating elements and blower to circulate the heated air are contained in one unit.
- Split Systems, which create heat energy in one piece of equipment, and then the heating medium is carried to another separate unit where it transfers heat to circulating air.
- Ductless Systems, which are installed in walls where unheated air is pulled from one side, across heating elements, and then the heated air is pushed directly into the served space without any ducting.

## Ventilation

*Ventilation* refers to the exchange of air for either people comfort or equipment operations. This air does not necessarily have to be conditioned, although heating and cooling are commonly integrated with ventilation. Particularly in buildings occupied by a large number of people or in small occupied spaces, it is important to prevent the buildup of excessive CO<sub>2</sub> from respiration and ensure adequate O<sub>2</sub> levels. Some equipment may have gaseous by-products that pose a danger to people or are simply unpleasant, so a subsidiary function of ventilation includes removing hazardous or unwanted pollutants via exhaust fans and ducting systems.



**Figure 4-2:** These large double-exhaust fans provide ventilation for an office building. (Source: PictorialEvidence/Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:HVAC\\_Ventilation\\_Exhaust.jpg](https://commons.wikimedia.org/wiki/File:HVAC_Ventilation_Exhaust.jpg))

## Air Conditioning

*Air conditioning* refers to a designed management of the ambient conditions being delivered to a space, either for people comfort or for the proper operation of equipment. It is important for MCO technicians to understand this means more than just keeping spaces cool—humidity control is just as important to modern critical equipment and technology. In the context of HVAC, then, dehumidifying and cooling the air are handled by the air conditioning systems, while warming the air and manipulating air pressures are handled by the heating and ventilation systems, respectively.



**Figure 4-3: Air conditioning units provide cooling and humidity control for an office building.** (Source: Raysonho/Creative Commons (Public Domain)/<https://commons.wikimedia.org/wiki/File:ACFujitsu.jpg>)

## Refrigerants

A *refrigerant* is a substance—typically a fluid—that handles heat transfer in an HVAC system by changing its state from liquid to gas and back again, absorbing the heat at the low temperature/low pressure state and transferring the heat at the high temperature/high pressure state.

There are a multitude of chemicals that act as refrigerants for different applications based on qualities such as operating pressures, operating temperatures, and heat transfer rate capabilities. You may be familiar with products such as R-114, R-134a, or Freon (which is actually a brand name of a specific refrigerant, but has become a common term for a general type), which are all just different compounds of refrigerant.

### CFCs in Refrigerants

Many refrigerants have been phased out over the years because they contain hazardous chlorofluorocarbons (CFCs). Although these refrigerants were among the first manufactured and extremely effective, the CFCs they contain are incredibly damaging to the ozone layer. Via a series of international environmental treaties signed in the late 1980's—referred to as the Montreal Protocol—production of substances containing CFCs particularly for commercial and industrial use has been largely replaced with hydrofluorocarbons (HFCs). HFCs are not without their own environmental impacts, but they serve their purpose in the industry and do not have the highly detrimental qualities of CFCs.

## Temperature Measurements

*Temperature* is the measurement of the amount of heat an object or substance possesses; or from a different angle, the quantitative capacity for an object or substance to transfer heat energy to something else. Very specifically, using basic physics, you measure the average kinetic energy of the

particles of a substance. Depending upon the scale used, this can vary due to atmospheric pressures surrounding the substance, as that may tend to add or remove energy from the substance compared to different pressures.

There are three common temperature measurements that you are likely to encounter.

<b>Temperature Measurement</b>	<b>Description</b>
Fahrenheit	Fahrenheit is the temperature scale used predominantly in the United States and is based around two fixed points (at sea-level and standard atmospheric pressure) of the freezing point of water being 32°F and the boiling point of water being 212°F.
Celsius	Celsius is the temperature scale used in most of the rest of the world outside of the United States, and is based around a fixed measure of a degree (related to Kelvin) with pure water freezing at 0°C and boiling at 100°C.
Kelvin	Kelvin is the most modern of the common temperature measurements and is the SI unit of temperature. It is based upon an absolute scale (measuring the kinetic energy of component particles), with 0 K representing absolutely no motion at the atomic level. As a physical differential measure, 1°C is the same quantity as 1 K, even though the scales do not align since we can easily achieve temperatures less than the freezing point of water.

To convert between these various temperature measurements, use the following conversion calculations.

<b>Conversion</b>	<b>Calculation Formulas</b>
Fahrenheit ↔ Celsius	<p>Fahrenheit to Celsius:</p> $^{\circ}\text{C} = \frac{(^{\circ}\text{F} - 32)}{1.8}$ <p>Celsius to Fahrenheit:</p> $^{\circ}\text{F} = (^{\circ}\text{C} \times 1.8) + 32$
Fahrenheit ↔ Kelvin	<p>Fahrenheit to Kelvin:</p> $^{\circ}\text{K} = \frac{(^{\circ}\text{F} + 459.67)}{1.8}$ <p>Kelvin to Fahrenheit:</p> $^{\circ}\text{F} = (^{\circ}\text{K} \times 1.8) - 459.67$

<b>Conversion</b>	<b>Calculation Formulas</b>
Celsius ↔ Kelvin	Celsius to Kelvin:  $^{\circ}K = ^{\circ}C + 273.15$  Kelvin to Celsius:  $^{\circ}C = ^{\circ}K - 273.15$

## Sensible and Latent Heat

*Sensible heat* is the property of heat most commonly recognized and understood: a change in sensible heat correlates to a change in measured temperature. The addition or subtraction of heat energy is sensible when you can see movement up and down a temperature scale. Think of it this way: when you see the mercury in your thermometer rise up or down to display a change in the ambient temperature—that is sensible heat.

*Latent heat* is the heat energy added or removed from a substance during a change in state of the substance. For example, in perfectly stable standard conditions, liquid water changes to steam at 212°F; this particular point in the state shift, in which the measured temperature of the steam is identical to the measured temperature of the water (moments before enough heat energy was added to cause the change of state), is referred to as "latent heat of evaporation." The same holds true in reverse: a certain amount of latent heat energy is removed from steam at the moment it condenses; this particular point in the state shift, in which the old steam and the new water measuring the exact same temperature, is referred to as "latent heat of condensation."

## Variable Air Volume

*Variable Air Volume (VAV)* refers to a type of a heating, ventilating, or air conditioning system that varies the conditioned air flow but maintains the air at a constant temperature. VAV works opposite from a Constant Air Volume (CAV) system, which varies the air temperature but maintains a constant air flow. The advantage of a VAV system is more precise temperature control, reduced compressor wear, and lower energy consumption by system fans.

## Humidity

*Humidity* refers to the liquid moisture content suspended in a gas; particular to MCOs, this generally means the concentration of water molecules in the air. Since all atmospheric systems are dynamic—energy is always being added or removed at some scale—so there's a bit of give and take in the air when it comes to absorbing water vapor or expelling it; hence, the humidity level in the air is prone to changing.





**Figure 4–4:** An electronic hygrometer monitors the amount of humidity in the air for an occupied space. (Source: Guillaume Piolle/Creative Commons (CC BY 3.0)/[https://commons.wikimedia.org/wiki/File:Honeywell\\_device.jpg](https://commons.wikimedia.org/wiki/File:Honeywell_device.jpg))

## Dew Point

The *dew point* refers to the equilibrium temperature at which water vapor is absorbed by and condensed from the air at the same rate. When the air temperature drops just below the dew point for a given humidity, water molecules will condense and collect on solid surfaces.

## Dry-Bulb Temperature vs. Wet-Bulb Temperature

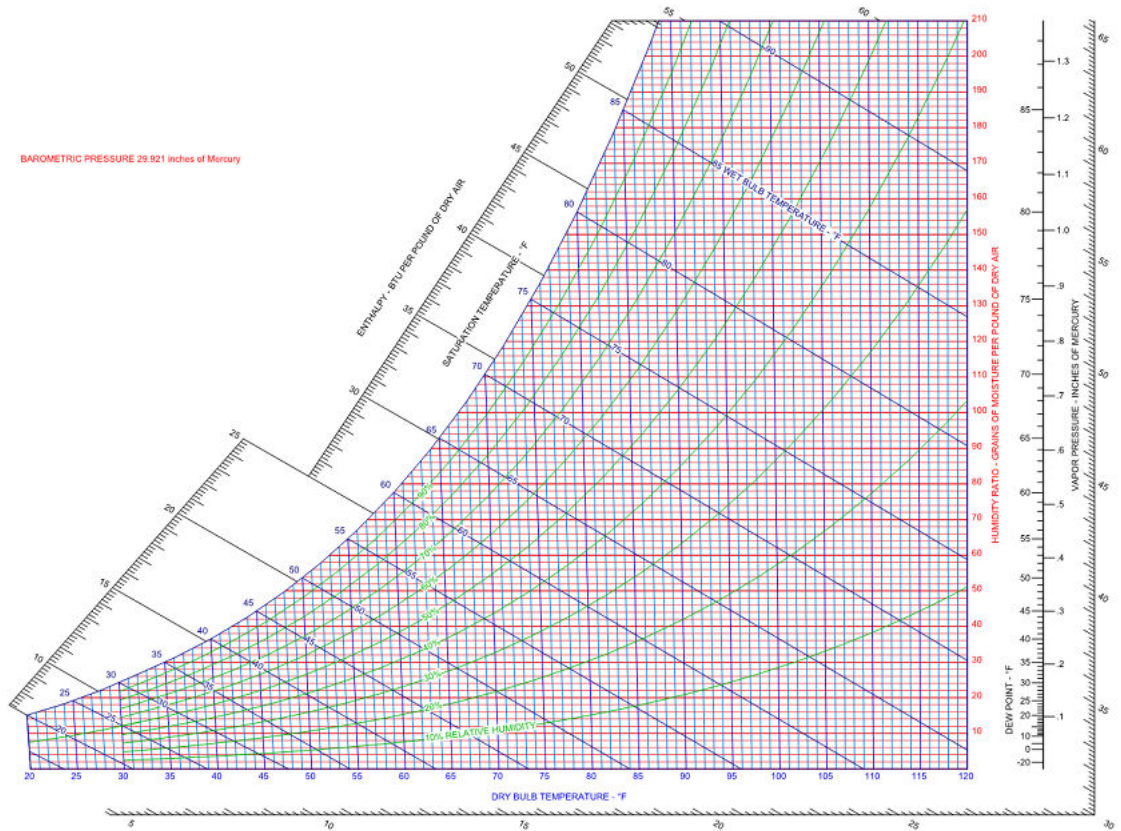
*Dry-bulb temperature* is the common temperature read by a thermometer exposed to the air, without taking into account the amount of moisture in the air. This measurement is the true thermodynamic temperature of the air. Changes in dry-bulb temperature correlate to changes in sensible heat added to or removed from the system.

As the name implies, *wet-bulb temperature* utilizes a small amount of moisture on the sensing bulb in the thermometer which—in addition to measuring the sensible heat—allows you to also measure the amount of latent heat in the system based upon how much water evaporates off the bulb and into the air. A very dry system will have a greater capacity to pick up water vapor. The water requires more heat energy to get to this higher energy state, so the bulb senses this as more heat energy leaving; thus the measured wet-bulb temperature will be something slightly lower than the dry-bulb temperature.


## Calculating Humidity and Dew Point


As an MCO technician, you should become familiar with using psychrometric charts to help you calculate humidity and dew point, especially when other calculation tools are unavailable. A psychrometric chart is a multi-axis chart with intersecting variables of humidity, dew point, temperature, and moisture content, relative to elevation, atmospheric pressure, and other environmental parameters. If you know at least two of the variables, you can find where they

intersect on the psychrometric chart and then determine where that point lies on the other axis to solve for the missing variable.



**Figure 4–5:** A psychrometric chart is a handy tool for calculating humidity or dew point if other variables are known. (Source: Logical Operations for NCMCO)

 **Note:** Calculating humidity and dew point can involve lengthy and complex mathematical operations and requires specific measurements that are not always available. This content does not cover all of these approaches, but there are plenty of websites, apps, tools, etc. that can solve for these missing variables when a few others are known (such as solving for humidity when temperature, dew point, and atmospheric pressure are available).

 **Note:** To further explore how to determine the humidity or dew point within your space, you can view the **Calculate Humidity and Dew Point Using a Psychrometric Chart** presentation from the Certified Mission Critical Operator Video Series.

## Fluids

A *fluid* is a substance that does not have a stable shape, flows with ease (relative to the surrounding environment), and is susceptible to external pressure changes. It is important to note that you shouldn't over-simplify the definition as "non-solids," because when looking at physical phases, some liquids may act like solids under particular conditions. However, for the purposes of MCOs, it is sufficient to mean "liquids and gasses" when you see or use the term "fluid."

## Pressure

*Pressure*, represented by the letter P, is the force applied to the surface of an object, measured by the unit area over which that force is distributed. There are three specific types of pressure that will be relevant to you as an MCO technician: fluid pressure, air pressure, and hydraulic pressure.

Fluid pressure is the force exerted by a fluid as a function of its weight. For instance, the pressure felt by a penny at the bottom of a one gallon bucket of water filled with a liquid will change based upon the density of that liquid. The density of that same liquid, filling that exact same space, will also be different based upon the temperature of that liquid and the air pressure pushing down on top of the bucket.



**Note:** Remember, weight is different than mass: mass is an absolute measure of the amount of "stuff" in a substance, while weight takes into consideration the effect of gravitational forces on that mass. It just so happens that the two are equivalent at sea level, since that is the basis for our scientific standards. This same holds true for fluids, as additional characteristics with identical measures—such as density, atmospheric conditions, fluid temperature, and so forth—can impact them in the same manner.

Air pressure (or atmospheric pressure) refers to the force exerted by the weight of air or any other gas, such as the mixture of gasses in our own atmosphere. Hydraulic pressure refers to the force exerted by the weight of any liquid (not just water).

## PSI

One of the most common measurements of fluid pressure is *Pounds per Square Inch (PSI)*. Just as the name states, this unit represents the force applied by one pound of weight evenly distributed over a surface area of one inch squared.

## PSF

Pounds per Square Foot (PSF) is another common (non-metric) measurement of pressure, most commonly used in low pressure applications such as rating an object for a maximum weight load. PSF is not often used in MCO scenarios, but if you ever encounter it as a unit of pressure, you should know how to convert it to the more commonly used measurement of PSI. 1 PSI equals 144 PSF, so to convert from PSF to PSI, use the following formula:

$$P(\text{PSI}) = \frac{P(\text{PSF})}{144}$$

## Inch of Water Column

An *inch of water column* is an English (non-SI) unit of pressure referencing the weight of a given amount of water. Specifically, it represents the pressure exerted by a column of water that is one inch in height under certain pre-defined conditions. It is used to measure small pressure differences, such as those that might occur across a pipe opening or within the pipeline itself.

## Flow

*Flow* refers to the volume of a fluid moving past or through a fixed point over a given period of time. The most common mechanical flow rate units you are likely to encounter as an MCO technician are gallons per minute (GPM), liters per minute (LPM), and cubic feet per minute (CFM or  $\text{ft}^3/\text{m}$ ).

	1 GPM	1 LPM	1 CFM
GPM		0.264	7.48
LPM	3.78		28.3
CFM	0.134	0.0353	

**Figure 4–6:** Here, you can see how to convert between the various units of flow. (Source: Logical Operations for NCMCO)

## Lead/Lag Cooling Systems

Lead/Lag cooling systems are terms MCO operators may likely run into when there are multiple and/or redundant sets of equipment installed. Lead/lag describes a system where one piece in a pair is operating normally (the lead component) and the second is ready in a standby condition in case it is called upon due to additional load (the lag component). This concept can apply to a system with numerous pieces of identical equipment; however, in a scenario with two out of four units running, there may not be a real "lead" unit and the "lag" or "standby" unit may actually just refer to the next unit in line that is ready to handle times of additional load.

# ACTIVITY 4-1

## Identifying HVAC Fundamentals

### Scenario

In this activity, you will identify fundamental concepts relating to heating, ventilation, and air conditioning (HVAC).

- 1. Which HVAC-related service is concerned with the cooling and humidity control of air used in people spaces or for critical equipment operations?**
  - Heating
  - Ventilation
  - Air conditioning
  - Cooling
- 2. Which fundamental HVAC concept refers to the addition or subtraction of heat energy that results in a physical temperature change?**
  - Latent heat
  - Dew point
  - Sensible heat
  - Humidity
- 3. Dry-bulb temperature measures both the sensible heat and the latent heat of a substance.**
  - True
  - False
- 4. Which HVAC-related service is concerned with the warming of air or water used in people spaces or for critical equipment operations?**
  - Heating
  - Ventilation
  - Air Conditioning
  - Cooling
- 5. Which fundamental HVAC concept refers to the amount of moisture suspended in a gas, such as air?**
  - Latent heat
  - Dew point
  - Sensible heat
  - Humidity
- 6. Which fundamental HVAC concept refers to the addition or subtraction of heat energy that occurs during a state change of a substance?**
  - Latent heat
  - Dew point
  - Sensible heat
  - Humidity

**7. What is heat?**

- The transfer of energy between two or more objects or substances, including that transferred through work.
- The transfer of energy between two or more objects or substances, excluding that transferred through work.
- The transfer of energy between two or more objects or substances, where the output is only warmed air or water for use in occupied spaces.
- The transfer of energy between two or more objects or substances, where the output is only heat energy used as a heat source for mechanical work.

**8. Which fundamental HVAC concept refers to the equilibrium temperature at which water vapor is absorbed by and condensed from the air at the same rate?**

- Latent heat
- Dew point
- Sensible heat
- Humidity

**9. Which HVAC-related service is concerned with the exchange of conditioned air used in people spaces or for critical equipment operations?**

- Heating
  - Ventilation
  - Air conditioning
  - Cooling
-

# TOPIC B

## Refrigerant-Based Cooling Systems

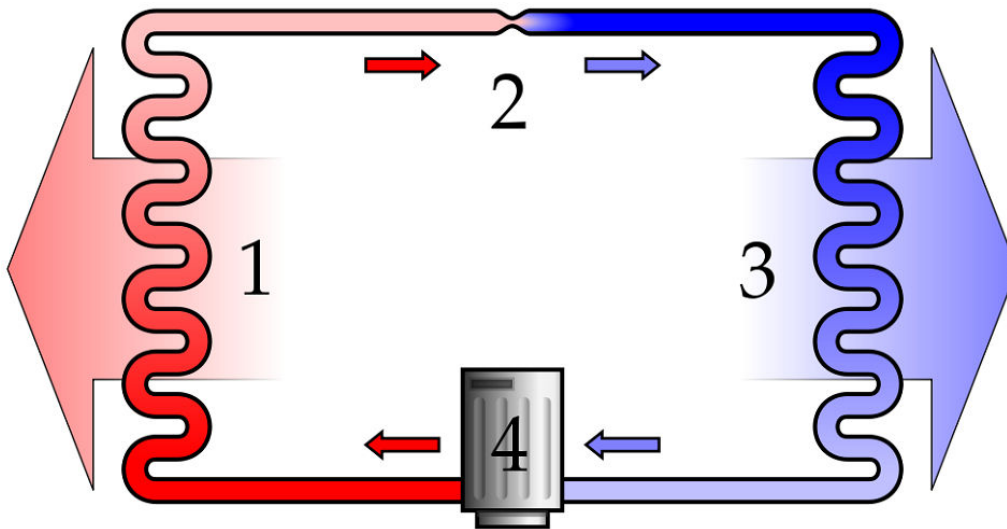
Whether it is to provide people comfort in occupied spaces or to ensure the proper operations of critical equipment, creating and maintaining optimal temperatures may fall under your responsibilities as an MCO technician. Sometimes, the concept of cooling is even more important than heating, as certain critical equipment has the potential to run so hot, it needs specific cooled temperatures to safely operate. In this topic, you will learn about one type of cooling mechanism—refrigerant-based cooling systems.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Chiller
- Air-cooled chiller
- Water-cooled chiller
- DX (direct expansion)
- Pumped refrigerant

### Chiller

A *chiller*, in general, is a cooling device that uses vapor-compression or an absorption cycle to remove heat from water, which is then typically piped into buildings and passed through heat exchangers—such as air handlers and fan coil units or other systems—in order to cool air or other equipment. There are numerous types of chillers, each with different characteristics, that may be used in an MCO facility.



**Figure 4-7:** A simple diagram of the vapor-compression refrigeration cycle where 1) is the condenser, 2) is the expansion valve, 3) is the evaporator and 4) is the compressor. Red is gas and pink is liquid at high pressure and high temperatures; blue is liquid and light blue is gas at low pressure and low temperature. (Source: Ilmari Karonen/Creative Commons (Public Domain)/<https://commons.wikimedia.org/wiki/File:Heatpump.svg>)

## Air-Cooled Chiller

An *air-cooled chiller* is a type of cooling equipment that removes heat from water and conducts it to the atmospheric air as the final stage in the heat rejection/cooling process. Air-cooled chillers are usually placed outside (but can operate indoors in a room with sufficient air exchange) and are cooled by fans driving air over the condenser coils.

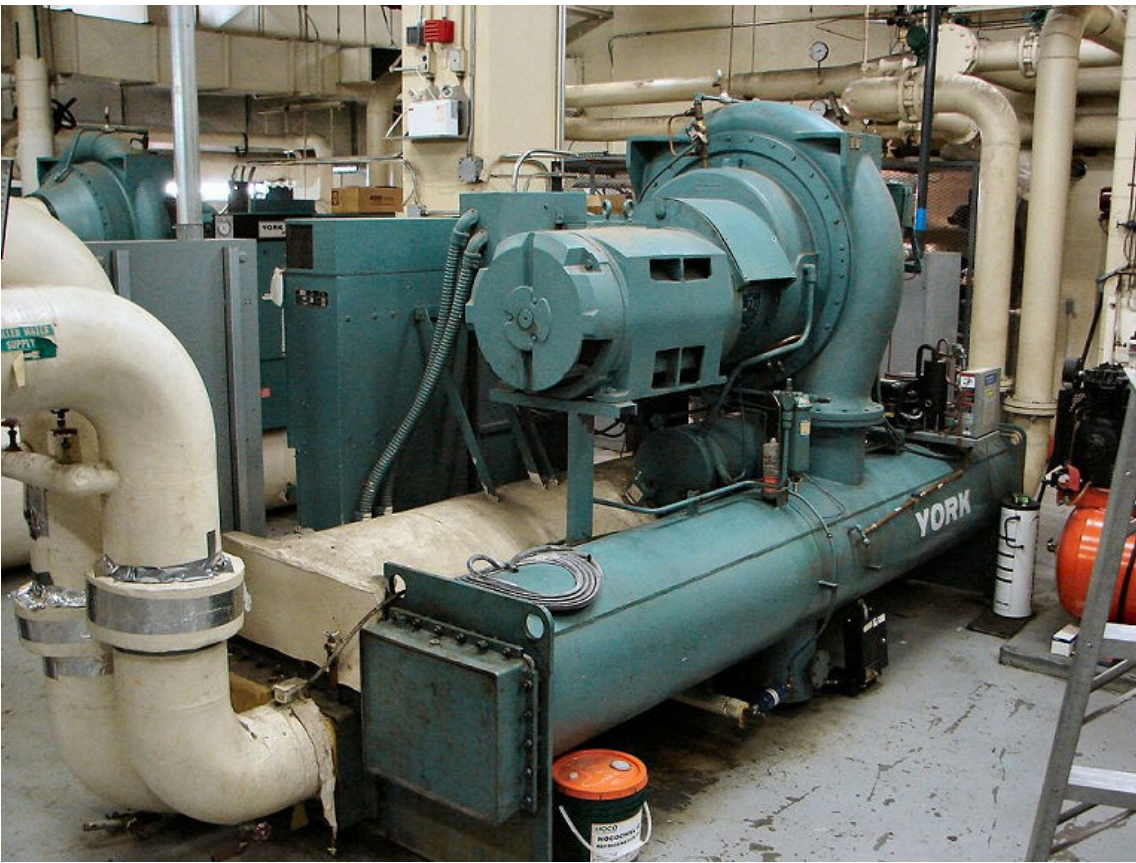


**Figure 4–8:** Workers guide a new air-cooled chiller into place for installation at a military base in Hawaii. (Source: United States Navy/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:US\\_Navy\\_100510-N-76290-003\\_New\\_air\\_conditioning\\_in\\_Hawaii.jpg](https://commons.wikimedia.org/wiki/File:US_Navy_100510-N-76290-003_New_air_conditioning_in_Hawaii.jpg))

## Water-Cooled Chiller

A *water-cooled chiller* is another type of cooling equipment that removes heat from water and conducts it to another source of water as the final stage in the heat rejection/cooling process. Water-cooled chillers are usually placed inside a building and the heat from these chillers is carried by re-circulating water to an outdoor cooling tower.





**Figure 4–9:** A centrifugal water-cooled chiller installed in a facility. (Source: P199/Creative Commons (Public Domain)/<https://commons.wikimedia.org/wiki/File:Chiller.jpg>)

## DX

*Direct expansion (DX)* is a type of cooling system that directly cools the supply air to an occupied space via the refrigeration cycle, where a refrigerant absorbs the heat directly from the air. DX units require a ventilation fan to distribute (supply) and recirculate (return) the cooled air, and are often split into systems or packaged units..

## Pumped Refrigerant

*Pumped refrigerant* refers to a type of cooling system that is a variation of the DX design. It cools the air by directly conducting heat from circulating air to a refrigerant loop. Within the loop, the bulk of the refrigeration cycle occurs in a central cooling device and then compressors pump the cooled liquid refrigerant throughout critical spaces in a closed loop with small sets of coils at desired cooling locations. This is sometimes referred to as "high-density" cooling, since a fairly precise, measured amount of cooling can be delivered to a very specific location.

## ACTIVITY 4-2

# Identifying Refrigerant-Based Cooling Systems

### Scenario

In this activity, you will identify the various types of refrigerant-based cooling systems.

---

- 1. Which type of cooling system directly cools the air being supplied to an occupied space by utilizing a refrigerant that absorbs the heat directly from the air?**
    - Air-cooled
    - Water-cooled
    - Direct expansion
    - Pumped refrigerant
  - 2. Which type of cooling system removes heat from water and conducts it to the atmospheric air, and then uses the cooled water in heat exchange systems to cool the air being supplied to occupied spaces or critical equipment?**
    - Air-cooled
    - Water-cooled
    - Direct expansion
    - Pumped refrigerant
  - 3. Which type of cooling system directly cools the circulating air in occupied spaces by moving cooled liquid refrigerant in a closed loop that contains small sets of coils at the desired cooling locations?**
    - Air-cooled
    - Water-cooled
    - Direct expansion
    - Pumped refrigerant
  - 4. Which type of cooling system removes heat from water and conducts it to another water source, and then uses the cooled water in heat exchange systems to cool the air being supplied to occupied spaces or critical equipment?**
    - Air-cooled
    - Water-cooled
    - Direct expansion
    - Pumped refrigerant
-

# TOPIC C

## Water-Based Cooling Systems

Refrigerant-based cooling systems are just one type of cooling system that could be implemented in your MCO facility. As an MCO technician, you will need to know about all the different common types of cooling systems, as you may be tasked with operating or maintaining a variety of equipment. In this topic, you will learn about another type of cooling system—water-based cooling systems.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Cooling tower
- Heat exchanger

### Primary Pumping Systems

A primary pumping system supports the flow demand for a primary cooling or process fluid loop. Primary pumping systems can be further classified as either manifold or dedicated systems. In a manifold system, pumps are installed in parallel together so more than one pump may be available for operational use or if maintenance issues arise. In a dedicated system, each pump is dedicated to a single loop.

### Variable Primary Pumping Systems

A variable primary pumping system, which is mainly used to chill water systems, varies the flow of water through the evaporator of the chiller to control the amount of water that is chilled, in order to be more efficient or in implementations where constant flow is undesirable or unnecessary. Variable frequency drives (VFD) installed on the primary fluid pumps vary the flow for the system in a finely scalable manner.

### Secondary Pumping Systems

The primary goal of a secondary pumping system is to deliver flow by maintaining a differential set point at one or more locations in the system. A secondary loop is normally supported by the secondary pump. Whether in an extra loop or tied directly into the primary fluid loop, secondary pumps are often referred to as "booster pumps" as they provide a little extra flow or pressure required by particular parts of the cooling systems.

For example, a secondary set of smaller pumps may be installed adjacent to a chiller lineup to run periodically when the chiller load jumps, allowing the primary pumps some time to catch up, without having to call for additional primary pumps or an increased energy demand.

### Cooling Towers

A *cooling tower* is a cooling device that rejects heat through the cooling of a water stream in a confined space, directly open to the atmosphere. Evaporation of water removes process heat and cools the working fluid to near the wet-bulb temperature. The evaporate clouds represent the excess latent heat that has been removed, but sensible heat is removed as well—only a small amount of the water actually evaporates. The rest of the cooler water moves back through the cooling system to remove heat again.

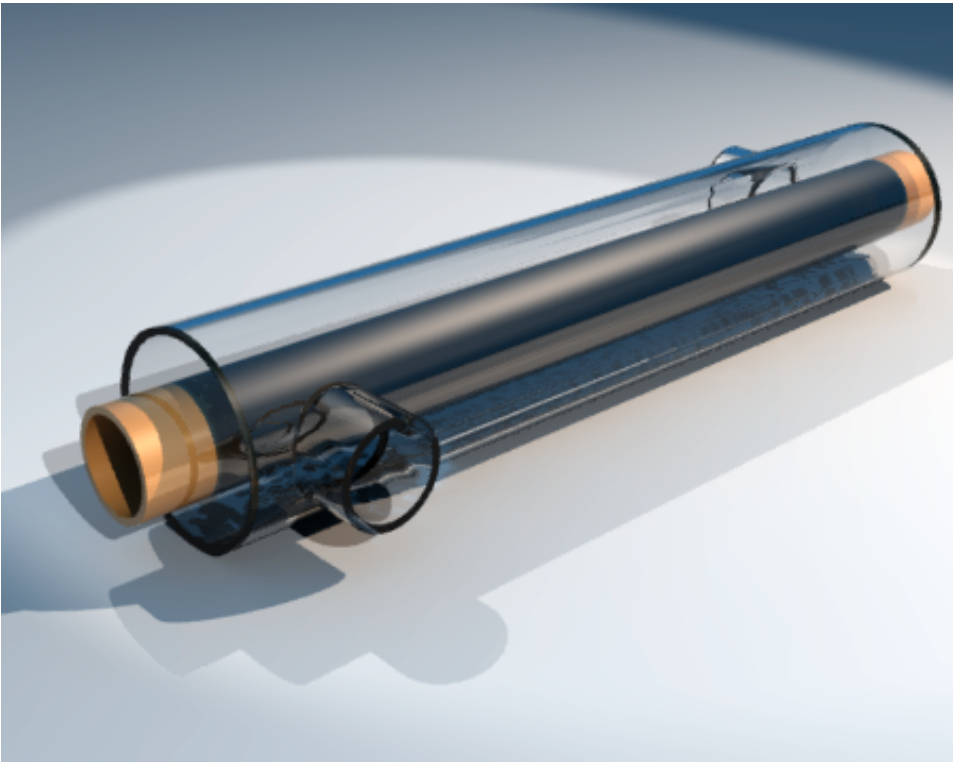
Large cooling towers of nuclear power plants often come to mind, but the basic design of any cooling tower is about the same, with the exception of the means for moving the water (pumps, gravity, spray, etc.).



*Figure 4–10: HVAC cooling towers on top of a shopping mall remove heat from the facility. (Source: Ingolfson/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Loop\\_Shopping\\_Centre\\_Exterior\\_1.jpg](https://commons.wikimedia.org/wiki/File:Loop_Shopping_Centre_Exterior_1.jpg))*

## Heat Exchangers

A *heat exchanger* is a cooling device that allows heat from a fluid to pass to a second fluid without the two fluids coming into contact. Shell and tube heat exchangers or plate and frame heat exchangers are the two most well-known designs within MCOs, but your average automobile radiator is a common example as well.



**Figure 4-11: A shell and tube heat exchanger.** (Source: KoenB/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Tubular\\_heat\\_exchanger.png](https://commons.wikimedia.org/wiki/File:Tubular_heat_exchanger.png))

## Thermal Storage and Reuse

Thermal storage and reuse refers to the maintenance of a reserve energy transfer source, typically in the form of chilled water storage tanks. Large volumes of cooling fluid are stored at normal operating temperatures such that, in the event of a failure of the cooling mechanism (chiller, condenser, etc.), this mass of cool water may be circulated throughout the system until it removes so much heat that it reaches equilibrium with the critical infrastructure being served. This buys MCO operators some amount of time to take action and restore the cooling mechanism or protect critical equipment from overheating. Thermal storage and reuse practices are usually applied to systems with low temperature heating or high temperature cooling.



**Note:** The same principle works in reverse for hot water storage, but this is a less common MCO application.

## Freeze Protection

In any facility where water-based cooling systems are in place, freeze protection is of equal importance because it provides dedicated protection against low temperature conditions to piping, valves, condensate systems, solar systems, safety showers, fire lines, spray nozzles, cooling coils, and other mechanical equipment that is used for moving water-based fluids.

Freeze protection applications can be mechanical, chemical, or operational in nature. Mechanical protection would be things like heat trace, in which wires are run along piping, tanks, and other components and are energized during low temperature conditions (very much like the defroster on vehicle rear windows).



**Figure 4-12: A self-regulating heat tracing wire is run alongside a copper pipe to provide freeze protection. (Source: z22/Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:Self-regulating\\_heat\\_tracing\\_tape.jpg](https://commons.wikimedia.org/wiki/File:Self-regulating_heat_tracing_tape.jpg))**

Chemical protection refers to the addition of anti-freeze solutions to the cooling system fluid (glycol-based substances being most common) which actually lower the freeze point of the fluid depending upon the concentration of the solution.

MCO technicians and operators can also take manual action to mitigate risk of freeze damage by periodically running pumps (even if not needed for cooling) or cycling isolation valves. Keeping the fluid moving adds some amounts of energy (translated to nominal temperature change) and prevents ice from forming at points in the system particularly exposed to the elements.

# ACTIVITY 4–3

## Identifying Water–Based Cooling Systems

### Scenario

In this activity, you will identify the various types of water-based cooling systems.

1. Which type of cooling system allows heat from one fluid to pass to another fluid, without the two fluids coming in contact with one another?
  - Cooling tower
  - Primary pump
  - Heat exchanger
  - Variable primary pump
2. Which type of cooling pump system changes the flow of water that is pumped through the chiller to control the amount of water that is chilled?
  - Primary pumping system
  - Secondary pumping system
  - Variable pumping system
  - Variable primary pumping system
3. Which type of cooling system uses evaporation to remove the heat from water within a confined space, and releases the excess heat as evaporate directly into the atmosphere?
  - Heat exchanger
  - Thermal storage
  - Cooling tower
  - Secondary pump
4. Which type of cooling pump system provides extra flow or pressure required by particular parts of the cooling system?
  - Primary pumping system
  - Secondary pumping system
  - Variable pumping system
  - Variable primary pumping system
5. In an MCO facility using a water-based cooling system, periodically running pumps or cycling isolation valves are actions that should be taken in order to provide which of the following preventative measures?
  - Thermal storage
  - Temperature maintenance
  - Freeze protection
  - Heat exchange

6. Which type of cooling pump system provides the flow of fluid needed to support the demand from a primary cooling or process fluid loop?
- Primary pumping system
  - Secondary pumping system
  - Variable pumping system
  - Variable primary pumping system
7. In an MCO facility using a water-based cooling system, maintaining large volumes of cooling fluid stored at normal operating temperatures is part of which of the following preventative measures?
- Thermal storage
  - Temperature maintenance
  - Freeze protection
  - Heat exchange
-



# TOPIC D

## Alternative Cooling Systems

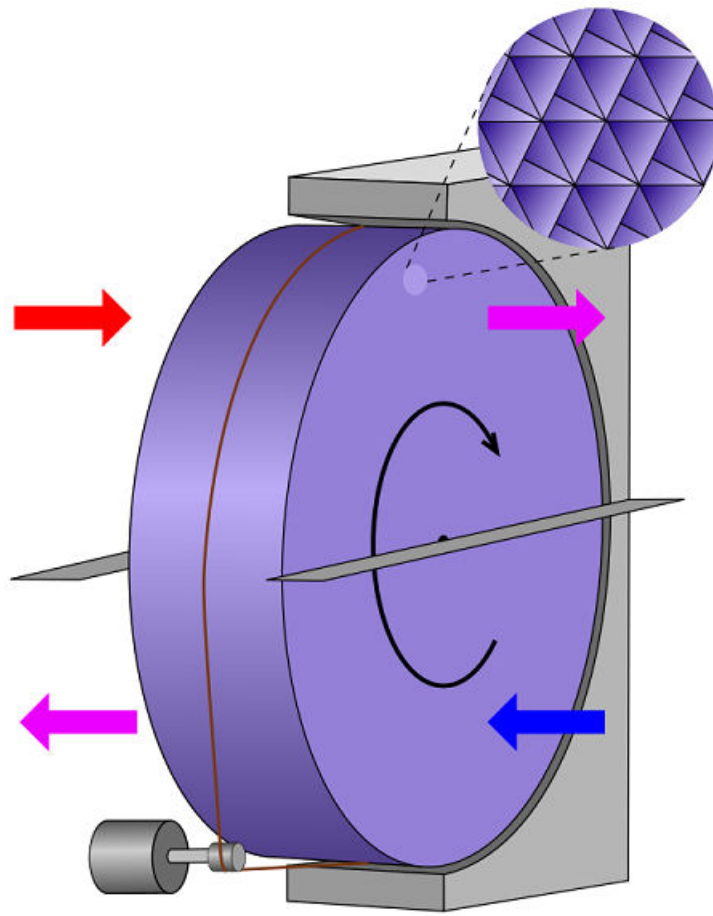
In addition to the more commonly used cooling mechanisms that fall under the refrigerant-based and water-based categories, there are a variety of alternative cooling mechanisms. As a Mission Critical Operator, you will need to have working knowledge of all of the available cooling systems that may be implemented in an MCO facility. In this topic, you will learn about that alternative types of cooling systems.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Thermal wheel
- Air-side economization
- Free-air cooling
- Geothermal cooling
- Evaporative cooling

### Thermal Wheel Cooling

A *thermal wheel* is a cooling system that uses a rotating wheel made of a conductive material to reject heat, usually in a two-stage process. Think of it as a rotating heat sponge that has air flow dividers creating two halves of the system. Exhaust air from other MCO systems is blown through one half, transferring some amount of heat energy to the wheel and leaving in a cooler condition for reuse. As the wheel turns, that part of it that was just heated rotates to the other half where another air stream (usually outside air being circulated through) blows through the wheel, removing the added heat and exiting the system. That part of the wheel rotates back down, in a cooler state, to the first half of the system to receive more heat. The wheel can be driven by force (motors, gears, pulleys, etc.) or be driven by the movement of the air through it, much like a turbine.



**Figure 4–13:** A diagram of how a thermal wheel operates. (Source: Tomia/Creative Commons (CC BY-SA 3.0)/<https://commons.wikimedia.org/wiki/File:Rotary-heat-exchanger.svg>)

## Air-Side Economization

*Air-side economization* is an energy efficient cooling process that uses supply and exhaust fan systems to circulate outside air through a facility for critical space cooling. This generally means using non-conditioned air (whatever the external ambient conditions may be) but may include some means of supplemental humidification or dehumidification. Although those supplemental systems do require energy, the design intent is primarily to remove the standard refrigeration/cooling systems that consume large amounts of energy.

Since the outside air must be a cooler ambient temperature than that of the recirculated air in the facility for air-side economization to work properly, it may not be practical for all MCO facilities. Depending upon the level of ambient condition stability that is required for the critical spaces, outside temperature vs. facility temperature will become a large factor in site selection considerations, so that an appropriate climate area may be chosen if this is to be included in the design.

## Free-Air Cooling

The term *free-air cooling* is often used interchangeably with air-side economization, but it really refers to the most pure form of outside air usage. Ideally speaking, this means no supplemental air-conditioning equipment is used, and to the greatest extent possible, natural air circulation is utilized in place of fan-driven air circulation. For this reason, systems using free-air cooling are sometimes referred to as 100% fresh air technology.

## Geothermal Cooling

*Geothermal cooling* is a type of cooling system that uses the earth as a heat sink instead of cooling tower or other final-stage cooling equipment. The heat rejection is delivered by moving warm air or water from above ground through a geothermal heat pump to a set of coils or simply through a large loop where the ground itself absorbs the excess heat. Cooled air or water is returned to the surface and used as a primary or secondary means of cooling critical spaces.

## Evaporative Cooling

*Evaporative cooling* is a type of cooling system that reduces temperature by removing the latent heat from an object by using the evaporation of a liquid coolant, usually water. This cooling method uses much less energy than refrigeration. Cooling potential is also dependent on the wet-bulb depression; the difference between dry-bulb and wet-bulb temperatures. An evaporative cooler—also known as swamp cooler, desert cooler, or wet air cooler—is normally used in very dry climates to provide air or water cooling.



**Figure 4-14:** An evaporative cooler hangs off the side of the building in Colorado, where drier conditions allow it to be used as a source of cool air. (Source: Billy Hathorn/Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:Evaporative\\_cooler,\\_CO,\\_IMG\\_5681.JPG](https://commons.wikimedia.org/wiki/File:Evaporative_cooler,_CO,_IMG_5681.JPG))

## Approach Temperature

An approach temperature is the difference (or delta) in temperature between coolant inlet streams of flow versus capacitor outlet streams of flow (e.g., ambient air or cooling water). The closer the delta, the more effective the system will be. A prime example are chiller approach temperatures: evaporator approach is the difference between the temperature of the evaporating refrigerant (measured at the well in the evaporator) and the temperature of the chilled water exiting the system;

condenser approach is the difference between the temperature of the liquid refrigerant (measured on the liquid line) and the temperature of the condenser water exiting the system.

# ACTIVITY 4-4

## Identifying Alternative Cooling Systems

### Scenario

In this activity, you will identify the various types of alternative cooling systems.

1. Which type of cooling system sends warmed air or water into the ground, where its heat is absorbed by the earth, and then delivers cooled air or water to the surface for cooling purposes?
  - Thermal wheel
  - Free-air
  - Geothermal
  - Evaporative
2. Which type of cooling system circulates non-conditioned outside air using existing system fans throughout the facility for cooling purposes?
  - Evaporative
  - Air-side economization
  - Free-air
  - Geothermal
3. Which type of cooling system uses a rotating device that first passes warmed exhaust air over a conductive material to absorb the heat, disperses cooled air for reuse, and turns the device; then, it passes circulated air over the conductive material to absorb the heat, and turns the device again?
  - Geothermal
  - Evaporative
  - Air-side economization
  - Thermal wheel
4. Which type of cooling system circulates the naturally cooler outside air to provide cooling for a facility?
  - Evaporative
  - Air-side economization
  - Free-air
  - Geothermal
5. Which type of cooling system removes heat by dispelling the humidity in a liquid coolant?
  - Evaporative
  - Geothermal
  - Thermal wheel
  - Air-side economization

# TOPIC E

## Air Circulation

While heating and cooling mechanisms are important parts of any HVAC system, that conditioned air will go nowhere without the help of the ventilation system. As an MCO technician, you will need to know the various types of air circulation systems and how they operate. In this topic, you will identify the various air circulation systems and their components.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Fan system
- Exhaust system
- Heat recovery system
- Air handling unit
- Blower
- Heating element
- Cooling element
- Sound attenuator
- Air filter
- Damper
- DOAS (dedicated outdoor air system)
- RTU (rooftop unit)
- AR unit (air rotation unit)
- Terminal unit
- Ductwork

## Fan Systems

A *fan system* refers to a very broad category of equipment used to circulate air throughout MCO infrastructure. Fans rarely work as a standalone unit, instead requiring ductwork, direction vanes, control dampers, etc. to accomplish the design intent, so that's why we look at it from a system perspective. People have been moving air for comfort and industrial use for thousands of years, so it is understandable that there are numerous types of fans and system design options. Selection of a specific type of fan and/or fan system depends upon necessary criteria such as air speed, air volume, air pressure, flow patterns, and more.

You are likely to encounter the following types of fan systems in MCO facilities.

<b>Fan System</b>	<b>Description</b>
Axial/Propeller	<p>In an axial or propeller fan design, the air flows in and out of the fan parallel to the shaft and blades, in a straight line through the fan blades themselves. The housing can be made with blades that can be adjusted when running to retain high efficiency. Table fans, box fans, and even ceiling fans are all examples of this type of fan.</p> <p>Axial/Propeller fans are most commonly used in implementations where moving large volumes of air are more important than trying to impart pressure or velocity.</p>

<b>Fan System</b>	<b>Description</b>
Centrifugal	<p>With centrifugal fans, the air flows in a radial direction relative to the shaft, which means that air blows out at a right angle to the air intake. There are actually four classifications of centrifugal fans, based on the blades and direction of movement within the wheel. The fans used in blow dryers, inflator fans/air pumps, and the large "squirrel-cage" fans you see in industrial fan systems are all examples of this type of fan.</p> <p>Centrifugal fans are most commonly used in implementations where imparting speed and/or pressure is more important than moving large volumes of air.</p>
Mixed/Cross-flow	<p>Mixed or Cross-flow fans can be of many different designs, but are distinctly classified because the air flows inward in an axial direction (parallel to the fan shaft) and then outward in a radial direction (at a right angle to the air intake). Small-scale fans of this nature are used for cooling circuit boards in computers and amplifiers; larger-scale fans of this nature (though still relatively compact) are used almost exclusively for HVAC purposes.</p> <p>Mixed/Cross-flow fans are most commonly used in implementations where imparting speed and/or pressure and moving large volumes of air are both important.</p>

## Exhaust Systems

An *exhaust system* is a mechanical discharge system where the air is removed from a building and discharged outside the building at a specific location or to a specific distance where it cannot again be readily drawn back in by the ventilation system. Examples of exhaust equipment and/or systems include clothes dryers, smoke purge, refrigeration discharge, machinery room discharge, battery room discharge, and air-side economizer discharge.



**Figure 4–15:** A whole house fan, seen here prior to installation, is used as the exhaust mechanism to help circulate the air in a home or other structure. (Source: Piercetheorganist/Creative Commons (CC BY 3.0)/<https://commons.wikimedia.org/wiki/File:Whole-house-fan-pre-install.JPG>)

## Heat Recovery Systems

A *heat recovery system* is the collection of equipment—such as a heat recovery ventilator, heat exchanger, air exchanger, and so on—that recycles the waste heat that is a by-product from the operation of equipment or machinery and uses it in another critical process, such as heating water or air.

## Air Handling Units

An *air handling unit* is another broad category of HVAC equipment, but refers to the collection of devices that drive the flow of conditioned air in HVAC systems. It is a central unit consisting of a blower, heating and cooling elements, sound attenuators, filter racks, dampers, humidifiers, and other equipment that comes in direct contact with the air flow.



**Note:** Ductwork is not considered part of the air handling unit, and will be covered separately.



<b>Component of an Air Handling Unit</b>	<b>Description</b>
Blower	A <i>blower</i> , generally a centrifugal fan, is a mechanical device for moving air or gases. What makes a centrifugal fan a blower is that its intake and exhaust are ducted, providing more control of desired air pressures, speed, etc. They can be belt driven or direct drive with designs that are sturdy, quiet, reliable and capable of operating over a wide range of conditions.
Heating and Cooling elements	A <i>heating element</i> is a coil or other arrangement of wires in which heat is produced by an electric current. A <i>cooling element</i> is generally the sets of coils or vanes through which the cooling medium flows to remove heat from the air.
Sound Attenuators	<p>Sound Attenuation is a design approach used to safely manage noise levels that are or would be uncomfortable or damaging to human hearing. A <i>Sound attenuator</i> is a material or device used to provide noise dampening within the air handling unit, typically installed within the duct system to absorb the sound. Thermal insulation materials in ductwork may provide a dual-purpose in sound attenuation, but additional material, such as rubber isolations at support attachment points, helps to better mitigate transmission of vibrations.</p> <p>In HVAC equipment, materials like wallboard (we prefer not to have flammable material in units, although wood is often found in older equipment) is added to paneling because typically sheet metal enclosures clearly don't trap sound well.</p>
Filters	<p>Filtering is the process by which a liquid or gas is passed through a material designed to remove impurities. While there are often filters installed in refrigeration lines or cooling water systems, <i>air filters</i> are the most commonly used in MCOs.</p> <p>Air filters are typically classified by the size of particulate they can remove from the air and/or their performance at a given particulate level. For example, a filter may be effective down to particulate of .1 mm in size, allowing no more than 100 ppm (parts per million) to pass through. High-quality filtration regularly found in MCO installations is commonly categorized by a MERV (Minimum Efficiency Rating Value) rating, which is a system of measurement based on the size of particulate captured (measured in microns) under worst-case conditions.</p>
Dampers	A <i>dampener</i> is a valve or plate that stops or regulates the flow of air inside a duct, chimney, VAV terminal unit (also known as a VAV box), air handler, or air handling equipment. Dampers are commonly used to regulate room temperature and climate control.

## DOAS

A *dedicated outdoor air system (DOAS)* is a type of HVAC system that consists of two parallel systems: a dedicated outdoor ventilation system for latent loads and a parallel system for sensible loads. The system must be decoupled between latent and sensible loads. The supply air dew point temperature must be suppressed more than is typically used in the more conventional variable air volume (VAV) systems that serve multiple zones. One downfall of this system is that cooling and dehumidifying the outside air in the summer and humidifying and heating it in the winter is a very energy-intensive method.

## Rooftop Units

*Rooftop units (RTUs)* are a packaged air handling unit that includes all of the necessary air handling components, usually mounted on a curb or slab on the roof of the facility. There are two common RTU designs: either a recirculating design or a one-time-through design.



**Figure 4–16:** A rooftop air handling unit. (Source: P199/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Rooftop\\_Packaged\\_Units.JPG](https://commons.wikimedia.org/wiki/File:Rooftop_Packaged_Units.JPG))

## Air Rotation Units

An *air rotation (AR) unit* is designed as an alternative to a rooftop unit and functions using the basic premise of "hot air rises and cool air settles." AR units pull the return air in at floor level using continuously running fans, and then directs that air back into the space, typically near the ceiling. The return air section, near the floor, has a thermostat that measures air temperature and will function to heat or cool the air to maintain a constant temperature in the space.

Due to the lack of ductwork, a lower horsepower fan motor can be used compared to that used with a conventional rooftop unit. However, an air rotation unit is best suited for buildings with high ceilings, like a warehouse or manufacturing space; buildings with a 12-foot-high ceiling or lower are physically not tall enough to project the air away from the unit, which will cause it to short cycle.

## Terminal Units

A small air handler used more locally, such as at the specific location where air handling is needed, is called a *terminal unit* (sometimes referred to as a fan coil unit). A terminal unit may only include an air filter, cooling coil and blower, and is typically used at more remote portions of the HVAC system for either additional air circulation or for fine-tuning the conditioned air delivery.

There are two main types of terminal units:

- A fan-powered terminal unit is used as a way of cooling and periodically heating the perimeter zones of a building using a single duct control system. If heating is required, the supplementary

heating coils may be activated. Fan-powered terminal units are available in two configurations. In Series (Constant Volume), the fan sits in the primary air stream and runs constantly when the zone is occupied. In Parallel (Variable Volume), the fan sits outside the primary air stream and runs intermittently.

- A Variable Air Volume (VAV) box can be used as a terminal unit. While the VAV is not technically adding additional conditioning to the air delivery, it does aim to control the air qualities of a specific, localized environment.

## Ductwork Systems

*Ductwork* refers to the system of pipes or tubes that transport and deliver conditioned air throughout a facility. There are two types of ductwork systems: flexible and rigid. Flexible ducts are made from fabrics coated with rubber or polyvinyl chloride, a non-flammable substance. Rigid ducts are typically made using galvanized steel, aluminium, or fiberglass and offer many benefits: they are suitable for underground transport, have lower resistance to flow than flexible duct, and are less likely to leak than flexible ducts. There are also duct socks, which are fabric air dispersion systems and can be permeable or non-permeable. They are often used as an alternative to galvanized steel spiral ductwork.



**Figure 4-17: Ductwork transports conditioned air within a facility. (Source: Jeff\_Hu/iStock/Thinkstock)**

Ductwork systems are insulated to varying degrees based upon the surrounding environment. If noise is not a large concern, or the delta between ambient air and the conditioned air is not great, the majority of the duct system may just be sheet metal and some flexible ductwork. On the other hand, if cool, dry air is required in an otherwise hot and humid ambient environment, the ductwork could be lined in its entirety with some manner of insulation, such as foam (most common) or rubber.

# ACTIVITY 4–5

## Identifying Air Circulation Systems and Components

### Scenario

In this activity, you will identify the different types of air circulation systems and their components.

**1. Which of the following components typically make up an air handling unit?**

- Blowers
- Ductwork
- Heating or cooling elements
- Terminal units
- Sound attenuators
- Dampers
- Filters
- Thermostats

**2. Which category of air circulation system is used to move only the conditioned air inside a building or structure?**

- Heat recovery system
- Exhaust system
- Air handling unit
- Ductwork system
- Fan system

**3. Which category of air circulation system is used to circulate both the conditioned and unconditioned air inside a building or structure?**

- Air handling unit
- Fan system
- Exhaust system
- Ductwork system
- Heat recovery system

**4. Which category of air circulation system reuses the heat that is created from the operation of facility equipment or machinery to heat the air or water for the facility?**

- Fan system
- Air handling unit
- Ductwork system
- Exhaust system
- Heat recovery system

5. Which category of air circulation system delivers the conditioned air throughout a building or structure through a series of pipes or tubes?

- Air handling unit
- Fan system
- Ductwork system
- Exhaust system
- Heat recovery system

6. Which category of air circulation system removes air from a building or structure and discharges it to a location and distance where it won't be drawn back into the larger air ventilation system?

- Ductwork system
  - Exhaust system
  - Heat recovery system
  - Air handling unit
  - Fan system
-

# TOPIC F

## HVAC Preventative Maintenance

Now that you can identify all of the various components of HVAC systems, you need to think about how you will maintain all of these components to ensure proper operations of the entire system. Since the HVAC system provides such important services to your mission critical facility—heating, cooling, and air circulation to both people spaces and critical equipment spaces—preventative maintenance helps ensure that all of these integral parts are working as efficiently as possible.

As an MCO operator, it is highly likely that your responsibilities will include completing these types of tasks. In this topic, you will identify the preventative maintenance procedures for HVAC systems and their components.

### Filter Maintenance

Filter maintenance is a vital regular maintenance function in MCOs because clogged, dirty filters can block airflow and reduce a system's efficiency significantly. Some filters are reusable and can be rinsed out, while others will need to be replaced each time. Filters may need more frequent attention if the air handler or air conditioner is in constant use. It is a good practice to monitor, analyze, and trend your filter usage for the first year (at least), and then set up a preventive/predictive maintenance schedule based on those trends. Replacing old filters can cause energy consumption to decrease by five to fifteen percent just from changing a dirty filter with a clean one!

Visual inspection can be a trigger to complete filter maintenance—clogged filters will appear dirty and could physically collapse if they become too “loaded”—but this can be time-consuming if filters are not easily accessible/visible. Remote monitoring comes in handy here as the differential air pressure (commonly referred to as d/p) across the filter will increase as the filter gets loaded towards the end of its useful life. At a minimum, MCO technicians should always consider installing inexpensive analog d/p gauges locally so they can keep an eye on filter performance during rounds or other maintenance activities.

### Coil Maintenance

Both evaporator and condenser coils collect dirt over months and years of service, and regular preventative maintenance can help keep them working properly. There are a few tasks that should be performed as part of preventative coil maintenance:

- While proper filter changes can prevent the evaporator coil from soiling as quickly as the condenser coil, dust is always going to be present in the air and the evaporator will still collect dirt. Evaporator coils need to be checked and cleaned at least once a year.
- Condenser coils can easily become dirty if the outdoor environment is dusty, polluted, or there is foliage around. Best practice for MCOs is to keep the area around the condenser free of debris and foliage at least two feet in all directions. Frequency of cleaning will be determined by the environment, but at least one cleaning a year is recommended.
- Coil fins should also be inspected; if they are bent, they can block air flow instead of directing it. MCO technicians can use a fin comb to get them close to their original condition.



**Figure 4-18:** Corrosion can occur on evaporator coils if not properly maintained. (Source: *Chinesedrywall/Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:Effects\\_of\\_Chinese\\_Drywall.jpg](https://commons.wikimedia.org/wiki/File:Effects_of_Chinese_Drywall.jpg)*)

## Belt Maintenance

Regular belt maintenance is necessary for air handlers that are belt driven. When belts wear out they will break or begin slipping and you will lose efficiency. There are a couple of actions that should be performed as part of preventative belt maintenance:

- Since an important component of the belt system is the sheave—the pulley system with a groove that holds the belt while it spins to turn the motor—whenever you are changing or maintaining your equipment's belts, you should also perform a sheave inspection and replace if necessary.
- Alignment is critical to the blower motor and all associated parts. Misalignment will cause abnormal wear on belts and sheaves, and can cause nuisance breakdowns which will eventually lead to failure.
- Tension of the belt is also important: too tight causes bearing wear and eventually bearing failure; too loose causes slippage, excessive wear, and loss of efficiency. Technicians should always have a belt tension checker tool and a pulley alignment tool on hand—both are affordable and readily available at any HVAC supply store.

## Testing, Adjusting, and Balancing

Testing, adjusting and balancing (TAB) are the major preventative maintenance steps you should follow to achieve proper operation of your HVAC systems. The tools and measurements may differ, but the approach and necessity for TAB holds true for air and liquid systems.

Testing is based upon the flow values from the mechanical engineering of the system, based on the system design. During this step, you use specialized and specifically calibrated instruments to

measure certain operating conditions for the HVAC system, such as temperature, pressure, or velocity.

Adjusting refers to dialing in the final balancing settings for system equipment (such as dampers), adjusting fan speeds, and/or calibrating automatic controls such as thermostats and flow controllers in order to achieve the specified performance and efficiency for normal operations.

Balancing is the method of evaluating and regulating system flow to achieve the most even, efficient design conditions for the system.



## ACTIVITY 4-6

### Identifying HVAC Preventative Maintenance Procedures

#### Scenario

In this activity, you will identify the appropriate preventative maintenance procedures for HVAC systems and their components.

1. **Which type of preventative maintenance for HVAC systems involves checking the alignment and tension levels of the key components that keep air handlers moving air in the system, and inspecting and replacing related components in this equipment, such as sheaves?**
  - Filter maintenance
  - Coil maintenance
  - Belt maintenance
  - Testing, adjusting, and balancing
  
2. **Which type of preventative maintenance for HVAC systems involves checking, cleaning, and (as needed) replacing the components of the HVAC system that remove impurities that may disrupt the air flow in the system?**
  - Filter maintenance
  - Coil maintenance
  - Belt maintenance
  - Testing, adjusting, and balancing
  
3. **Which type of preventative maintenance for HVAC systems involves completing a multiple-step process that measures, calibrates, evaluates, and regulates the various components to optimize system operations?**
  - Filter maintenance
  - Coil maintenance
  - Belt maintenance
  - Testing, adjusting, and balancing
  
4. **Which type of preventative maintenance for HVAC systems involves checking, cleaning, and (as needed) replacing the components of the HVAC system that provide the heating or cooling mechanism for the system?**
  - Filter maintenance
  - Coil maintenance
  - Belt maintenance
  - Testing, adjusting, and balancing

## Summary

In this lesson, you identified and described the fundamental concepts of heating, ventilation, and air conditioning—most commonly known as HVAC—and the critical components that make up an HVAC system, particularly as they apply to a mission critical facility. Having a strong understanding of heating, cooling, air conditioning, and air circulation, as well as the components that are used to provide these services in your facility appropriately, will help you properly manage the important ambient conditions of your MCO facility.

# 5

# Mission Critical Infrastructure: Plumbing and Other Mechanical Systems

## Lesson Objectives

In this lesson, you will identify and describe plumbing and other mechanical systems present in a mission critical facility. You will:

- Identify water supply and drainage systems and their components.
- Identify secondary mechanical systems and their components.
- Identify preventative maintenance procedures for plumbing and other mechanical systems and their components.

## Lesson Introduction

As noted, there are a few critical systems that will be found in every single Mission Critical Operations (MCOs) facility you might encounter—HVAC is one, and plumbing is another. Every facility will rely on the water supply and waste removal that a plumbing system provides. In addition, there are numerous other kinds of secondary mechanical systems that you may come across as an MCO operator, directly related to the kinds of services or products that the MCO facility provides.

As such, as an MCO operator, you will need to understand the various components of the water supply and drainage system and the other mechanical or secondary systems that might be present in a facility, and how to properly maintain those components for continued operations. In this lesson, you will identify and describe plumbing and other mechanical systems present in a mission critical facility.

# TOPIC A

## Water Supply and Drainage

Regardless of the purpose of the MCO facility, one of the key systems necessary for the proper functioning of a facility is the plumbing and drainage system. Every facility needs water coming in and going out of the building, whether it is solely for people use or for use within the facility's critical components. As an MCO technician, you will need to have a strong understanding of the systems that work together to bring water into the facility for use and remove it from the facility once it has been used. In this topic, you will identify the water supply and drainage systems and their various components.

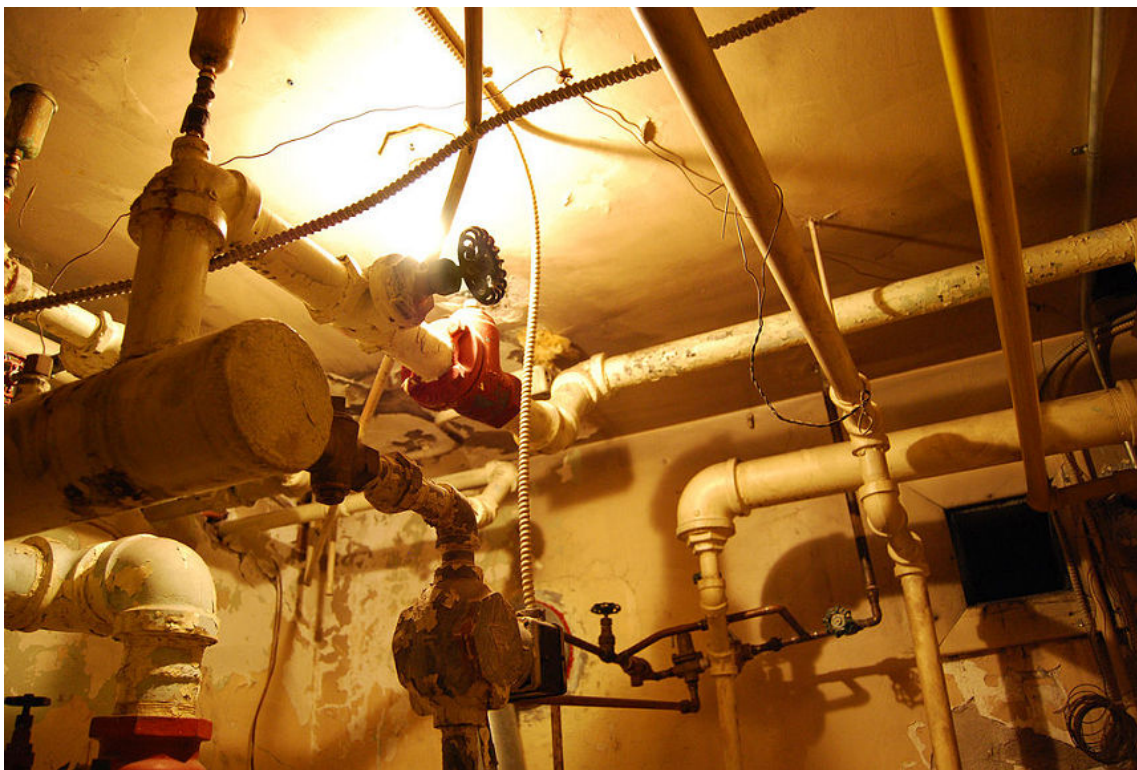
The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Plumbing
- Graywater
- Effluent
- Drainage
- Makeup water
- Backflow prevention

### Plumbing

General *plumbing* refers to the system used to transport, capture, and remove miscellaneous fluids throughout a facility, including supply water or potable water, *graywater* (the relatively clean wastewater generated from sinks, showers/baths, dishwashers, washing machines, etc.), sewage or *effluent* (often called blackwater), and other waste drainage.

Plumbing systems consist mostly of pipes, valves, drains, and other fixtures that are involved in the movement of fluids, and the occasional holding tank for storing them. The fluids being delivered are generally pressurized, so pumps are not frequently found on the supply side of the plumbing system; however, it is a bit more common to find pumps on the return/drain/waste side of the plumbing systems, particularly if the effluent is being pulled from a sump.



**Figure 5-1: The various pipes, pumps, valves, and other components of a plumbing system.**  
 (Source: Tjmhay/Creative Commons (Public Domain)/[https://en.wikipedia.org/wiki/File:Pipes\\_various.jpg](https://en.wikipedia.org/wiki/File:Pipes_various.jpg))

## Water Sources

Water of different qualities is used throughout MCO facilities. Potable water refers to a quality of water safe for human consumption (faucets, drinking fountains, etc.) but is often used for showers and toilets. Non-potable water includes two categories of water of a lesser quality: water that is not designed for human consumption but could be used for outdoor fixtures, irrigation, or flushing toilets; or water collected onsite that is not necessarily hazardous, but is not treated in any manner to ensure it is safe for ingestion.

When it comes to the sources of these various types of water, there are four main supply sources that you should be familiar with.

<b>Water Source</b>	<b>Description</b>
Municipal	Municipal water supply is the same utility supply that also ends up in residential settings, although some locations may have specific industrial municipal supplies (for instance, if the scale of use and demand characteristics are sufficiently different to justify the cost of a municipality building and operating a second system). Acknowledging the waste when it comes to cost and energy for using potable water to flush toilets and water landscaping, most utilities in the United States are very slow to consider providing any lower quality sources for these non-people uses.

<b>Water Source</b>	<b>Description</b>
Reclaimed	Reclaimed water refers to water that has already been delivered to and possibly used in the facility, and has been captured and/or reused within the facility. This could mean using water from sinks or shower drains for irrigation, capturing HVAC condensate for use in flushing toilets, collecting rainwater for watering landscaping, or a host of other combinations.
Stored	Water may be stored onsite in quantities from hundreds of gallons to hundreds of thousands of gallons. Reclaimed water may be stored for future use since it is not always collected in the same quantity or rate that it will be used. Potable water may also be stored onsite, but it is important to understand and designate what the intended use is. If the utility-supplied water is simply being stored for refilling equipment, landscaping, or other miscellaneous usage, the quality of the storage tank or the water treatment considerations are not a high concern. On the other hand, if the intent is to store water for people use, the cleanliness of the tanks is critical, and regular testing of water quality (at least a frequently as required by local jurisdictions) and some chemical treatment or filtration may be required.
Well	An MCO design may also take advantage of well water, but usually only for use in secondary plumbing systems. Even if it has been verified that the well taps into a large, sustainable water table, the potential for interruption of water supply must be taken into consideration; for instance, if damage were to occur to the shaft due to seismic activity, the time it takes to dig and connect a new well can be lengthy. MCO personnel can deal without indoor plumbing for a bit, but critical equipment that uses water for supplemental functions simply can't afford the downtime.

## Drainage

Plumbing systems don't always use water in a straight pass, so as it is dispersed and used, it must then be collected. *Drainage* refers to the collection of components that remove the surplus water or effluent from the plumbing system.

There are numerous components that make up a drainage system:

<b>Drainage System Component</b>	<b>Description</b>
Floor drains	Floor drains are typical for general use and may be used regularly for cleaning and washdown, or for any overflow or leaks that could occur in fluid systems. Floor drains usually connect into common headers underneath the main structure (or flooring for multi-story facilities), all installed at a slight angle to encourage gravity draining to a main exit point from the property.

<b>Drainage System Component</b>	<b>Description</b>
Traps	<p>Drain traps are fixtures in the piping, near open drains, that create a water seal between the drain system and the atmosphere. Since many drains run out through sewage connections, you don't want sewer gases coming back up through dry traps, which is both a comfort and a safety issue.</p> <p>Part of the water path through the trap runs lower than the drain piping, preventing a small slug of water from being able to completely drain. During use, this slug is pushed out through the trap, but replaced by the last bit of water running through the drain.</p> <p>Traps are mostly classified by the shape of the water path through the piping of the trap—P, S, or U—with P-traps being the most common in the US.</p>
Trap primers	<p>Even with a properly installed drain trap, the fluid slug in an infrequently used trap could simply evaporate. To address this occurrence, trap primers may be installed in such systems. There are many types of devices, piping designs, and/or valves used as trap primers, but they all perform the same function—keep liquid in the trap. This could be a small line connected to nearby fixtures that use water regularly (sink, drinking fountain, etc.) or a piped connection to the main water supply that pulls a small amount of liquid into the trap when the liquid level in the trap drops below a certain level.</p>
Fluid-recovery drains	<p>Fluid-recovery drains refer to any type of drain that directs fluid for collection or reuse, rather than just piped out of the facility with sewer or other wastewater connections.</p>
Dedicated chemical drains	<p>Some drains are designed to catch only a specific type of effluent, such as a chemical or other (potentially) hazardous fluid, so they need to be segregated from the facility's main drainage system. These may be pumped to other areas for treatment, or simply to a holding tank that needs to be emptied/hailed away when filled.</p>

## Drainage Documentation

In an ideal situation, there should be adequate documentation—design drawings are generally acceptable—that captures the number of drains in the plumbing system and describes how they all connect. Some designs allow for more emergency drains to be connected to a common drain header in larger numbers than regular drains due to the unlikeliness of all of them being utilized at once. If permitted by local authorities, this is fine, but later construction efforts may overlook this criteria, and think they can use any drain they can find for new equipment going in.

## Makeup Water

*Makeup water* refers to the water supplied for equipment that consumes water in some form, whether it is discharged, evaporated, or flushed—all typical functions of systems other than a closed-loop system.

While the makeup supply could be for critical equipment or general building machinery, makeup water isn't often included in the primary critical design considerations. Critical equipment that does require some sort of makeup source should have internal storage design characteristics, assuming that a loss of makeup water supply is possible while still needing to serve its design purpose.

## Water Treatment and Filtration

Aside from the noted needs associated with potable water, mechanical systems that require a water supply may call for additional treatment or filtration due to sensitivity to a particular contaminate or the quality of supplied water. There are two common types of treatment processes for these kinds of water: blowdown and chemical treatment.

Blowdown refers to a water treatment process that may also be called "flush and fill." In blowdown, used, dirty, or otherwise standing water is drained from the component or system, and new water is added. Variations could involve multiple flushes, drying time, or even cleaning cycles.

Chemical treatment is always a consideration for fluid systems to improve fluid quality, prevent undesirable buildup, or maintain some specific characteristic of the fluid. Even potable water tends to have trace amounts of minerals in it that are perfectly fine for humans; however, if that water was left even partially stagnant in equipment, those chemicals could cause build-up that could hamper operations—particularly any heat transfer applications.



**Note:** It should be noted that chemical treatment is not always indicated in information provided by manufacturers. The astute MCO technician should always be on the lookout for deficiencies in fluid systems and proactively search out products to combat the problem. There are many surface coatings, for instance, that prevent buildup of almost anything, but are not installed on equipment at the factory.

## Pumps and Pressurization

While pressure is the natural and primary force that moves fluids through a system, there is generally a need to create or add to the differential pressure (possibly created by gravity, heat, or some other system processes) to help those fluids move more efficiently within the system. Pumps are the common means of taking some external energy source—usually electricity, but sometimes compressed air, steam, or some other rotational force—and convert it to a rotational or compression force to push fluid through the system.





**Figure 5-2:** A small, electric-powered pump can add pressurization—and therefore increased fluid movement—within the plumbing system. (Source: KVDP/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Jet\\_pump.jpg](https://commons.wikimedia.org/wiki/File:Jet_pump.jpg))

## Pressure Variations Throughout the Various Plumbing and Mechanical Systems

MCO operators need to understand the requirements of all systems, but with secondary mechanical systems in particular, there may be multiple pieces of equipment that are being served by a single supply source, but operate with different characteristics—such as varied pressure. Shared systems should take into consideration the most limiting factor. In the case of water supplies, for example, a piece of rooftop mechanical equipment might require the highest supply pressure, which could exceed the municipal utility supply especially if lower elevations systems are concurrently drawing off the water. To combat this situation, we might need a booster pump installed, or maintain a holding tank on the roof above the unit to provide pressure.

Due to the varied nature of supplemental mechanical systems, it can be hard to get a holistic operational view of how they all work together, collectively. Pressure gauges on secondary systems, for instance, are important devices within the system that are often left off of the controls and monitoring systems. This heightens the need for awareness of MCO operators and/or necessitates the idea for investigating how to get them connected for remote monitoring.

## Backflow Prevention

An important addition to the plumbing system is *backflow prevention*, which refers to the protective devices installed that fully segregate operational systems from the supply in order to prevent any sort of backwards or upstream contamination of the water supply. Backflow prevention is required and regulated mostly by local (i.e., city or county) jurisdictions and usually requires inspection and maintenance by a certified or licensed technician.

Backflow devices are generally differentiated based upon operational pressures and pipe volume or flowrates. Although design and construction has become nuanced with more products on the market, the basic concept involves a check-valve installed in the device that allows flow in only one direction. In some instances, backflow devices can act as pressure control, in order to prevent back pressure damage, but this is more easily and effectively accomplished with pressure relief valves.



**Figure 5-3:** Check-valves keep the flow of the plumbing system moving in one direction. The arrows on these check valves show the direction that fluid is moving. (Source: The Alloy Valve Stockist (Heather Smith)/Creative Commons (CC BY 3.0)/[https://commons.wikimedia.org/wiki/File:Swing\\_Check\\_valves.JPG](https://commons.wikimedia.org/wiki/File:Swing_Check_valves.JPG))

# ACTIVITY 5-1

## Identifying Water and Drainage Systems and Their Components

### Scenario

In this activity, you will identify water and drainage systems and their various components.

---

- 1. Which concept of water supply and drainage refers to a type of water treatment where used or dirty water is removed from a system while new, clean water is added?**
    - Reclaimed water
    - Backflow prevention
    - Blowdown
    - Makeup water
  - 2. Which concept of water supply and drainage refers to the inclusion of protective devices that segregate operational systems from the water supply in order to prevent contamination of the water supply?**
    - Reclaimed water
    - Backflow prevention
    - Blowdown
    - Makeup water
  - 3. Which concept of water supply and drainage refers to a water supply source where water that has been delivered and/or used in the facility is captured and reused within the facility?**
    - Reclaimed water
    - Backflow prevention
    - Blowdown
    - Makeup water
  - 4. Which concept of water supply and drainage refers to water that is supplied for equipment that consumes water in some form, such as evaporation?**
    - Reclaimed water
    - Backflow prevention
    - Blowdown
    - Makeup water
-

# TOPIC B

## Secondary Systems

While the plumbing system is arguably one of the most important systems in MCOs, providing water for both people use and critical system use and removing wastewater, there are numerous other systems that are integral to the proper functioning of a specific facility. For some MCOs, there are very specific resources that must be supplied to the facility for it to continuously provide its critical services or products. As an MCO operator, you need to have working knowledge of all of these various secondary systems and the purposes they serve. In this topic, you will identify secondary mechanical systems and their components.

## Vacuum Systems

In reference to secondary systems, especially operationally-speaking, a vacuum system refers to a physically isolated system or component that operates at pressures lower than atmospheric pressure. Although there are thermodynamic means of creating vacuums, MCOs typically use an air pump or compressor to remove gasses from the system.

One regular use of a vacuum system in MCO installations is to provide cleaning functions. For example, consider a piece of machinery with fine tolerances and many small moving parts; maintaining a vacuum within its casing can help remove any dust or contaminate particles that might cause damage. Loosely speaking, air cleanliness is another issue MCOs address with vacuums. For highly critical exhaust functions, the design may call for something stronger than a simple fan to more fully remove smoke, toxic by-products, etc., from the air in critical spaces, and a vacuum system can perform that function well.

Additionally, some specialty equipment use vacuums to perform its function. If you recall, lowering system pressure on a fluid—which can be done via a vacuum—lowers its phase change temperatures; under those conditions, you could boil a fluid at a lower temperature or keep a substance in its liquid state through lower temperature ranges. For instance, consider a vacuum evaporator, which is sometimes used to treat industrial wastewater. A vacuum evaporator reduces the pressure in the tank below the vapor pressure of the liquid, allowing the liquid to evaporate at a lower temperature.



*Figure 5-4: A vacuum evaporator. (Source: Condorchem/Creative Commons (CC BY-SA 3.0)/ [https://commons.wikimedia.org/wiki/File:Vacuum\\_evaporation\\_plant.jpg](https://commons.wikimedia.org/wiki/File:Vacuum_evaporation_plant.jpg))*

## Compressed Air Systems

Compressed air systems create and deliver pressurized air for general use or specialized equipment functions. One or more air compressors pressurize and filter the air and send it to a holding tank (or receiver) prior to the system distribution piping. The purpose of the receiver is to maintain some volume of pressurized air ready for use, as well as help absorb fluctuations in demand by either acting as a buffer if demand spikes due to a large, quick draw on the system, or by receiving output from the compressor while it's shutting down and demand has already dropped off. Compressors should be maintained in accordance with the manufacturer's recommendations, including performing periodic piping inspections that focus on leak checks at accessible joints.



**Figure 5–5: An air compressor station creates and delivers pressurized air for use in a power plant. (Source: Sensenschmied/Creative Commons (CC BY–SA 3.0)/[https://commons.wikimedia.org/wiki/File:Kompressorstation\\_mit\\_Druckluftspeicher.jpg](https://commons.wikimedia.org/wiki/File:Kompressorstation_mit_Druckluftspeicher.jpg))**

## Process Water Systems

*Process water* refers to water that serves a very particular function for an MCO facility, and therefore will have specific characteristics needed for proper system operation. To do so, process water may need to be strictly treated and controlled to obtain a very high level of purity or to maintain a particular pH. The need for process water is more frequently tied to manufacturing environments for washing and rinsing, formulation and mixing of specific solutions, and many other chemistry-related functions.

On the back-end of operations, process water systems may be required because of the nature of the solution after a mission critical process has occurred. General de-ionized or even tap water may be fine to supply to something like a nuclear reactor, but it's the characteristics of the effluent that require strict controls to manage, purify, or dispose of properly. The process water will pick up hazardous properties that need to be treated with more sensitivity than general drainage systems.

## Chilled Water Systems

While chilled water is notably a regular component of both critical and/or primary systems, there are many ways chilled water systems show up in secondary or non-critical systems within MCO installations. Their purpose remains the same: providing a medium with which to remove heat, especially when there are large quantities of HVAC and/or refrigeration equipment onsite.

When looking at the total picture, the need for redundancy and reliability is not nearly as high since it's just a cooling system for general purposes or for support equipment. As such, MCO operators are likely to see chilled water (for these functions) provided as a central service for all facilities if the MCOs reside in campus-style settings.

## Humidity Control Systems

Humidity control systems vary in style and scale, but all boil down to adding and/or removing moisture from the air in critical spaces. Common types of supplemental humidification systems include mist or spray systems integrated within air handling equipment or ultrasonic humidifiers. De-humidification is accomplished by either using a desiccant-type system (a substance that has the ability to absorb large quantities of water molecules) or condensing systems that pass air over cool surfaces (like chilled water or refrigerant coils) to draw moisture out of the air.



**Figure 5-6:** A large, industrial strength dehumidifier helps moderate the humidity levels for a building. (Source: jim pruit/iStock/Thinkstock)

For instance, an MCO facility with a lot of computers and electronics (such as a data center) tends to work within a fixed relative humidity range; too much moisture in the air can damage circuit boards, while air that is too dry increases the buildup of static electricity that can cause shock or equipment damage hazards. A humidity control system is imperative for this facility, to add or remove moisture to the air as needed to maintain a constant, consistent humidity level that allows for optimal operations.

## Natural Gas Systems

The use of natural gas systems occurs throughout many MCO facilities and they serve many purposes: from general heating, to firing boilers, to other specialized manufacturing processes. While natural gas systems typically don't have many other components in the system beyond the gas lines that deliver the gas to the equipment, it is crucial for MCO technicians to maintain awareness of their presence in the facility. Simply put, the consequences of a leaking valve or pipe joint are much more serious for gas lines than chilled water or air systems.



**Figure 5–7: Natural gas pipes and valves in a building. (Source: tdhster/iStock/Thinkstock)**

MCO operations personnel should conduct regular inspections of natural gas systems at least annually to verify the integrity of its connections and to inspect the general condition of piping. Additionally, audits should be performed to ensure that all locations with gas lines, particularly those hidden by structural components (such as walls, ceilings, raised floor, etc.) are properly marked, so that repairs to adjacent equipment do not end in disasters. Operators should also be intimately familiar with all isolation points and main facility shutoff valves.

## Other Compressed Gas Systems

The use of other compressed gasses—anything aside from natural gas or plain pressurized air, essentially—will be unique to certain types of MCO installations. Some common examples of other gasses being used in MCOs include:

- R&D or manufacturing facilities often use a variety of gasses in their production processes.
- Hospitals often have centralized oxygen systems for patient treatment.
- Many MCO facilities use nitrogen generation systems, as nitrogen is a valuable asset as an inert gas.

## Radiation Systems

Radiation systems are another secondary system that MCO technicians are likely to encounter. Radiation may be an inherent product of the critical system or generated for specific use. For instance, medical and research facilities commonly use radiation on a daily basis for diagnosis or treatment, and large-scale communication centers use broadcast equipment that generates large amounts of radiation. MCO technicians generally don't work on the radiation sources directly (nuclear power plant operators aside); however, as the owners of the facility at large, MCO operators do need to be aware of these systems and will likely be responsible for maintaining support equipment for the system such as radiation shields, emergency power, and other safety features.





**Figure 5–8:** An x-ray machine is a common implementation of radiation systems in a facility.  
(Source: Olga355/iStock/Thinkstock)

## ACTIVITY 5-2

# Identifying Secondary Systems and Their Components

### Scenario

In this activity, you will identify secondary systems and their various components.

---

1. **Which secondary system is used to supply water to the facility that has very specific characteristics that are necessary for proper operations?**
  - Chilled water
  - Process water
  - Vacuum
  - Radiation
  
2. **Which secondary system is used to provide a supply of gas to the facility that can be used for heating, powering equipment, or other manufacturing purposes?**
  - Vacuum
  - Compressed gas
  - Natural gas
  - Compressed air
  
3. **Which secondary system is used to manipulate pressure levels in order to allow components or equipment to perform certain tasks under specific atmospheric conditions, such as lower temperatures?**
  - Compressed gas
  - Process water
  - Humidity control
  - Vacuum
  
4. **Which secondary system is used to create and deliver pressurized and filtered air for general use or specific equipment functions?**
  - Vacuum
  - Compressed gas
  - Compressed air
  - Humidity control
  
5. **Which secondary system is used to create and maintain proper atmospheric moisture levels in a critical space?**
  - Humidity control
  - Process water
  - Compressed air
  - Vacuum

6. Which secondary system is used to supply water to the facility that has very specific temperature characteristics in order to remove heat from critical components or spaces?

- Humidity control
  - Process water
  - Vacuum
  - Chilled water
-

# TOPIC C

## Plumbing and Other Mechanical System Preventative Maintenance

Now that you know about the various plumbing and other secondary systems that you may encounter in an MCO facility, you need to be prepared to keep those systems working properly in order for the MCOs to provide critical services or products. Since water supply, drainage, and other mechanical systems are integral for the facility to function, following preventative maintenance procedures and schedules helps to ensure that all the critical components are online and operating at their optimal conditions.

As an MCO operator, your responsibilities will likely include completing these preventative maintenance tasks. In this topic, you will identify the preventative maintenance procedures for plumbing and other mechanical systems and their components.

### Rounds and Readings

In regard to preventative maintenance for plumbing and other mechanical systems in MCOs, rounds and readings are the fundamental best practice for MCO operators and technicians. Rounds and readings refers to actually going around to the various plumbing or other mechanical systems to check the necessary components and read their available outputs to make sure they are functioning properly. This physical check is important for secondary or non-critical mechanical systems which may not have all of the digital or remote monitoring features installed and/or available, as compared to power distribution systems and equipment. It, therefore, takes human sets of eyes, ears, and noses to monitor and maintain these systems. To the greatest extent possible, rounds should be taken daily (once a shift or more, if possible, for more critical equipment) to interact with every operating mechanical system at the MCO facility.

Keeping operational logs is often a matter of debate amongst MCO leaders, but—regardless of whether or not all readings are recorded, trended, and analyzed—the simple act of making the effort to write down a condition being observed further reinforces the MCO technician's familiarity and understanding of systems. The specific operating parameters (temperature, pressure, etc.) of mechanical equipment may vary greatly depending upon level of use, as do the more qualitative aspects like sound and smell. If you don't observe the equipment regularly, how would you learn to know if a pump is just more noisy at a certain speed, or if a bearing is starting to go bad? By capturing these varying conditions over time, it is more likely that you will notice specific variations that could point to a potential failure in the system before it happens.



**Figure 5–9:** An MCO technician performs rounds and readings for the components in a boiler room. (Source: Dmitry Kalinovsky/iStock/Thinkstock)

## System Inspections

General mechanical system inspections broadly refers to performing recommended preventative maintenance procedures based on operating manuals and/or guidance from other documentation provided by the manufacturer. These preventative maintenance tasks are classified as inspections because, generally speaking, there may not be very many moving parts to take apart, or the level of criticality of the system simply doesn't warrant taking the time out of an MCO technician's busy schedule to do a deeper dive.

Inspections always start with a visual check of the cleanliness, safety, and working order of accessible system components. Items that are most likely to wear—such as o-rings, gaskets, filters, etc.—should be specifically inspected and replaced at the slightest level of concern. Any available operational logs should be reviewed and real-time "running checks" of the equipment should be compared against normal operating ranges and specifications, such as temperatures, pressures, flowrates, and so forth.

System inspection preventative maintenance should be scheduled with the same rigor and regularity as that for more critical systems in the facility. You don't want to put a critical piece of equipment in jeopardy just because you forgot to put a drainage system back online, for instance, and allowed condensate to back up into a primary A/C unit.

## Filter Maintenance

In addition to the necessity of filter maintenance for HVAC equipment, other MCO mechanical infrastructure—that which can be more loosely defined as components that improve or preserve the quality of moving fluids—has a variety of filter maintenance needs.

MCO technicians are likely to encounter fluid filters throughout other mechanical systems, excluding systems whose sole purpose is to purify a process liquid (those systems should have highly specific maintenance procedures). For instance, fluid pumps may have low-level filters or strainers

installed at their suction points. Depending upon the frequency of system operation and criticality, miscellaneous fluid filters may be checked and/or cleaned on a quarterly basis, but certainly no less frequently than annually.

Fluid filters are not the only type of filtration that may support plumbing or other mechanical systems, though; air filters that are ancillary components should also be checked and maintained. For instance, air-cooled mechanical equipment generally has some type of filtration, such as the crankcase breather on an air compressor, or the engine oil/engine coolant systems on a generator. You could also add to this list all sorts of manufacturing equipment with moving pieces or tight tolerances for operation. The list is exhaustive, and highly dependent upon the specific MCO installation, but in most cases, these are filters that MCO operators and technicians should check at least semi-annually, even if the filters themselves may go a year or two without replacement.

Regardless of the filter type, it is important for operators to maintain as much equipment documentation as possible, so that manufacturers' recommendations for preventative maintenance for all critical components are known and followed by facility personnel.

## ACTIVITY 5–3

### Identifying Plumbing and Other Mechanical System Preventative Maintenance Procedures

#### Scenario

In this activity, you will identify the appropriate preventative maintenance procedures for plumbing and other mechanical systems and their components.

- 
- 1. In general, how often should you perform filter maintenance for the air and fluid filters used in plumbing and other secondary systems?**
    - Daily
    - Weekly
    - Monthly
    - Quarterly or semi-annually
    - Yearly
  - 2. In general, how often should you perform rounds and readings for the components used in plumbing and other secondary systems?**
    - Daily
    - Weekly
    - Monthly
    - Quarterly or semi-annually
    - Yearly
  - 3. In general, when performing regular system inspections as part of preventative maintenance for plumbing or other mechanical systems, what kinds of information should you reference or keep in mind during your inspection?**
    - Building plans or blueprints
    - Operating manuals
    - Operational logs
    - Maintenance schedules
    - System design specifications
    - Other manufacturer documentation
-

## Summary

In this lesson, you identified and described the plumbing and other mechanical or secondary systems that you may encounter in an MCO facility, particularly as they apply to the continued operations of the facility. Having a strong understanding of these various systems and their components will help you ensure that your MCO facility is always operating safely and efficiently, and can continue to provide the critical products or services to the community at large.



# 6

# Mission Critical Infrastructure: Fire Safety, Systems, and Equipment

## Lesson Objectives

In this lesson, you will identify and describe the fire safety, systems, and equipment integral to a mission critical facility. You will:

- Identify fire detection systems and their components.
- Identify fire suppression systems and their components.
- Identify the components of a fire-safe facility.
- Identify exit and emergency lighting options.
- Identify emergency power off systems.
- Identify preventative maintenance procedures for fire systems and their components.

## Lesson Introduction

In a facility where operations are critical, it is equally as important that there is infrastructure in place that will protect the people and critical equipment in the event of an emergency, such as a fire or electrical event. There are numerous components and devices that are part of the fire detection and suppression systems that provide the necessary preventative and protective services should such a hazardous event take place.

As an MCO operator, you need to be very familiar with these systems, their components, and how to properly maintain them to ensure that they are operating properly—and subsequently allow for your facility to operate safely and efficiently. In this lesson, you will identify and describe the fire safety, systems, and equipment that are integral to a mission critical facility.

# TOPIC A

## Fire Detection

The threat of fire is a serious concern to both the people and equipment within an MCO facility. Regardless of what products or services it provides, every facility needs to have fire detection systems in place to recognize smoke or fire and notify facility personnel of the emergency as soon as possible. As an MCO operator, you need to know the various components of the detection and alarm systems, and how they work together in the event of a fire. In this topic, you will identify fire detection systems and their components.

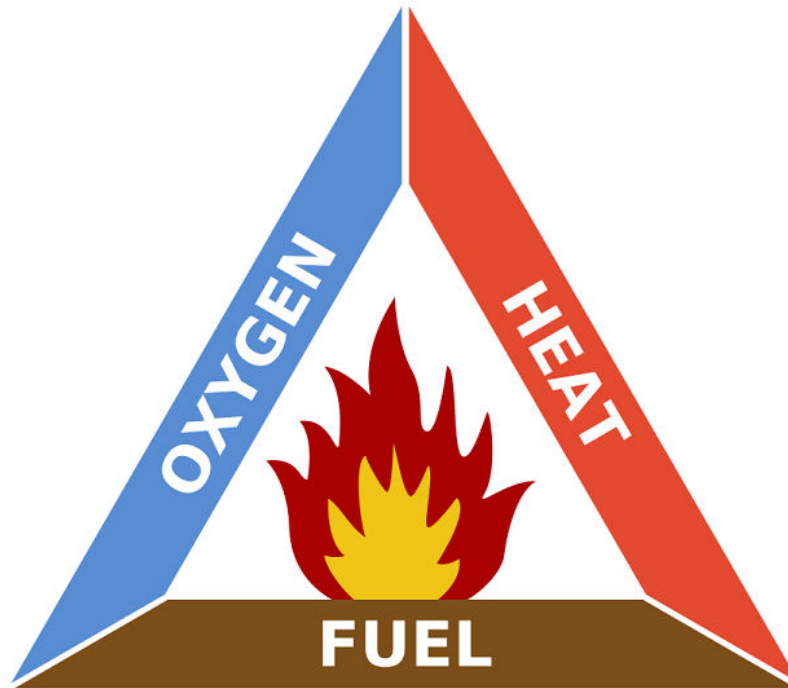
The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Fire triangle
- Fire detection
- Fire alarm

## The Fire Triangle

The *fire triangle* is a simple representation of the three elements required for fire:

- Heat (as the source of ignition).
- A fuel source (such as a combustible material or chemical).
- An oxidizing agent (usually, the oxygen in the air).



**Figure 6–1: The fire triangle.** (Source: Gustavb/Creative Commons (CC BY–SA 3.0)/[https://commons.wikimedia.org/wiki/File:Fire\\_triangle.svg](https://commons.wikimedia.org/wiki/File:Fire_triangle.svg))

Fire occurs in the presence of the fire triangle components once they reach appropriate levels. This mixture varies based on environmental conditions and the fuel source. We call it combustion because fire just "happens" once this precise mixture of conditions is reached, even if it looks like something "sparked" the fire.

For example, in taking a match to a candle, it's not the fire on the match head itself that ignites the candle, but the addition of sufficient heat (from the burning match) to the fuel (the candle wick) and oxidizing agent (atmospheric O<sup>2</sup>). This is an important distinction to understand and remember because we fight fires not by knocking down flames, but by stifling or removing one (or more) of the three elements of the fire.

## Fire Detection

As a concept, *fire detection* refers to sensing the presence of one or more of the by-products resulting from a fire, including smoke, heat, infrared or ultraviolet light, and even gas. Under the umbrella term of fire detection systems, there are a number of specific detection systems that monitor for and alert personnel when those conditions are present in a facility.

## Smoke and Heat Detection

Smoke and heat detection are the primary functions of fire detection systems. Depending upon the nature of the event, one may more noticeably precede the other. For instance, electrical wiring usually has a rubber or plastic based insulation which has a high tendency to smolder under steadily increasing temperatures prior to full ignition. In this case, smoke detectors would likely be the first to catch an alarm. Alternately, specific MCOs might call for construction materials that emit little to no smoke when burning, or the velocity of airflow through an area may be great enough that smoke will not rise directly to a smoke detector. In this case, heat detectors will be the first to respond. Heat detectors can be mechanical in nature, like the small glass bulb that bursts in a sprinkler head, or electronic, like a thermocouple.



**Figure 6–2:** A typical smoke detector, installed on the ceiling. (Source: Tumi-1983/Creative Commons/CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:Smoke\\_detector.JPG](https://commons.wikimedia.org/wiki/File:Smoke_detector.JPG)

## High-Sensitivity Smoke Detection

High-sensitivity smoke detection devices are exponentially more sensitive than traditional detection devices, allowing them to sense the presence of smoke much earlier and in much smaller quantities. The drawback here is that, under normal atmospheric conditions, the air must be very clean within the critical space to prevent false alarms from occurring. Because of their sensitivity level and the possibility of false alarm, these systems tend to be used as an initial alert system to which MCO personnel need to respond, as opposed to a full alarm system that activates suppression systems or dispatches emergency services. However, as the criticality of MCOs increases, raising the cost of downtime, high-sensitivity smoke detection is being implemented more frequently, and you are more likely to encounter them installed in the MCO facilities you manage.

## Flame and Flash Detection

Another traditional means of fire detection is flame or flash detection, which operates by sensing the intense light signals emitted by the fire's flames or explosive flashes. Flame and flash detectors can monitor for high-intensity visible light sources, but their capabilities can extend into ultraviolet (UV) and infrared (IR) spectrums.

Think about looking at a candle or campfire, and the distortion you notice just above the flames—this is light operating outside the wavelengths light that is visible to the human eye. To a flame or flash detector, however, these distortions to the light signals may be noticed just before a fire is about to start or may be detectable outside an enclosure in which a fire is smoldering or burning.

The variety of flame and flash detection products that are available compliment the variety of MCO hazards, including both general flame detectors and those designed to spot flames from very specific fuel sources. These devices can be used as a primary, standalone system to signal that there is a fire emergency, or they can act as a secondary system to piggyback on smoke detection in order to activate the fire suppression system.

## Beam Detectors

Beam detectors—some of the newest options for fire detection—operate by sensing the interruption or obstruction of a light source, traveling between a transmitter and a receiver, from fire or fire by-products. These units can be manufactured with highly sensitive tolerance levels and can detect minute amounts of particulate in the airstream, so they are often used as an early-warning system in MCO facilities as opposed to initiating suppression systems off a single detection alarm.

There are a number of common types of beam detectors, based on design:

- **Optical Beam** projects light across large areas and generates a signal when a certain percentage of that light is obstructed from being read by the receiver.
- **End-to-End** is a more focused version of the optical beam.
- **Reflective** projects a light beam to a reflector or prism and analyzes the light signal received back to detect the presence of smoke.
- **Laser** uses a laser beam to count the number/concentration of combustion particles crossing the beam.



**Figure 6-3:** The transmitter (left), receiver (right), and control box (middle) of an end-to-end beam detector. (Source: Fire Fighting Enterprises (Depwaldrontoo)/Creative Commons (CC BY 3.0)/[https://commons.wikimedia.org/wiki/File:Optical\\_beam\\_smoke\\_detector.jpg](https://commons.wikimedia.org/wiki/File:Optical_beam_smoke_detector.jpg))

## Fire Alarms

*Fire alarms* refer to the system of devices designed to alert facility occupants of hazardous conditions in the event of smoke and/or fire. Alarm devices usually consist of horns (any loud, obnoxious sounds used to draw attention), strobes (extremely bright flashing lights to aid in attention and specifically to notify the hearing-impaired), and sometimes a pre-recorded announcement with response or evacuation instructions. The alarm devices may be part of the detection devices, standalone units tied into the fire panel, or combined with other emergency devices like exit signs and lighting.



**Figure 6-4:** The speaker and strobe light of a fire alarm system. (Source: Ben Schumin/Creative Commons (CC BY-SA 2.0)/[https://commons.wikimedia.org/wiki/File:Mircom\\_Fire\\_Alarm\\_HornStrobe.jpg](https://commons.wikimedia.org/wiki/File:Mircom_Fire_Alarm_HornStrobe.jpg))

## Fire Alarm Control Panels

Fire alarm control panels (or fire panels) are the master control devices used to collect input from all remote monitoring devices, monitor the digital health of these devices, and use programmed logic to initiate alarms and/or notifications in the event of a fire. Older fire panels are composed largely of relays providing on/off signals for each device or zone, while newer panels have many more electronic components and control boards that have the ability to receive and compute large numbers of digital input signals (although relays are still used as some inputs). As an MCO technician, you may encounter either in your MCO facility, as both are still in use.

Similar to an alarm system you may have installed in your home, MCO fire panels regularly rely upon connectivity to monitoring and response networks. Whenever possible, fire panels should be fully integrated into building monitoring systems to provide real-time status and notification to operations personnel. Fire panels are becoming further digitized with network connectivity, both internal and external, with more alerting capabilities beyond the traditional phone line dialing into emergency services. Outside firms can also tie into the fire system to monitor the facility and automatically dispatch local emergency services during alarm incidents.



**Figure 6-5:** A fire alarm control panel. (Source: Wile e2005/Creative Commons (CC BY 3.0)/  
<https://commons.wikimedia.org/wiki/File:Simplex4100Upnel.JPG>)

# ACTIVITY 6–1

## Identifying Fire Detection Systems and Components

### Scenario

In this activity, you will identify fire detection systems and their various components.

---

**1. What are the three elements that make up the fire triangle?**

- Heat
- Fuel
- Smoke
- Oxygen
- Accelerant

**2. Which fire detection system uses sound, light, or other visual or auditory cues to notify site personnel of hazardous conditions in the event of smoke or fire?**

- Smoke detection
- Heat detection
- Flame detection
- Fire alarms

**3. Which fire detection system functions by sensing the intense light signals that are emitted by a fire?**

- Beam detection
- Smoke and heat detection
- Flame and flash detection
- High-sensitivity smoke detection

**4. Which fire detection system functions by sensing the temperature changes and air quality changes that accompany a fire?**

- Beam detection
- Smoke and heat detection
- Flame and flash detection
- High-sensitivity smoke detection

**5. Which fire detection system functions by sensing any interruptions to light traveling between a transmitter and a receiver that is being caused by smoke or fire?**

- Beam detection
- Smoke and heat detection
- Flame and flash detection
- High-sensitivity smoke detection



6. Which fire detection system functions by sensing very minimal changes to the air quality caused by a fire?

- Beam detection
  - Smoke and heat detection
  - Flame and flash detection
  - High-sensitivity smoke detection
-

# TOPIC B

## Fire Suppression

Detecting a fire is just one important piece of the fire safety systems puzzle; controlling and extinguishing the fire is the other important part. Fire suppression systems need to be in place and operating properly in order to quickly activate and eliminate a fire before it can cause extensive damage. As an MCO technician, you will need to have a strong understanding of the various fire suppression systems, how they are activated, and how they work to extinguish a fire. In this topic, you will identify fire suppression systems and their components.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Fire suppression
- Sprinkler system
- Fire pump system
- Clean agent system
- Foam system

## Fire Suppression

Understanding the principles of *fire suppression* is rooted in the fire triangle: no matter how complex and modern the suppression systems are, the primary goal is to remove one or more of the elements from the triangle in order to control and extinguish the source of the fire. Most commonly, fire suppression systems seek to negate heat or oxygen from the reaction.

The various types of fire suppression systems, then, target different sources of fire. Water-based systems work to drop heat below the point of combustion. Gaseous-agent systems primarily function by displacing oxidizing agents from the space. Smothering agents, like foam, remove heat but also act to separate the fuel source from the oxidizing agent.

## Sprinkler Systems

A *sprinkler system* categorically refers to all of the devices that deliver water as the method of fire suppression to the space being affected by the fire, and spread it to adequately cover all equipment and structures. Actually, sprinkler designs are varied and may be highly specific to the MCO application, but operators and technicians should at least make themselves familiar with the sprinkler system's "coverage" based on height and spray pattern.



**Figure 6–6: A ceiling-mounted sprinkler is part of the larger sprinkler system. (Source: Brandon Leon/Creative Commons (CC BY-SA 2.0)/[https://commons.wikimedia.org/wiki/File:Fire\\_sprinkler\\_roof\\_mount\\_side\\_view.jpg](https://commons.wikimedia.org/wiki/File:Fire_sprinkler_roof_mount_side_view.jpg))**

There are a few major classifications of sprinkler system design.

<b>Type of Sprinkler System</b>	<b>Description</b>
Wet Pipe	Wet pipe systems refer to sprinkler systems that remain fully "charged"—the piping is always completely filled with water, all the way out to the sprinkler heads. Wet pipe systems do not necessarily have to be completely pressurized (particularly if fire pumps are installed), but the advantage is that water is immediately available at the sprinkler heads upon system activation.
Dry Pipe	Dry pipe systems, as the name implies, are largely empty except for main supply headers. This is often seen in data centers or MCO installations with large amounts of sensitive (i.e., primarily electronic) equipment with which a delay in the availability of water flow from the sprinklers is an acceptable sacrifice, given the risk of damage to the MCO equipment should an unnecessary activation of the sprinkler system occur.
Mist/Fog	Mist or fog systems operate differently than the traditional sprinklers you're used to seeing by creating high pressures at the nozzle to atomize the water. As there isn't a direct stream of water, these systems are not as effective at fighting small fires or spot fires, but work well in responding to large fires engulfing a space. With more distinct water molecules, there is an exponentially larger total surface area of water exposed to allow heat transfer. Additionally, smaller individual amounts of water more easily flash to steam, the expansion of which displaces a large amount of oxygen from the space.

<b>Type of Sprinkler System</b>	<b>Description</b>
Pre-Action	A common design modification for dry systems is what is called pre-action, meaning that the system activates in stages. An initial fire detection alarm will cause the system to charge to some extent, and a subsequent detection will fully activate the system. Again, the focus is on preventing damage to critical equipment due to inadvertent or unnecessary system activations.
Single Interlock	A single interlock system is a version of the pre-action design that fully charges the entire system with the first detection, and deploys water with the second. For instance, a smoke detector that senses smoke will trigger header valves to open and flood the piping all the way to the sprinklers, and then heat detected at the sprinkler will release the water.
Double Interlock	A double interlock system will look for the same sequence as a Single Interlock system, but keeps the piping dry until the second detection signal is received. The first signal may call for fire pumps or other design features to fully pressurize the main header if such features exist.

## Fire Pump Systems

A *fire pump system* consists of water pumps dedicated solely to MCO sprinkler systems, and should absolutely be treated with the same level of criticality for maintenance and repair as any other critical equipment onsite. They are designed to help move the water in the fire suppression system to the location of the fire, specifically to the sprinkler system. Typically, they are installed when the utility water supply may deliver insufficient or unreliable pressures or the system is being supplied from a static source (without inherent pressure), such as a storage tank.



**Figure 6-7:** A fire pump system helps move water quickly and efficiently to the location of the fire. (Source: Toddastephens/Creative Commons (CC BY-SA 3.0)/<https://commons.wikimedia.org/wiki/File:Vertturbdsfirepump.jpg>)

There are a few different types of pumps used within a fire pump system.

<b>Type of Pump</b>	<b>Description</b>
Primary	A primary pump is the main piece of equipment providing motive force to ensure adequate water pressure during system activation. It is the largest pump installed in the system and operates in standby mode to begin pumping when the system is activated. Primary pumps should be connected to a protected emergency power supply, but are often powered by their own diesel motor to aid in the ability to fight fires even if all power is lost to the facility.
Secondary	A secondary pump can either act as a backup pump (if sized the same as the primary pump) or as a booster pump to help ensure adequate water pressure reaches the most remote parts of the system. Secondary pumps may be configured to energize automatically with the primary pump, or using pressure sensors that detect when the system flow drops below designed set points.
Jockey	A jockey pump is a smaller pump installed at various points in the system to ensure particular piping or devices are fully pressurized. In doing so, they also ensure a pressure drop will be easily sensed if sprinklers are activated, as the main pumps in the system are usually triggered to come online by the decrease in pressure that should be associated with sprinkler flow.

## Clean Agent Systems

A *clean agent system*, otherwise known as a gaseous suppression system, operates by dispersing some type of inert gas throughout a space, removing the oxidizing agent element of the fire triangle. These systems have tanks with highly pressurized gas that is piped out to protected spaces and dispersed through nozzles. In some cases, the gas used can also have properties that chemically interrupt the combustion process. Clean agent systems have become more common as more information becomes available regarding the impact of other fire suppression substances on both personnel and the environment and safer alternatives become more available.

There are a few types of clean agents that have been most commonly used:

- Halon was once the most widely recognized and used gaseous suppression agent, but has become less prevalent in recent decades due to the harmful effects on people and the environmental (in fact, in some places, it has been deemed illegal to use).
- The halocarbon HFC-227 (most recognized under the trade name FM-200), quickly replaced halon, as it is safe for human contact. While personnel can't remain in a space where HFC-227 has been activated, since it displaces the oxygen we breathe, minimum inhalation of it doesn't have harmful effects.
- HFC-125 is a newer class of clean agents that has even less of an impact on the environment and is significantly more affordable to produce. HFC-125 does not displace the oxygen in a space, making it safe to use even when the space is occupied.

## Fire Extinguishers

A fire extinguisher is probably the most recognizable device for fire suppression. It is a portable or hand-held fire suppression device that personnel can use to combat small fires. They work off the same principle as full fire systems, attacking one or more elements on the fire triangle.



**Figure 6–8:** A CO<sub>2</sub> fire extinguisher. (Source: Rt66lt/Creative Commons (CC BY–SA 3.0)/[https://commons.wikimedia.org/wiki/File:CO\\_extinguisher\\_2.PNG](https://commons.wikimedia.org/wiki/File:CO_extinguisher_2.PNG))

Fire extinguishers are classified by the types of fire(s) for which they are useful.

<b>Type of Fire Extinguisher</b>	<b>Suppressive Substance</b>	<b>Effective Against</b>
Class A	Water, Carbon Dioxide (CO <sub>2</sub> )	General combustible materials, such as wood or paper.
Class B	Foam	Flammable liquids (such as oil) or gases.
Class C	Non-conductive agent (CO <sub>2</sub> , HFC, PKP)	Electrical fires.

Fire extinguishers should be permanently mounted and accessible in all areas with fire hazards and/or spaces occupied by personnel. AHJs (Authority Having Jurisdiction) determine specific requirements for how many extinguishers must be installed in a particular type of space. As they are pressurized containers, and they need to be available for emergency use, proper mounting ensures that personnel don't accidentally knock them down and cause them to discharge.

## Foam Systems

A *foam system* operates by dispensing a foamed fire suppressant liquid that combats many of the elements of the fire triangle: it reduces the fire's heat and coats the fuel to prevent it from coming into contact with the oxidizing agent. This type of fire suppression system is most commonly used in MCOs to combat Class B fires and is typically installed only when excessive amounts of fuel or oil are present in the facility. The foam can either be from a pressurized substance that expands when it is released through the fire system nozzles, or it can be created by mixing a base substance and water while it is being released. For instance, AFFF (aqueous film forming foam) is a common class of foam agent that works by releasing water through or into a highly concentrated mixture of surfactants or solvents.

## ACTIVITY 6–2

# Identifying Fire Suppression Systems and Their Components

### Scenario

In this activity, you will identify fire suppression systems and their various components.

---

1. **Which type of fire suppression system functions by dispersing some type of inert gas throughout the affected space in order to remove the oxidizing agent element of the fire triangle?**
  - Foam
  - Sprinklers
  - Clean agent
  - Fire extinguisher
  - Fire pumps
  
2. **Which type of fire suppression system functions by delivering water to the location of the fire, where it will be used by other devices to reduce the heat below the point of combustion?**
  - Foam
  - Sprinklers
  - Clean agent
  - Fire extinguisher
  - Fire pumps
  
3. **Which type of fire suppression system functions by dispensing a bubbled fire suppressant liquid throughout the affected space in order to reduce the heat and coat the fuel to prevent it from coming into contact with the oxidizing agent?**
  - Foam
  - Sprinklers
  - Clean agent
  - Fire extinguisher
  - Fire pumps
  
4. **Which type of fire suppression system functions by dispensing water throughout the affected space in order to reduce the heat below the point of combustion?**
  - Foam
  - Sprinklers
  - Clean agent
  - Fire extinguisher
  - Fire pumps



5. Which type of fire suppression system functions by dispensing fire suppressive agents via small or hand-held devices to combat any of the elements of the fire triangle?

- Foam
  - Sprinklers
  - Clean agent
  - Fire extinguisher
  - Fire pumps
-

# TOPIC C

## Building Construction and Fire Prevention

While fire detection and suppression are important components of the fire safety systems in your facility, they are largely there to act reactively in the event of a fire emergency. When planning for and building an MCO facility, there are a number of specific components and materials that should be included in your facility's design and construction that you can use to proactively prevent smoke and/or fire from being able to spread throughout the facility. As an MCO operator, you should be aware of both the required and suggested steps you should take to ensure that your facility is constructed in a safe manner. In this topic, you will identify the components of a fire-safe facility.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- AHJ (Authority Having Jurisdiction)
- Egress route
- Firewall
- Containment
- Penetration
- Penetrant
- Firestop

### AHJ

An *Authority Having Jurisdiction (AHJ)* refers to an individual or organization that has statutory or regulatory responsibility for upholding and enforcing certain standards. Specific to MCOs, this mostly concerns those building codes relating to Fire and Life Safety, including access to fire safety equipment and fire-ratings for building materials and design. An AHJ maintains specific responsibility relative to a certain safety-related topic, but an individual AHJ or office may cover more than one area of practice.

Common examples of AHJs are city, county, or state inspectors; state or federal regulators (such as OSHA—Occupational Safety & Health Administration); or industry-specific authorities. Due to the nature of differing geographies and myriad local laws, most fire codes (especially as they relate to construction of a facility) are regulated by city or county AHJs. These could be specific enforcement offices or public officials such as the local fire chief.

Additionally, many sectors within the MCO industry have formulated highly specific operational guidelines and standards that do not exist as laws or codes, but as insurance-enforced items. In remote locations, or those areas not entirely familiar with MCOs, local AHJs may choose to defer to industry insurance-firm inspectors to enforce those standards that may be more restrictive than whatever laws exist.

There are two major types of regulations that might fall under AHJ enforcement.

<i>Type of Regulation</i>	<i>Description</i>
Municipal codes	The detail and breadth to which municipal codes address Fire and Life Safety design or operational guidelines is extremely varied across the country. It is unreasonable for all MCO personnel to be familiar with all these standards, so it is in the best interest of the MCO installation to maintain a close working relationship with local AHJs. They are the experts, and both expect and are more willing to answer questions. What may be considered sufficient fire suppression coverage in one city may be insufficient the next county over. Furthermore, many municipal bodies typically do not have the resources to widely publicize updates to codes and regulations, so when in doubt—call and check!
Insurance regulations	As more MCO sectors are developing their own industry-wide guidelines, insurance firms are similarly specializing their own regulations and coming to the forefront as the leading AHJs for those applications. While an insurance engineer may not be able to deny a certificate of occupancy or sign-off on an electrical installation, the fines they can levy on the MCO owner absolutely grab the attention of MCO executives. These specialized insurance firms make an effort to stay aware of the leading edge of safety and design discussions for their industry, making them a great source of current best practices—aside from trying to avoid their financial penalties.

## Safety Access

Personnel safety must be the primary consideration when it comes to designing and building the fire protection systems and infrastructure of an MCO facility. When it comes to the people interacting with the building, there are two main goals: personnel must be able to quickly and safely exit spaces in danger, and personnel must be able to quickly and safely access emergency equipment.

An *egress route* refers to the escape path from individual spaces within the facility or from the entire facility in general to a safe location in the event of an emergency, such as a fire. In many cases, these escape paths are marked with arrows, reflective tape, emergency lighting, or other visual cues to help guide you to the location quickly and easily. AHJs will determine the specifics regarding your egress routes, such as the width of egress aisles, the number of exit paths required, necessary additional lighting along the egress route, and so on.

Emergency equipment should also be clearly marked with appropriate signage, and free from obstruction. Examples include wall-mounted fire extinguishers, fire alarm pull stations, fire panels, and system override buttons.

## Walls and Firewalls

As an MCO technician, you need to maintain a solid understanding of what parts of your facility are fire-rated and to what extent, and this starts with the walls. A *firewall* may or may not be load-bearing for the structural integrity of the facility, but its primary purpose is to prevent the spread of fire. The various elements of a firewall—such as material make-up, thickness, penetration potential, and so forth—work together to establish a boundary that can help contain a fire in order to protect personnel and other critical infrastructure or equipment. Firewalls are most commonly classified by duration of fire they are able to withstand (30-min rated, 2-hour rated, etc.).



**Figure 6–9:** The concrete firewalls separating various spaces are clearly visible in a building under construction. (Source: Blahedo/Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:Firewall\\_construction\\_2.JPG](https://commons.wikimedia.org/wiki/File:Firewall_construction_2.JPG))

MCO design should take into account the minimum rating, required by the most restrictive standard. There may be some gray area surrounding when or what type of firewall is required by the city/industry/insurance regulations, so it's always best to play it safe. There is clearly a higher cost to stronger walls, so the cost-benefit analysis should be thoroughly reviewed during the design phase of an MCO facility. It is extremely costly and disruptive to retro-fit structures after the fact, making firewall considerations all the more important during your design and design evaluation.

## Doors and Windows

Doors and windows are also fire-rated, and are similarly rated to walls and firewalls. With doors and windows, however, materials selection is much simpler and they can be more easily modified after the fact. The number and location of doors and windows in the facility plays a large role in the overall fire rating of a particular space, since they generally diminish the level of protection provided by solid walls.

## Containment

Fire-safety construction considerations extend beyond the major structural components of the facility, so we refer to other means of fire-protection considerations under the general umbrella of *containment*. In this sense, containment can be any component or device used to prevent or mitigate the spread of fire and/or smoke.

In addition to the structural components such as walls, doors, and windows, then, containment typically includes the following components.

<b>Containment Component</b>	<b>Description</b>
Dampers	The dampers within an HVAC system are frequently used to serve safety purposes beyond controlling the ambient conditions of a people-space or equipment-space. Certain dampers can be used to provide enhanced fire protection functions; specifically, they are used to prevent the spread of fire inside the HVAC ductwork. For instance, the dampers installed in walls may be closed to isolate an area if fire detection or suppression systems are activated or they can be aligned in a specific sequence that creates an exhaust path to evacuate smoke from the facility. In either case, these dampers can be tied into fire panels or directly to detection devices.
Shutters	Shutters, when used in fire-safety applications, function just like dampers, but are typically not part of HVAC ducting. Shutters that cover windows, doors, or other openings can be manually or automatically repositioned to prevent the spread of fire, by either isolating an affected space or providing an exhaust path for smoke or fire.
Opening Protectives	As MCO installations are unique in their design and the infrastructure makeup, there can be any number of openings that need to be evaluated from a fire-safety standpoint, such as access panels in equipment housing, material or conveyor chutes, and so on. When these openings are part of a partial or full fire-rated space containment, custom devices to protect these openings can be fabricated and installed.
Other Containment Devices	As the focus on industrial safety increases, there are many other containment devices coming onto the market at any given time. For example, there are now panels/curtains with fuseable links that melt and release upon high heat or command, which can automatically drop onto critical equipment to isolate it from the fire or provide longer fire suppression coverage.

## Penetrations and Fire Protection Integrity

A *penetration* refers to an opening created in a material that needs to have a fire-rating (such as a wall) by a *penetrant*, which is any mechanical, electrical, or structural component that needs to pass through that opening as part of the larger facility system that it belongs to. For example, penetrations through walls are regularly necessary for plumbing pipes, electrical conduit, HVAC ductwork, and so forth. However, whenever a penetration occurs in a firewall or other containment component, fire protection integrity becomes an important consideration. At the penetration points, a *firestop* must be created by properly sealing the openings and/or joints; to do so, there are many types of fire-resistant materials such as caulk, foam, insulation, etc. and each have their own specific fire ratings (for heat and smoke resistance). If not properly applied, however, these sealants may be useless.



***Figure 6–10: A firestop pillow is installed in a penetration in a concrete slab to provide fire protection. (Source: Achim Hering/Creative Commons (CC BY 3.0)/<https://commons.wikimedia.org/wiki/File:Pillowinst.jpg>)***

Beyond the initial construction period of a facility, regular inspections should be done by MCO operators to ensure the integrity of these penetrations is maintained. Environmental conditions could cause expansion or contraction of these materials or they could be damaged by getting hit with a ladder, lift, tool, or person.

# ACTIVITY 6–3

## Constructing a Fire-Safe Facility

### Scenario

In this activity, you will identify the components needed to construct a fire-safe facility.

---

- 1. Which of the following terms describes any devices, other than the structural components of a building, that prevent or mitigate the spread of fire and/or smoke?**
    - Firewall
    - Penetrations
    - Firestops
    - Containment
  - 2. Which of the following terms is used in MCOs to describe a clearly marked path to safety that site personnel should follow in the event of an emergency?**
    - Escape route
    - Exit route
    - Egress route
    - Emergency route
  - 3. Which of the following terms describes any opening that is created when a part of a facility system passes through a material or component that needs to have a fire-rating?**
    - Firewall
    - Penetrations
    - Firestops
    - Containment
  - 4. Which of the following terms describes the components or materials that must be added at a point of penetration to prevent the spreading of fire or smoke through the openings?**
    - Firewall
    - Penetrations
    - Firestops
    - Containment
-

## TOPIC D

### Exit and Emergency Lighting

In the event of a fire or other emergency, you need to have systems in place that help direct and guide the people and personnel within the facility to a safe location. The exit and emergency lights in the facility serve this very specific purpose, and must be well-placed, clearly visible, and always functioning properly to ensure the safety of your facility. As an MCO technician, you need to be aware of the different lighting systems available for use in your facility. In this topic, you will identify exit and emergency lighting options.

#### Exit Signs and Emergency Lights

For a host of reasons ranging from safety, to security, to general construction design, MCO facilities rarely have windows in critical production or infrastructure spaces, so when normal lighting goes down, it gets dark—real dark. Emergency lights and visible exit signs are crucial to help MCO personnel respond to incidents that take down power and to direct people to the proper egress route during dangerous situations.



**Figure 6–11:** An exit sign very visibly tells people where to go to exit the building, especially in the case of an emergency. (Source: KRoock74/Creative Commons (CC BY–SA 3.0)/[https://commons.wikimedia.org/wiki/File:Exit\\_light\\_sign.JPG](https://commons.wikimedia.org/wiki/File:Exit_light_sign.JPG))

#### Battery Backup Emergency Lighting

Most emergency lighting at MCO facilities runs off battery backup, which could be local batteries at each fixture or some type of UPS setup connected to emergency lighting circuits. The largest benefit of battery-powered emergency lighting is portability—it can be installed just about anywhere. Most emergency lighting fixtures are wired into the building to keep the batteries charged and ready for use. In the event of facility work that takes down or disables installed emergency lighting circuits, a simple fixture can be added with a photocell that energizes the fixture when darkness is sensed. For fixtures that are not tied in to general building electrical circuits for charging, it is best practice for MCO operators to keep an accurate inventory and a map of these fixtures, and to check and replace the batteries on a regular basis.



## Generator-Sourced Emergency Lighting

Generators are another common source of power for emergency lighting in MCO facilities. Power for these fixtures is provided from the generator supply. In most cases, the circuit is automatically (and likely, only) engaged and energized when the power is supplied from the generator. This is not to say that this lighting can't also be battery-backed or installed to turn on when darkness is sensed, but efforts to simplify MCO design tend to install the emergency lighting on one circuit only: either on the facility or battery circuit or on the generator feed.

## Night Light Circuits

The purpose of night lights in an MCO facility is actually the same premise as that for night lights in your home: they provide a nominal amount of lighting in the absence of natural lighting or when regular lighting circuits are not being utilized by personnel. Night light circuits are generally low intensity and are not intended to be the primary or sole source of emergency lighting. Common expected use for these circuits would be to bridge the time gap for generator-powered emergency lighting to come on. For non-emergency scenarios, these would provide just enough lighting to safely exit a space in the event of localized power losses (or regular lighting failure) when other emergency systems were not otherwise called upon.

# ACTIVITY 6–4

## Identifying Exit and Emergency Lighting Options

### Scenario

In this activity, you will identify the various exit and emergency lighting options available.

---

1. **Which type of lighting system is used to point site personnel to the closest point of egress in the facility?**
    - Exit signs
    - Emergency lights
    - Night lights
    - Overhead lights
  
  2. **Which type of lighting system is used to provide a nominal source of illumination in the absence of natural or power-supplied light sources?**
    - Exit signs
    - Emergency lights
    - Night lights
    - Overhead lights
  
  3. **Which type of lighting system is used to guide site personnel to and/or through the egress route during a potentially hazardous event?**
    - Exit signs
    - Emergency lights
    - Night lights
    - Overhead lights
-

# TOPIC E

## Emergency Power Off System

In the event of a fire or other electrical emergency, especially one that has caused damage to critical equipment or injury to a person, you may need to consider cutting the power to all or part of the facility. In most cases, an MCO facility will have a system in place that allows you to immediately shut off the power to the facility, a subsystem, or even a specific piece of equipment to respond to such an event or prevent further damage from occurring. In this topic, you will identify an emergency power off system.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- EPO (Emergency Power Off)

### EPO

*Emergency Power Off (EPO)* refers to any variation on a design that provides a single source of action—such as a button, switch, command, or other automatic safety feature—that instantly kills all power to a facility or subset of its infrastructure.



**Figure 6–12:** An EPO kill switch for a piece of machinery equipment in a laboratory. (Source: Cjp24/Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:Emergency\\_stop\\_button.jpg](https://commons.wikimedia.org/wiki/File:Emergency_stop_button.jpg))

There is plenty of debate around the need, efficacy, and operational risks of using EPO, which has only grown over the years as there are fewer and fewer standards and regulations actually requiring the installation of such systems. Adding to the debate, the range of EPO design begs the question: does the setup at my MCO facility actually count as an EPO? For our purposes, if an MCO operator can trigger a single action that removes all electrical power entering an area, then that is an EPO.

## General EPO Design and Use

While an EPO sounds simple—which is sort of the point and purpose of it as a system—the design is a bit more complex than you would think. You're not just opening a main breaker for all the electrical and mechanical equipment in an area; you are completely isolating an area, electrically speaking, in the event of danger. For the overwhelming majority of MCO installations, regardless of the scope and criticality of infrastructure affected, the litmus test is simple: Is there an out of control fire or flooding event? Is someone being electrocuted? Yes to either or both of those questions means you need to push the button. For other scenarios, even serious events like capacitors that have exploded or a pump shaft sheared, you'll probably want to rely on the other installed protective features in the infrastructure before you resort to EPO.

Given the conditions above, you can also approach the use of EPO from another angle—removing the energy source injuring someone or fueling a fire (or imminent danger such as massive flooding in a room with electrical gear). From a design standpoint, that means you need to secure power to the obvious electrical and mechanical infrastructure, as well as any controls and monitoring devices, lighting, even backup systems or subsystems. Many EPOs are targeted towards a specific room or section of a facility, so it isn't nearly as simple as cutting off the main utility input to the MCO facility and preventing backup power from kicking on.

Needless to say, the list of electrical systems and subsystems that could be affected by engaging EPO is long and requires accurate and detailed electrical drawings to ensure that all power sources are identified and addressed. Any new equipment installed in the facility post-construction needs to be checked against the EPO system(s) to ensure a new source of power is not added to an area that won't be stopped by the EPO in the event of an emergency.

## Pros and Cons of EPO

An EPO is unquestionably the fastest way to secure dangerous electrical energy sources, whether it be preventing an electrical fire from getting worse or allowing immediate access to give aide to a person that is electrocuted. Beyond the initial response, the follow-on benefit of using EPO is passed on to non-MCO technicians or other personnel. The fire department or EMT's responding to an emergency likely have no knowledge of the infrastructure; having no power to a specific location and being able to unequivocally report that an area is safe for them to enter allows them to respond quickly and thoroughly. From another perspective, there tends to be many personnel at an MCO location that are not part of the facility operations team; with EPO as an available option, you can train these personnel to recognize the severity of an event and respond by activating the EPO without having to wait or go find an MCO technician.

The clear downside of an EPO is that some or all critical operations are immediately ceased; all critical load goes down, all communications and monitoring are lost, and so forth. Depending upon the type of MCO installation, the recovery time (using an electrical event, for example, where no equipment was damaged) to bring the facility back online could be lengthy and create a severe interruption to business operations. Design and construction is the other area of concern. An EPO typically cannot be retrofitted to an existing facility due to the risk of not being able to fully identify all power sources. Conversely, should you need or want to decommission the EPO in an existing facility with live operations, it would likely require working on live electrical equipment to remove some connections.

# ACTIVITY 6–5

## Identifying EPO Systems

### Scenario

In this activity, you will identify Emergency Power Off (EPO) systems and their use, benefits, and drawbacks.

---

#### 1. What is Emergency Power Off (EPO)?

- An emergency system that utilizes a set of specific actions, performed in order, to stop all power flowing to an entire facility, subset of the infrastructure, or specific piece of equipment.
- An emergency system that utilizes a single action to start all power flowing to an entire facility, subset of the infrastructure, or specific piece of equipment.
- An emergency system that utilizes a single action to stop all power flowing to an entire facility, subset of the infrastructure, or specific piece of equipment.
- An emergency system that utilizes a set of specific actions, performed in order, to start all power flowing to an entire facility, subset of the infrastructure, or specific piece of equipment.

#### 2. EPO should be your first course of action for any electrical emergency in your MCO facility.

- True
- False

#### 3. EPO should only be used when absolutely necessary, as using it can greatly disrupt normal operations and recovery time can be extensive.

- True
  - False
-

# TOPIC F

## Fire Systems Preventative Maintenance

Now that you know about the fire safety systems and components that you may encounter in an MCO facility, you need to be prepared to keep those systems working properly in order for MCOs to operate safely or for the necessary actions to take place in the event of an emergency. Since these systems and their components are so integral for the safety of people and critical equipment, it is imperative that preventative maintenance procedures and schedules are followed to ensure they are always working and operating at their optimal conditions.

As an MCO operator, your responsibilities will likely include completing these preventative maintenance tasks. In this topic, you will identify the preventative maintenance procedures for fire systems and their components.

### Fire System Equipment Testing and Inspection

Fire systems in general don't have as many moving parts as other systems, so preventative maintenance on the equipment tends to lean more towards inspections. Depending upon local jurisdictions or insurance regulations, these activities can be performed by MCO technicians, or by licensed contractors. Regardless of who performs them, the following preventative maintenance testing and inspection tasks should be completed regularly to ensure that all the components of the fire detection and suppression systems are working properly:

- Verify the proper operation of detection devices by creating an artificial signal (such as smoke cans or heat guns, or digitally inserting a signal) and making sure that the device can recognize the signal at the appropriate threshold and can generate an output signal to the main system.
- Cycle fire system isolation valves to check for proper movement and verify that they are in the correct position.
- Conduct flow tests on air and water valves.
- Check suppression agent tanks for proper pressure/temperature indications and verify that vessel pressure test ranges have not expired (depending upon the tank, this could be 5, 10, 20 years or more).
- Inventory all fire extinguishers, physically check them for any indications of tampering, verify they are at their proper holding pressure, and weigh them to validate their fill levels.
- As needed, perform the necessary deeper preventative maintenance activities for fire pumps such as greasing bearings, checking shaft alignment, and performing pressure tests.



*Figure 6-13: A technician checks on a fire extinguisher to make sure it is working properly. (Source: sdigital/iStock/Thinkstock)*

## Fire Alarm System Maintenance

As fire alarm systems become more comprehensive in relation to the complexity of MCO installations, it is imperative that fire system controls experts check the entire system at the very least on an annual basis. A variety of digital and/or logic checks must be performed to verify that signals are being properly sent and received between main panels, remote zones, and individual devices. Most panels and devices have backup batteries installed, which are often forgotten or missed (until power is lost and the batteries are found to be dead!), so it is important to remember to check the battery life of anything running on backup battery power. When possible, alarm activations should take place to verify proper operations of horns, strobes, and speakers. If you are able to test the alarm system notifications, this is a perfect time to run building evacuation drills so site personnel are aware of what the system alarms look and sound like and are prepared for action in the event of a real emergency.



**Figure 6–14:** A certified technician performs maintenance tasks on a fire alarm control panel for a facility. (Source: Lisa F. Young/iStock/Thinkstock)

## Fire Alarm System Outages

MCO technicians must maintain a keen awareness and understanding of the status of fire alarm systems, as preventative maintenance activities will often require an operational outage of some or all of the protection systems. For instance, when checking global alarm functions, you will need to disable sprinkler systems (for obvious reasons). Since some equipment or areas may have localized shutdowns in the event of smoke/fire detection, if the fire system will be disabled for any amount of time for maintenance purposes, you should consider performing more frequent rounds or establishing fire watches throughout the duration of the maintenance activities.

Depending upon communication protocols, operators may need to inform monitoring companies or local emergency response units that maintenance is taking place and that any alarms that are triggered during that time should be ignored. It is critical to keep track of these kinds of communications when they are made (and to who they are made) so the site does not forget to tell them to resume monitoring and response once maintenance is complete.



## ACTIVITY 6-6

### Identifying Fire Systems Preventative Maintenance Procedures

#### Scenario

In this activity, you will identify the appropriate preventative maintenance procedures for fire systems and their components.

---

1. **In general, how often should you check on the proper functionality of and perform preventative maintenance as needed on the fire alarm systems in your facility?**
    - Daily
    - Weekly
    - Monthly
    - Quarterly or semi-annually
    - Yearly
  
  2. **Fire systems don't have as many moving parts as other systems, so physical checks and inspections are the most common preventative maintenance tasks that you are likely to perform on their components and equipment.**
    - True
    - False
  
  3. **If a fire system outage will occur as part of preventative maintenance tasks, you should communicate with any local emergency response groups or monitoring companies before and after the outage.**
    - True
    - False
-

## Summary

In this lesson, you identified and described the fire safety, systems, and equipment that are integral to ensuring that the people and critical spaces within the facility are protected in the event of a fire or electrical emergency. Having a strong understanding of the fire detection and suppression systems and their various components ensures that you and your MCO personnel are ready and prepared in the event of an emergency and can respond promptly, taking the necessary actions to keep the people and equipment in your facility safe from harm.

# 7

# Personal Safety and Emergency Response

## Lesson Objectives

In this lesson, you will identify and apply personal safety and emergency response protocols and procedures. You will:

- Identify common safety hazards and relevant protective devices.
- Identify emergency response procedures in an emergency response plan.

## Lesson Introduction

In a Mission Critical Operations (MCO) facility, it is highly likely that there are hazardous materials or specialized equipment that could pose a threat to those working with these items and even just the personnel or general public in the vicinity of the space. When people are working in or generally occupying this kind of environment, there needs to be protocols in place to keep everyone safe and plans for a prompt response should an emergency occur.

As an MCO technician, you need to be aware of the numerous hazards that could potentially harm the critical equipment or people in your facility, and how to respond if any of these hazards threaten to affect operations or cause injury—or worse. In this lesson, you will identify and apply personal safety and emergency response protocols and procedures.

# TOPIC A

## Common Hazards and Personnel Protection

When working in an MCO facility, it is highly likely that you and your colleagues will be working around some pretty serious equipment or materials that each present their own potential risks. When working under these kinds of hazardous conditions, it is important to have protective measures in place to keep personnel and any other people that may be in the facility as safe as possible. As an MCO technician, you are responsible for knowing what the hazards in your facility are and the protective equipment in place to help keep you and your colleagues safe from harm. In this topic, you will identify common safety hazards and some of the relevant protective devices you are likely to encounter.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Hazard analysis
- PPE (Personal Protective Equipment)
- Confined space
- LOTO (Lock Out/Tag Out)
- GHS (Globally Harmonized System of Classification and Labelling of Chemicals)
- MSDS (Material Safety Data Sheets)
- SDS (Safety Data Sheets)

### Hazard Analysis

MCO environments are often dangerous and—whether under normal operating conditions or emergency considerations—preventing injury (or worse) to your team must *always* trump the concerns of business interruptions (killing power to a data center, shutting down a nuclear power plant, losing research, etc.).

When it comes to ensuring the safety within an MCO facility, then, *hazard analysis* is of the utmost importance. Hazard analysis refers to the general process of evaluating the environment, facility, and systems for safety risks for personnel occupying the spaces, as well as the general infrastructure itself. Hazard analysis may be guided by specific industry principles and regulations, organizational policies, insurance requirements, or a combination of any or all. The evaluation of major risks—such as fire, flooding, structural integrity, and so forth—are quite commonplace, and most MCO and facilities professionals are familiar with the evaluation techniques.

Beyond just reviewing infrastructure design for equipment hazards, the best MCO leadership teams view safety through the lens of the daily tasks of personnel. All tasks should be reviewed with a singular focus on identifying and mitigating hazards. Hazard analysis is most successful when it takes on a persistent, questioning attitude—whether it's the first time thinking about an activity or the 100th time completing it. The kinds of questions that you should always be thinking about include:

- Are there shock hazards? Can they be prevented by design or does specific safety gear need to be provided to personnel?
- Are there access issues? Are ladders, scaffolding, or handrails available? Are safety restraints needed?
- Are there sharp objects or surfaces that personnel might come in contact with? Can they be eliminated or covered?
- Are there health risks associated with this task/activity?
- Are additional personnel needed to serve as safety watches or supervisors for this activity?
- Will other onsite personnel be at risk due to the nature of the task/activity?

This list is not exhaustive, nor is this list truly ever complete; as an MCO operator, you should never stop asking these questions while working, and should only feel satisfied when you've taken all practical measures to make sure systems are working properly and personnel are safe.



**Note:** To further explore how to evaluate the potential risks within your space, you can view the **Analyze an MCO Space for Safety Hazards** presentation from the Certified Mission Critical Operator Video Series.

## Common Hazards

While it is obvious that all MCOs inherently have a wide range of hazards which are specific to the product or service they provide, there are many common hazards that operators and technicians will almost certainly encounter, regardless of the environment. These tend to be the easiest to protect against, but they are also among the hazards that account for the majority of accidents and injuries that occur—simply because they aren't at the forefront of your mind.

Let's take a closer look at the most common hazards within an MCO facility.

<i>Item</i>	<i>Description</i>
Noise	MCO infrastructure regularly contains notable quantities of large, incredibly noisy equipment, making noise hazards very common. Engines and rotating machinery—anything with a motor like a fan or pump, really—are obvious sources of noise. Additionally, fluid systems such as compressed air are also potential sources of noise hazards, like when a high pressure system vents off.
Falling objects	MCO facilities also tend to have multiple levels of equipment, so the risk from falling objects from upper levels or walkways is a common concern. In particular, technicians should be cognizant of any work occurring above them; dropped tools and parts cause more injuries than suspended equipment breaking and falling down.
Bodily harm	While not unique to MCOs, any risk of bodily harm to personnel, regardless of the type or severity of injury, is a real hazard concern. This could include slips/trips and falls, chemical burns, inhalation of irritating gases, and so on—the list is pretty extensive.
Eye and vision	Among all types of injuries, damage to eyes and/or vision can have the greatest impact on personnel—if you can't see, you can't work. Hazards range from foreign objects, chemicals, and extreme light from sources such as welding.

## PPE

*Personal Protective Equipment (PPE)*, which is sometimes also called *Personal Protective Gear (PPG)*, is the common term that refers to anything an operator wears or uses to minimize risk of injury from safety hazards. Note that, when defining or discussing PPE, we specifically say that it "minimizes" risk instead of "prevents" them, because there is nothing that absolutely removes all chance of injury. If PPE is not worn properly, or in the event of extreme conditions, injury is still possible. The point is: just because you wear recommended or required PPE, you should never assume that you don't have to worry about safety hazards anymore.



**Figure 7-1: FEMA workers wear the necessary PPE required when working with radiation during a training exercise. (Source: United States Navy/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:US\\_Navy\\_100608-N-9520G-005\\_Members\\_of\\_the\\_Federal\\_Emergency\\_Management\\_Agency\\_\(FEMA\),\\_Mobile\\_Emergency\\_Response\\_Support\\_\(MERS\)\\_based\\_in\\_Bothell,\\_Washington,\\_use\\_a\\_ANPDR-77\\_radial.jpg](https://commons.wikimedia.org/wiki/File:US_Navy_100608-N-9520G-005_Members_of_the_Federal_Emergency_Management_Agency_(FEMA),_Mobile_Emergency_Response_Support_(MERS)_based_in_Bothell,_Washington,_use_a_ANPDR-77_radial.jpg))**

The following are a number of common pieces of PPG/PPE that are likely to be required in an MCO facility.

<i>Item</i>	<i>Description</i>
Ear plugs/Ear muffs	<p>Sound waves are a form of pressure, so although we measure sound in volume, it is the increased pressure from loud sounds that will injure parts of the ear. There are many different levels of hearing protection based on sustained noise level exposure versus peak levels, so it is extremely important for MCO personnel to understand what regulations are applicable to their working environment.</p> <p>Ear plugs are PPE inserted into the ear itself to muffle hazardous sound levels. They are typically of a moldable material that expands to better fit individual ear shapes. Ear muffs are worn over the head and cover the entire ear, having the ability to block out even more sound. Double hearing protection (plugs and muffs) may be required depending upon the situation.</p>

<i>Item</i>	<i>Description</i>
Hard hats	<p>If any amount of construction or other work is happening above an often used or traversed area, it is sometimes impossible to prevent people movement underneath these potential hazards. The easiest way to protect from falling hazards is to wear your hard hat! Hard hats are made of a protective shell that surrounds the head, which provides a strong surface for falling objects to hit (instead of your head), as well as a cushioning action to absorb some of the force.</p> <p>Hard hats need to be inspected regularly and worn properly. Sustained exposure to UV light (working outside) can degrade the shell material. Hard hats should also generally be replaced if you have had something fall on them—even if they don't look damaged, the structural integrity of the hard hat may be compromised once it has sustained a hit.</p>
Eye protection	<p>Eye protection comes in several forms. Regular safety glasses are rated for strength based upon the material of the lens, and protect your eyes from flying objects (such as metal shavings, dirt or dust particles, etc.). Goggles (or modified safety glasses) make contact with your face around the eyes and are used to prevent liquids and gasses from getting in your eyes. Special, highly shaded glasses or helmets are used for activities like welding where extremely bright light sources exist.</p>
Gloves	<p>Gloves protect against many common hazards, but it is important to ensure you match the hazard to the application:</p> <ul style="list-style-type: none"> <li>• Rubber/latex gloves are appropriate when dealing with chemicals, oils, greases, and so forth.</li> <li>• General work gloves help to ensure grip-on tools, equipment, and structures.</li> <li>• Padded work gloves may be appropriate to absorb large amounts of movement.</li> <li>• Cut resistant work gloves are appropriate when dealing with sharp objects/tools or when working around materials with sharp edges, like sheet metal</li> </ul>
Steel toe footwear	<p>Steel toe footwear is a common requirement in most industrial settings. Ideally, you would like to have leather shoes or boots to prevent from cuts as well. Advances in material technology have created composites that have similar crush resistant properties as the traditional steel toe and are generally acceptable. The need for special soles (such as slip resistant and/or electrically rated) should be evaluated as well, although good work boots tend to have all of these characteristics.</p>

## Gown Up/Gown Down

In MCOs, the phrase "Gown Up/Gown Down" refers to the order and/or method in which PPE should be put on and removed. The easiest way to think about it is from a contaminated substance angle: working in reverse, you want to remove the articles that are most likely to be contaminated first, so that when you ultimately come in contact with your skin or undergarments, you are less likely to contaminate yourself. When donning multiple articles or layers of PPE, keep this in mind so you don't overlap items incorrectly and prevent safe, proper removal.

## Case Study: A Lack of PPE

Personal Protective Equipment (PPE) is an important safety component to ensure that personnel are protected from the harmful effects of some of the equipment or materials with which they commonly work. So, when there is a lack of PPE in a situation where it is necessary, there can be disastrous results. In one such case, the death of an employee has resulted in numerous citations for the parent company that neglected to provide the PPE required to keep him and other workers safe.

In November, 2014, an employee with Ferro Magnetics (a battery charger manufacturer) was accidentally electrocuted while testing transformers in the company's high frequency testing department. The Occupational Safety and Health Administration (OSHA) performed an in-depth investigation into the accident and found that the company had not provided employees with adequate PPE—specifically, the necessary electrical insulation gloves—for conducting the tests with live leads to the transformers, which were operating at 1,200 volts. Without this required PPE, the technician unfortunately came in direct contact with the live wire and was electrocuted; though he was rushed to the hospital, he did not survive.

OSHA's investigation of Ferro Magnetics after the deadly accident resulted in a total of 15 violations, 14 serious and 1 willful (with the death of the technician being cited as a willful violation) that carried proposed citation penalties of more than \$106,000. The willful violation was quite damaging: it cited that the company willfully placed employees at risk by failing to provide and require employees to follow safe practice when working with live parts, failing to provide employees with the PPE necessary for the dangerous work being performed, and failing to install the necessary protective items (protective shields, protective barriers, and/or insulating materials) required to protect those employees working with energized equipment.

The serious violations claim that the company did not provide a safe, hazard-free workplace; did not do its due diligence of assessing the hazards of the workplace and evaluating the need for PPE; did not provide the necessary PPE for a variety of hazardous tasks (including proper eye and face protection, skin protection, and hand protection); did not establish proper protocols for energy control prior to performing maintenance tasks; did not provide proper emergency wash stations; did not provide proper training for employees; and many other violations that could have resulted in serious injury or death to an employee.



**Note:** To view the complete list of OSHA's citations, visit [www.osha.gov/ooc/citations/FerroMagneticsCorporation\\_1007955.pdf](http://www.osha.gov/ooc/citations/FerroMagneticsCorporation_1007955.pdf).







**Figure 7-2: An eye washing station.** (Source: Ildar Sagdejev/Creative Commons (CC BY-SA 3.0)/ [https://commons.wikimedia.org/wiki/File:2008-07-02\\_Eye\\_wash\\_station.jpg](https://commons.wikimedia.org/wiki/File:2008-07-02_Eye_wash_station.jpg))

## Confined Spaces and Ventilation

Broadly, a *confined space* is any area that has limited or challenging entry and egress paths and/or poor ventilation due to lack of clean air supply or buildup of harmful gasses. Spaces that meet these criteria that are regularly accessed should be permanently marked as such, and required safety precautions should be clearly posted. When it comes to safety regulations for confined spaces, there are many criteria for identification and required precautions; for this reason, it is best for decisions regarding these areas to be made (or at least guided) by a trained safety manager.



**Figure 7-3:** A notice warning about a confined space is posted on a piece of equipment. (Source: Joe Mabel/Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:Confined\\_space\\_warning\\_01.jpg](https://commons.wikimedia.org/wiki/File:Confined_space_warning_01.jpg))

As an MCO technician, you might also deal with a rarely accessed space like a tank or void, so individual confined space assessments should be performed for each of these activities. Required precautions may include respirators, supplemental ventilation, and/or rescue equipment like hoists.

## Warnings and Labels

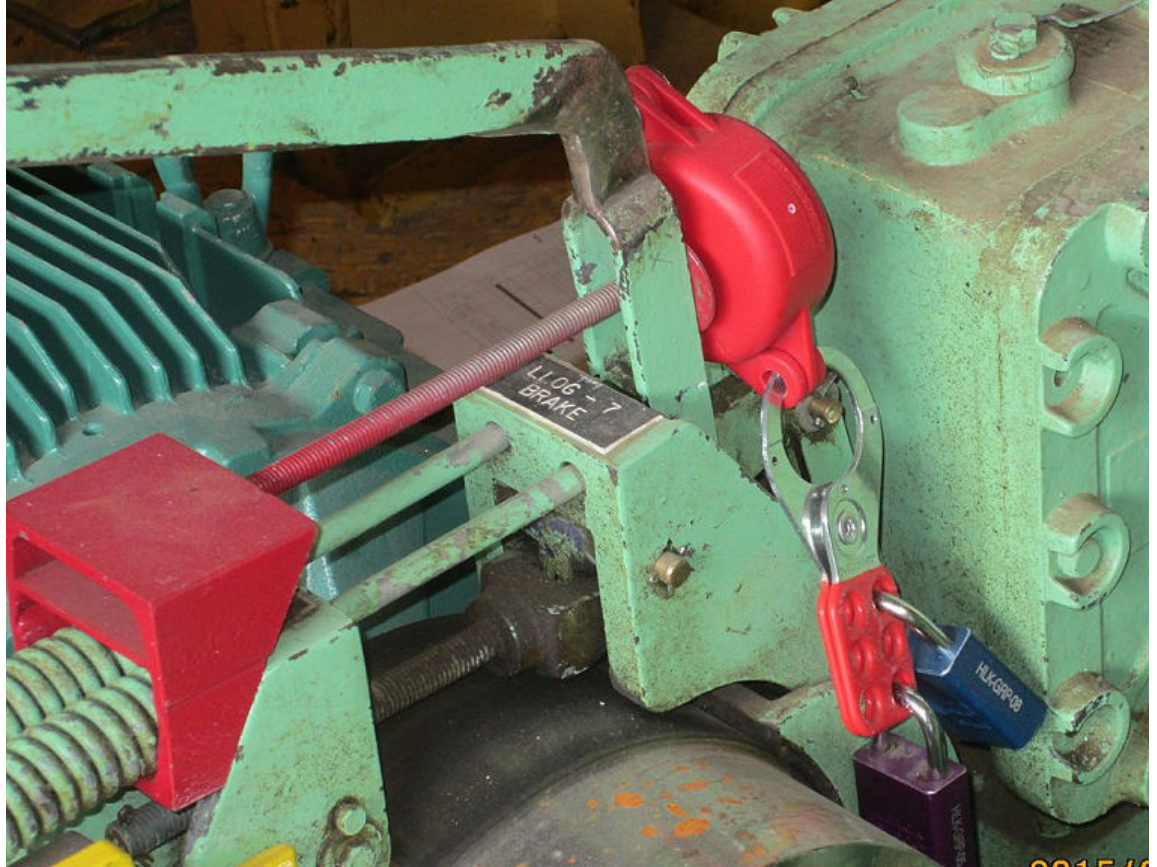
All MCO facilities have inherent safety risks beyond most typical facilities, and it is difficult to know everything about the MCO infrastructure. For this reason, most equipment comes with warnings and labels from the manufacturer that detail important information about their safe operation, and the potential safety risks and hazards if they are not handled properly. Additionally, most MCO operators will also add labels and warnings based upon site-specific safety concerns and evaluations. It is incredibly important, then, to remember to do one thing: read the label! And, you should never remove these labels. If warning labels become illegible or go missing, consult with leadership to determine the best course of action for replacing them.

## Arc Flash Labels

Arc Flash labels are a specific type of warning label located on electrical equipment (particularly panels and switchgear) to notify personnel of the potential risk from possible arc flashes. They are categorized based upon the maximum potential energy with and without covers or doors installed, which will correlate to the proper level of electrical safety PPE that operators must wear to work on the equipment. These labels should also indicate the safe working distances around the equipment both with and without these required levels of PPE. Arc Flash labels are becoming more commonplace in MCO facilities, especially as more standard regulations or AHJs (Authority Having Jurisdiction) are requiring them to be in place.

## LOTO

*Lock Out/Tag Out (LOTO)* refers to the practice of physically securing a source of energy with a latch, hasp, chain, or other kind of locking mechanism and noting the danger to equipment and personnel if operated with some sort of tag or label. Generally LOTO is applied to breakers, switches, and valves, but anything that can introduce a source of energy (power, water, gasses, etc.) to a work area can be locked out.



**Figure 7-4:** A lockout scissor clamp and two padlocks—one to secure the device, the other to prove it has been checked and verified—are applied to a hoist brake to prevent unexpected movement. (Source: Wtshymanski/Creative Commons (CC BY-SA 4.0)/[https://commons.wikimedia.org/wiki/File:Lockout\\_on\\_hoist\\_brake.JPG](https://commons.wikimedia.org/wiki/File:Lockout_on_hoist_brake.JPG))

LOTO training should be provided for all MCO personnel at all MCO locations, since the details of the program could vary. Sometimes double-barriers (LOTO for two sequential energy sources) are required, sometimes multiple verification signatures on the tag are required, sometimes regular (every shift or daily) audits and verifications of all hanging tags are required. Some AHJs do not require locking out an energy source if the worker can see it at all times and stop someone else from energizing the source. The best MCO programs will pull from all applicable AHJs and regulations, choosing at least the most conservative requirement and considering taking extra precautions when practical.



**Note:** It is worth noting that regardless of whether or not a specific LOTO is required by the AHJ, unauthorized manipulation of a LOTO'd device is not only grounds for termination, but often a criminal act—particularly if equipment damage, personnel injury, or death is a result.

## Chemical Cabinets

Hazardous chemicals present risks to personnel health and can potentially cause damage to the facility, and they should always be stored properly; generally, they should be stored securely in specific chemical cabinets. These cabinets may simply be dedicated storage lockers that can be locked and appropriately labeled to prevent access by unauthorized or untrained personnel. For chemicals that have particular risks of flammability or explosion, these lockers will be of a high-strength steel to attempt to contain any explosion and should be located outside or in a space that is not regularly occupied, away from critical equipment or flammable sources.



**Figure 7-5: Chemicals stored securely in a chemical cabinet.** (Source: U5680336/Creative Commons (CC BY-SA 4.0)/[https://commons.wikimedia.org/wiki/File:Chemical\\_cabinet3.JPG](https://commons.wikimedia.org/wiki/File:Chemical_cabinet3.JPG))

## Safety Barriers and Machine Guards

Safety barriers and machine guards should be installed on any sort of equipment with rotating, moving, or sharp components. The intent is obvious—to prevent injury—but it is unfortunately an oft-neglected safety measure in MCO facilities. Barriers and guards make it more difficult to access equipment and components (this is their design, after all) so in the interest of being able to work more easily and efficiently, some technicians get in the habit of leaving barriers and guards down. In some cases, these must be removed to access the infrastructure, but should always be replaced when that access point is no longer being utilized—even if this is just for two minutes to go grab some other tools.

## Slip and Fall Prevention

Slip and fall prevention is a safety responsibility of everyone within an MCO facility. Typically, there are planned preventative measures that will be in place throughout the facility, such as marking trip

hazards with high visibility tape or paint, requiring personnel to wear footwear that provides additional traction, and making sure to properly use safety barriers. While these may help limit the potential for slips and falls, accidents can still happen. Therefore, all personnel should do what they can to help prevent slips and falls in the workplace, beyond these standard measures. That means, if you see something on the floor, pick it up or clean it up. If a safety chain is down, put it back. Or, at the very least, tell someone with the proper authority or knowledge to do something about the problem to prevent a slip or fall from occurring.

## The Importance of Custodial Services

The sources of safety issues are both varied and plentiful in all sectors of MCOs, but the common thread that has the biggest impact for every single one is cleanliness. Custodial services at MCO facilities mean more than just a nice looking building and, depending on the particular needs of the facility, may be handled by an outside vendor or could be the responsibility of the MCOs' facilities operations team. Either way, the positive impact of custodial services within any facility include the following benefits:

- Clean floors prevent slips.
- Clean surfaces, especially in common areas, prevent infection.
- Trash removal helps prevent pest problems.

The list of direct benefits goes on, but there are also indirect benefits. If floors are not kept clean, MCO technicians may not notice an accumulation of fluid or rust coming from overhead piping. Excessive amounts of dust may interfere with high-sensitivity smoke detectors or general air-quality monitoring systems. By keeping the facility free of dirt, dust, spills, and other messes, custodial services acts as a first line of defense in some ways, helping to prevent common hazards from happening in the first place.



**Figure 7-6: Custodial Services personnel not only help keep the facility clean, they help prevent potential injuries from other common hazards. (Source: Thinkstock Images/Stockbyte/Thinkstock)**

## Environmental Health and Safety Programs

An Environmental Health and Safety Program (EHS, or sometimes ESH) refers to the comprehensive approach to safety at a facility that includes personnel training, detailed rules & regulations, PPE, infrastructure design, and more. While there are plenty of industry-specific regulations, as well as local/state/federal AHJ-directed requirements, organizations should formalize their own EHS programs and make them as site-specific as possible.

The Safety Officer is the EHS leader at an MCO facility. This could be a dedicated job (such as a Safety Manager or Safety Director) or a member of the operations team that is identified as having the responsibility of ensuring the EHS programs are properly implemented.

The list of EHS reporting requirements is exhaustive and highly dependent upon the specific MCOs. Regular reports include environmental items (emissions, hazardous substance inventory, etc.), code-related inspections (fire protection systems), and injury/incident reporting. Again, these will be specific to the related AHJs. Internal reporting requirements should go even further, documenting all aspects of the EHS program including PPE inventories, personnel training, etc. The Safety Officer and/or Operations Management will take the lead on this, as they are responsible for adhering to all internal and external reporting requirements.

## Materials Safety and Awareness

MCO personnel are responsible for understanding the equipment and material used in support of daily operations, but it's impossible to be an expert on everything, with all the details memorized. To help with this, Materials Safety and Awareness is something supported by everyone involved—from the people that make the equipment, to those who sell it, to those who work with it every day.

Manufacturers, suppliers, and vendors provide relevant information about the composition of MCO materials, as well as safety information for working with them.

There are a number of standardized Materials Safety and Awareness systems that you are likely to encounter in MCOs.

<i>Item</i>	<i>Description</i>
Globally Harmonized System (GHS) of Classification and Labelling of Chemicals	<p>Recently, several international trade, manufacturing, and labor organizations came together to address the disparities in how materials safety was dealt with across industries and around the world. The result is the <i>Globally Harmonized System of Classification and Labelling of Chemicals (GHS)</i>, which is a standardized system for classifying and labelling chemicals. Under this system, the GHS systematically:</p> <ul style="list-style-type: none"> <li>• Defines hazard criteria for chemical types, including the related physical, environmental, and health risks they pose.</li> <li>• Using a unified classification process, classifies each chemical based on available data and the hazard criteria it meets.</li> <li>• Communicates the hazards that each chemical poses and the protective measures that should be taken to prevent them (via labels and data sheets).</li> </ul>
Material Safety Data Sheets (MSDS)	<p><i>Material Safety Data Sheets (MSDS)</i> have been the long accepted standard for classifying and labelling chemical-based materials, as well as providing relevant safety information. While the exact format may appear different, general sections regularly include:</p> <ul style="list-style-type: none"> <li>• Product name and other known/generic names.</li> <li>• Chemical makeup.</li> <li>• Flammability/explosiveness information.</li> <li>• Health exposure risks and first aid guidelines.</li> <li>• Storage guidelines.</li> <li>• Manufacturing details.</li> </ul>
Safety Data Sheets (SDS)	<p><i>Safety Data Sheets (SDS)</i> are the new, highly standardized version of MSDS based upon GHS guidelines. The intent is to make the same information available in a familiar format regardless of industry, region, manufacturer, etc. SDS are already replacing MSDS, particularly in domestic MCO industries.</p>



**Note:** GHS is not a regulation in and of itself, and individual nations have chosen different timelines and degrees to which adoption is being enforced. As many material manufacturers and suppliers are international organizations, and they want to continue doing business in all markets efficiently, it is likely they will lead the charge for adopting and following the GHS standards, even in regions where GHS is not yet required.



## ACTIVITY 7-2

### Identifying Common Safety Hazards and Related PPE

#### Scenario

In this activity, you will identify common safety hazards and their related PPE.

1. **Which type of personnel protection is designed to limit access to machinery or equipment with potentially dangerous moving components?**
  - Personal Protective Equipment
  - Lock Out/Tag Out
  - Safety barriers/machine guards
  - Chemical cabinets
  
2. **Any warning or other informative labels that a manufacturer has placed on a device or material can be removed once it is in place in your MCO facility.**
  - True
  - False
  
3. **Which type of personnel protection is designed to physically secure and notify personnel of machinery or equipment with potentially dangerous energized conditions?**
  - Personal Protective Equipment
  - Lock Out/Tag Out
  - Safety barriers/machine guards
  - Chemical cabinets
  
4. **Any space with limited paths for entry and exit or that have poor ventilation need to be clearly marked for personnel safety.**
  - True
  - False
  
5. **Which standardized Materials Safety and Awareness system provides guidelines for classifying and labelling chemicals in a consistent manner, regardless of country or language?**
  - GHS
  - SDS
  - MSDS
  
6. **Which type of personnel protection is designed to minimize the risk of injury by physically placing special clothing, devices, or other gear on a person's body?**
  - Personal Protective Equipment
  - Lock Out/Tag Out
  - Safety barriers/machine guards
  - Chemical cabinets

7. When working with hazardous materials, showers and eye wash stations should be located in the immediate vicinity in case of an emergency.
- True
  - False
8. Which type of personnel protection is designed to store, secure, organize, and label hazardous materials in a safe, specific location in a facility?
- Personal Protective Equipment
  - Lock Out/Tag Out
  - Safety barriers/machine guards
  - Chemical cabinets
-

# TOPIC B

## Emergency Response Procedures

When dealing with the types of equipment and materials that you are likely to encounter in an MCO facility, there is a high likelihood that some sort of emergency will occur. Being prepared to respond to a variety of emergency events helps ensure that your MCO facility can withstand the emergency and quickly return to normal operations, with limited interruptions, damage, and serious consequences. As an MCO operator, you are responsible for understanding the potential threats to your facility and how to appropriately respond to each. In this topic, you will identify emergency response procedures in an emergency response plan.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- IAP (Incident Action Plan)
- Hazardous material
- Biohazard
- Nuclear material

## Incident Reporting

As you may recall, an *incident* is any occurrence, natural or man-made, that may cause harm and which requires action in order to maintain the functional operation of a facility and offer protection to people and/or property. Immediate reporting of any incident, no matter the size or severity, should not be downplayed and every incident must be documented. Minor incidents can worsen over time and become more of an issue. If there is no report of the initial incident, it may be difficult to recreate the specific details. Immediately reporting an incident also allows for corrective action to be taken sooner and may help to prevent similar future occurrences.

An *incident report* needs to include all the essential information. This begins with fact finding and ends with recommendations for preventing such incidents. An incident reporting form may exist, but—in any case—the following tasks should be completed and the information included in the incident report.

<b><i>Incident Reporting Task</i></b>	<b><i>Information to Include in Report</i></b>
Gather and record all the facts	<ul style="list-style-type: none"> <li>• Date, time, and specific location of the incident.</li> <li>• Name, job title, department, and supervisor of any employee involved.</li> <li>• Names and accounts of witnesses.</li> <li>• Events (if any) leading up to the incident.</li> <li>• The details of the incident.</li> <li>• Any environmental conditions that occurred at the time of the incident (weather, electrical outage, etc.).</li> <li>• Damage sustained to equipment, materials, data, etc.</li> </ul>

<b>Incident Reporting Task</b>	<b>Information to Include in Report</b>
Describe the sequence of events	<ul style="list-style-type: none"> <li>• The cause of the incident, including (if possible) an analysis of the contributing factors leading up to the event.</li> <li>• The events that took place during the incident, described in sufficient detail to portray a clear picture of what happened.</li> <li>• The events that took place immediately following the incident, described in sufficient detail to portray a clear picture of what happened.</li> <li>• Any available photos or diagrams that show or support the series of events.</li> </ul>
Recommend corrective actions (immediate and long-term)	<ul style="list-style-type: none"> <li>• Determine any employee/staff training that could help prevent or better mitigate a similar incident in the future.</li> <li>• Preventative maintenance processes that will help keep equipment in good operating conditions.</li> <li>• Evaluate operating procedures for affected equipment/devices and, as needed, make recommendations for changes.</li> <li>• Consider design and/or engineering changes that could prevent a similar incident in the future.</li> </ul>

## Public Response Systems

In the event of an incident, especially one affecting the general public, there are various standardized approaches that could and/or should be followed in order to respond in a consistent, well-coordinated manner. While there are a number of other Incident Management Systems (IMS) available, the most recognized and followed in the United States is the National Incident Management System (NIMS), developed by the Department of Homeland Security. This system, which was established in 2004 and then revised in 2008, provides responders a consistent process for incident response that better enables government, private-sector, and non-governmental organizations (NGOs) to coordinate their response efforts during domestic incidents.

## Notifications and Communication

A detailed and well-documented process for notifying the appropriate individuals or groups during an emergency is critical. This process shouldn't just sit in a file cabinet somewhere, either—it needs to be *practiced*. Someone in your organization should be the point person and, as an MCO operator, you need to know who that person is.

The following are a few communication methods to notify the necessary parties in the event of an emergency.

<b>Method</b>	<b>Description</b>
Phone Trees	Every institution should have an established protocol to contact specific individuals within the organization that need to be notified of the emergency, no matter how minor the event may be. A simple emergency phone tree—sometimes called an escalation path, since communication is not limited to phones these days—identifies who should contact who (usually beginning with the Public Information Officer) and provides all contact information (office number, home number, cell phone number, and email) for everyone that needs to be contacted. A phone tree also delineates what to do if you can't reach someone and closes the loop when all are contacted. Since it is the sole record of who to contact in an emergency, it should be tested on a regular basis and kept up-to-date by assigned personnel.
Mass Notification Systems	While a phone tree is used to contact specific individuals within the organization, certain events will require mass notification to inform all facility personnel and others occupying the facility of an emergency event. Mass notifications can be sent by automated text or cell phone calls (sometimes called "robo calls") to all personnel, through a public broadcast system (i.e., building-wide speaker system) within the facility, or via speakers or sirens in the outdoor spaces surrounding the facility.

## IAPs

An *Incident Action Plan (IAP)*, sometimes also called an Emergency Action Plan (EAP), describes the procedures that should be followed in any event that has the potential for disrupting the normal operations of a facility. The IAP should be unique to the specific site's operations.

During the initial planning process for the IAP, the various personnel or organizations that would be engaged in an emergency are gathered together to form the plan itself. These key individuals brainstorm the types of incidents that could occur, develop an action-centered plan for each potential incident, determine how to communicate the plan proactively to the necessary parties, and decide how to evaluate and revise the plan (if needed) on a regular basis. The IAP should clearly describe the roles that individuals will be responsible for, the resources that may be required, any potential health and safety issues that could arise, and contingency plans to deal with anything unpredictable (like the weather).

## ICS

In the event that a minor incident at a facility escalates beyond the control of onsite staff, the use of a nationally approved system is recommended. The Federal Emergency Management Agency (FEMA) has coordinated an Incident Command System (ICS), a unified system that provides all partners involved in an incident (in-house staff, emergency personnel, non-governmental organizations, and local state and federal agencies) the ability to coordinate and unify the efforts in a defined manner. As an incident escalates, this process provides clear guidance to those managing the incident.

## Fire Drills

A fire drill is meant to provide the personnel in a facility with the opportunity to practice the emergency response and evacuation plan in a controlled environment, but as though a real fire had occurred. Typically, personnel (and emergency response teams) are notified in advance that a drill will be taking place at a specific time; then, the fire alarm system is triggered to signal that the fire drill is happening and all personnel evacuate the building using their predetermined egress routes. In many cases, the amount of time it takes to evacuate the entire building safely will be measured, to make sure that the emergency plan is functioning according to design.

Fire drills are often mandated by the state and instituted by the onsite Fire Marshal or the Environmental Health and Safety (EHS) officer. In smaller or standalone operations, these positions may not exist, in which case personnel should work with local municipality to establish a fire drill procedure and document both the process and the occurrence of on-going drills.

## Utility Outages

In the event of a utility outage, there are a number of actions that should be taken in response. Once an outage has been detected, you should initiate the notification/escalation process to communicate the event to the necessary parties. Immediately after that, you should evaluate the facility's infrastructure, to verify that the facility is operating on a backup power source and that all critical equipment is operating properly on the backup source. You should think about and check on all the equipment: make sure that everything has swapped over automatically, and there is nothing that needs to be handled manually. If there is limited power available, you may consider evacuating any non-essential personnel from any critical spaces to prevent unnecessary power usage from the limited source and to prevent any potential accidents.

Once you have verified that critical personnel and equipment are safe and operating properly on backup power, only then can you attempt to determine the cause of the utility outage and find out more information about how long the outage may occur. Hopefully, by this time, the utility company (or, for some facilities, the local utility plant operator) has communicated this information with you; if not, you should definitely check in with them to find out the cause (weather, an accident or other event, etc.), if it is a localized event specific to your facility or a wider-reaching event to the larger region, and how long they anticipate that the utility power will be out of service. With this information in mind, you can then prepare a longer-term plan for keeping critical spaces up and running on the available backup power.



**Figure 7–7: Inclement weather brings down tree branches on power lines, causing a utility outage. (Source: Robert Lawton/Creative Commons (CC BY-SA 2.5)/[https://commons.wikimedia.org/wiki/File:Crossed\\_wires.JPG](https://commons.wikimedia.org/wiki/File:Crossed_wires.JPG))**

## Fires

The proper response to a fire in an MCO facility will really depend on the specific event and the particular facility. First and foremost, some actions that MCO personnel might take to combat the fire could actually be prohibited by site rules, insurance requirements, and so forth. Generally speaking, however, the size and severity of the fire should determine what actions to take: if it is clearly small enough to be controlled and/or extinguished with an appropriate class hand-held fire extinguisher, MCO personnel can (and should) do so. Otherwise, the best course of action is to evacuate the area, allow installed fire protection systems to do their job, and notify emergency personnel.

In all cases, the safety of people in the vicinity are your priority. Even if the most critical piece of equipment in the facility is on fire and you can put it out yourself fairly easily, if anyone has been injured due to the fire or other extenuating circumstances, you need to attend to their injuries first and have emergency responders or specific facility-related fire personnel attend to the fire.



**Figure 7-8: A firefighter puts out a fire during a facility drill practicing fire response procedures. (Source: United States Navy/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:US\\_Navy\\_080730-N-5277R-003\\_A\\_Commander,\\_Naval\\_Forces\\_Japan\\_firefighter\\_douses\\_a\\_fire\\_on\\_a\\_dummy\\_aircraft\\_during\\_the\\_annual\\_off-station\\_mishap\\_drill\\_at\\_Naval\\_Support\\_Facility\\_Kamiseya.jpg](https://commons.wikimedia.org/wiki/File:US_Navy_080730-N-5277R-003_A_Commander,_Naval_Forces_Japan_firefighter_douses_a_fire_on_a_dummy_aircraft_during_the_annual_off-station_mishap_drill_at_Naval_Support_Facility_Kamiseya.jpg))**

## Gas Leaks

A gas leak can be hazardous to both personnel and the environment. Not only is it a fire hazard (since it is a highly flammable gas), but it can be incredibly harmful to humans, can kill nearby vegetation, and can release harmful greenhouse gases into the atmosphere.

To help you determine if there is a gas leak, you can use the three senses of smell, sound, and sight. If there is a leak, you will smell the distinct, pungent smell of rotten eggs. You may hear a hissing noise (if the leak is small) or a more distinct roaring or rushing noise (if the leak is large). You may

see dirt or dust blowing near the leak, or you may see bubbles forming in liquid near the leak. In fact, one method of determining if you have a gas leak is to place a mixture of detergent and water on the area of a suspected leak; if it bubbles, you've found the leak. There are also a number of gas-detecting devices, both fixed and portable, that can be used to help detect the presence of gas in a space.



**Figure 7-9: A portable gas detector can be used to monitor hydrogen concentration. (Source: Sansumaria/Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:Detector\\_for\\_Gas.jpg](https://commons.wikimedia.org/wiki/File:Detector_for_Gas.jpg))**

Gas leaks can be difficult to detect, but once they are detected, you have to act quickly: call 911, call emergency personnel, and evacuate the area. In the meantime, do not use anything that would cause a spark that could ignite the gas fumes, including lighters, matches, cigarettes, telephones (including cellular), flashlights, or motorized equipment. Don't attempt to operate gas pipe valves on your own if there is a leak, as this may worsen the situation.

## Severe Event Preparation

In addition to these more commonplace emergency events that every facility could experience, such as a fire or utility outage, there are more severe, unpredictable events that MCO personnel need to be prepared for. MCO management should spend some time evaluating the likelihood that your site may be affected by the following types of severe events and have a plan in place for how to respond to them.



<i>Event</i>	<i>Description</i>
Inclement weather	<p>The various types of inclement weather—excessive/extreme snow, rain, heat, or cold—could each have their own unanticipated consequences on an MCO facility, and need to be planned for accordingly. In most cases, there are some general questions that you should ask to help evaluate your facility's susceptibility to and readiness to respond to each kind of severe weather event.</p> <ul style="list-style-type: none"> <li>• Snow: Is your facility at all susceptible to extreme amounts of snow? Is any equipment exposed to the weather and could become difficult to access? What is the load capacity of the roof? At what point will the facility close due to hazardous travel related to the weather? Is the facility prepared to shelter staff overnight if travel is impossible?</li> <li>• Rain: Is your facility at all susceptible to extreme amounts of rain? Is your facility in a flood plain? Are all roof drains, gutters, storm water pipes, etc. installed, operating, and maintained appropriately? Does the grade around the facility slope away from the building? Is all equipment (internal and external) elevated sufficiently above any potential flooding levels?</li> <li>• Heat: Is your facility at all susceptible to extreme hot conditions? What is the maximum temperature at which your critical equipment can functionally operate? If there is an unanticipated utility outage related to the heat (brownouts, blackouts, etc.), is critical equipment backed up to generator power and is it automatically transferred to it?</li> <li>• Cold: Is your facility at all susceptible to extreme cold conditions? What is the minimum temperature at which your critical equipment can functionally operate? Are any pipes susceptible to freezing, can they be shut off and/or drained if needed, and what would be the consequences? If there is an unanticipated utility outage related to the cold, is critical equipment backed up to generator power and is it automatically transferred to it?</li> </ul>
Onsite emergency events	<p>As MCO facilities have become more susceptible to acts of foreign or domestic terrorism, lockdowns or shelter-in-place events are becoming more commonplace. While most of these kinds of events are impossible to predict, you should evaluate the likelihood that your facility may experience this type of event; regardless of susceptibility, you should always have a plan in place for acting and responding to an emergency event of this nature.</p> <p>The responses for other types of onsite emergencies—such as electrical outages, fires, or accidents related to hazardous materials—are covered in greater detail in their own separate sections.</p>

<i>Event</i>	<i>Description</i>
Local and regional emergency events	<p>The location of your facility can be as critical as the components within your facility. It is important to be aware of where your facility is in relation to other places or facilities that could experience emergencies, especially any that might in turn affect your facility. Is it close to a major transportation hub (airport/flight paths, train station/train routes, highway/truck routes), where a major transportation accident could affect the facility or personnel?</p> <p>A local or regional emergency event may also include some of the other types of emergencies that have already been discussed (a fire in an adjacent facility or in your region, severe weather, or a utility outage) that may not be affecting your facility directly, but has the potential to escalate. In this kind of event, you should maintain contact with the agencies that are involved in responding to these conditions to be prepared in the event that the emergency escalates and threatens the security of your facility.</p>
Natural disasters	<p>Natural disasters include hurricanes, earthquakes, tornadoes, mudslides, and any other kind of unpredictable natural event that can cause major damage (including some that have already been covered here, like floods, wildfires, blizzards, etc.). These kinds of emergency events can be harmful to both the facility itself (and the critical equipment it houses) and to facility personnel, so your plans will need to be twofold: how to protect the facility/critical equipment and how to protect the people. These plans should include backup operations to keep critical equipment operating or to protect important data, as well as evacuation or shelter-in-place plans to keep your personnel safe.</p>

## Case Study: Failing to Plan Ahead

Failing to plan ahead for any emergency event at an MCO facility can have disastrous—and in many cases, even dangerous—consequences for the facility, its personnel, or any of the general public that relies on the services or products that the MCOs provide. Let's take a look at what could potentially happen when a facility fails to plan ahead.

A pharmaceutical facility has been located in the Philadelphia suburbs for over 30 years. At the time it was built, the location was classified as outside of a 100-year floodplain, deeming it nearly flood-proof. For this reason, though, they did not construct the facility with the most precise flood-related design in mind—the extent of plumbing intended for use in the case of a flood were floor drains and emergency sump pumps. Over the years, the eight one-story, stand-alone buildings and surrounding grounds have been upgraded, and it is now considered a state-of-the-art facility, including an environmental health and safety office and a highly trained facilities staff.

In recent years, strong summer storms with intense rainfall have increased, and have been resulting in ponding in the parking lot and on road surfaces. Then, last summer, a series of storms rolled through, with heavy rain almost daily over a two week period. After the first week, standing water formed in the parking lot and remained there for two days. By the beginning of the second week, the water in the parking lot wasn't draining at all—the catch basins were pushing water out instead of allowing water to drain. Low sitting cars were told not to park in the parking lots and employees wore boots or flip-flops to walk from building to building.

By the middle of the second week, the water had risen above the thresholds of the buildings, which were equipped with the floor drains and sump pumps. However, the floor drains were piped to the storm water system which was, unfortunately, also operating as the overflow drains for the parking lots that were now filled with water. The sump pumps that had been installed had been intended only to be used as a last resort, and hadn't been used or tested in several years; several were no

longer operating and those that were only dumped water into the already flooded parking lots. Although the research lab benches were sufficiently elevated off the floor, the storage racks full of pharmaceutical products and other equipment used in research were all floor-mounted.

But this became the least of the facility's problems. The chillers for the air conditioning system located outside the building had been installed on 6-inch concrete pads, and were now sitting in 12 inches of water—causing them to automatically shut down. Temperature and humidity levels in the buildings rose, and the facilities personnel had no ability to control them. To make matters worse, the primary server room for the entire complex was not equipped with an independent system. The temperature rose to a point where the servers shut down and all the important company data for the past thirty years was lost—all because of a few week's worth of rain.

## ACTIVITY 7-3

### Failing to Plan Ahead: Reflective Questions

#### Scenario

Based on the previous case study, think about the following questions in regard to how this specific scenario relates to Mission Critical Operations.

1. What does this scenario tell you about the importance of having an emergency response plan in place when it comes to MCOs?
  
  
  
  
  
  
  
  
  
  
  
  
  
  
2. What plans should have been put into place or what actions should have been taken that could have prevented and/or mitigated the situation at the pharmaceutical facility?

---

## Hazardous Materials

The term *hazardous material* (often simply called "hazmat") refers to any substance—liquid, solid, gas, or combination thereof—that can be harmful to people and/or the environment. The identification and awareness of hazardous materials is particularly important in the event of accidents or misuse, but the hazards likely exist even with proper handling and application.

MCO personnel must be fully trained in the proper handling of hazmat, specifically with the PPE required during use. Operators and technicians also need to know what the risks are related to these kinds of materials, how to respond to spills and contamination, and the proper protocols for transport and disposal.



Figure 7-10: A sign on the Pennsylvania Turnpike denotes which hazardous materials are prohibited from being transported through a tunnel along the highway. (Source: Shanel/Creative Commons (Public Domain)/<https://commons.wikimedia.org/wiki/File:Prohibitionboard.jpg>)

## Spills and Leaks

When it comes to hazardous materials, there is always the potential for the substance to spill or leak. As with most hazards in MCOs, if there is a life-threatening situation, always address that first, particularly if someone has become incapacitated. Allowing the leak to get worse, equipment damage, or further contaminating the space all take a backseat to the safety of your colleagues and other people in the vicinity. Beyond that, the next action that you should take is to stop the spill or leak, whether that is securing the source of the leak or preventing it from further affecting the space.

There are a number of different types of spills and leaks that could happen in your MCO facility; and you need to be aware of each type and be prepared to handle them.

<i>Type</i>	<i>Description</i>
Fuel leaks	Fuel leaks present two primary concerns: chemical contamination and fire hazards. Clearly, most fuels are not environmentally friendly, may cause irritation of skin and eyes, and are at least somewhat harmful if ingested. When possible, the fire hazard should be addressed first by securing the source of the leak, ideally via remote shutoff devices. Outside of very rare and extreme circumstances, this should always be a top priority, even if it means shutting down the mission critical systems.

<i>Type</i>	<i>Description</i>
Refrigerant leaks	Refrigerant leaks are not the most easily detectable unless on a large scale. In contact with skin or the eyes, refrigerants will likely cause chemical and/or thermal burns (instant frostbite in most cases). Most refrigerants that are significantly harmful to the environment have been phased out, so that is not an immediate concern, although we want to minimize what we do discharge. Some refrigeration equipment has recovery features built in to take over upon shutdown, so securing the gear could actually exacerbate the situation. Ideally, competent personnel should be alerted for response, but if there is some amount of urgency, look to isolate the leak if clearly evident.
Electrolyte leaks	Electrolyte or battery acid leaks from battery systems are another ever-present concern in MCO facilities. While the likelihood is low if batteries are maintained properly, there is always a risk for material failure or an accidental spill during maintenance (such as over-filling a flooded wet cell). Almost all battery solutions are highly caustic, causing chemical burns on the skin, damage to eyes, and serious harm if ingested. Absorbent material should already surround battery strings in a good installation, but additional “socks” may be needed to stop a leak from spreading beyond these boundaries. Eyewash stations and/or showers should be located in close proximity to batteries in the event of personnel exposure.
Chemical spills	There are any number of different chemicals onsite at MCO facilities, each with their own set of safety hazards. Stopping the source of the spill or preventing the spill from spreading is always your top priority. With chemical spills in particular, you should never attempt to start cleaning up a spill without donning proper PPE. As with all hazardous material spills, materials used for cleanup should be disposed of separately, and may require special handling. Unless there is a life threatening situation, you should not attempt to start cleaning up a chemical spill without first taking the time to review the MSDS/SDS for the specific chemical or chemicals.

## Case Study: Disaster in Bhopal

As noted, spills and leaks can have damaging, harmful effects on both people and the environment. This was the incredibly unfortunate case following a serious toxic gas leak at the Union Carbide India Limited (UCIL) pesticide plant in Bhopal, India—commonly considered the worst industrial accident in history.

The UCIL plant was located in an area surrounded by the small shanty towns where thousands of people lived. The plant used many chemical substances in the production of its pesticides, including methyl isocyanate (MIC)—a highly toxic substance that is extremely hazardous to humans. On a night in early December, 1984, a malfunction in some pipes and valves allowed water to enter one of the MIC holding tanks, causing a chemical reaction and increased pressure in the tank. The emergency venting system engaged, releasing around 30 tons of a dangerous mix of MIC gas and other chemicals into the air. The gas cloud, buoyed by winds, made its way out of the plant and into the neighboring shanty towns.

While the cause of the leak is still a matter of debate—the Indian government says that a lack of routine pipe maintenance caused a backflow of water into one of the holding tanks, while Union Carbide Corporation (the plant's holding company at the time) contends that someone sabotaged the holding—its consequences are undeniable. More than 558,000 people have experienced injuries from the event, close to 4,000 of which are permanent disabilities. The official death toll, according

to the Indian government, was close to 4,000 people (though others have estimated that closer to 8,000 died within the first two weeks of the accident and another 8,000 have died from related issues in the years that followed).

Additionally, facility records showed that there had been seven other chemical-related incidents at the plant in the eight years preceding the disaster, five of which were MIC or other chemical leaks that resulted in severe injuries to the workers involved. In one case, in 1982, 24 workers were exposed to a gas leak and were admitted to the hospital, because they hadn't been required to wear PPE to protect them from the toxic fumes. In most of these cases, local authorities were aware of the issues and had warned the company of these problems, but no corrective actions were ever taken. Evaluation of the facility after the disaster also pointed to a lax attitude towards safety precautions, including the lack of proper maintenance of critical equipment.

The long-term effects continue to this day, with many who live in the immediate vicinity suffering from neurological disabilities, blindness or other vision issues, skin and respiratory disorders, and birth defects. It's possible that these ongoing medical issues are linked to the environmental effects of the disaster, as the soil and ground water surrounding the plant have been confirmed as contaminated with the toxic substances released during the event.

Cleanup of the site continued for close to 15 years, but stopped in 1998 when the holding company at the time, Eveready Industries India Limited, terminated its lease and gave control of the site to the state government. Environmental tests in the years since have shown that the affected area continues to be contaminated. 20 years on, samples taken of the local drinking water have levels of contamination 500 times higher than the maximum amounts (according to the World Health Organization) and groundwater tests show that contamination can be found almost two miles from the facility. As recently as 2011, environmental scientists and activists have called for renewed efforts to finish cleanup of the site and address the ongoing environmental effects of the Bhopal disaster—more than 30 years after the initial event.

# ACTIVITY 7-4

## Disaster in Bhopal: Reflective Questions

### Scenario

Based on the previous case study, think about the following questions in regard to how this specific scenario relates to Mission Critical Operations.

---

1. What does this scenario tell you about the important responsibilities you have as an MCO technician in an MCO facility, especially if you are working with hazardous materials?

2. What could have and likely should have been done to prevent the Bhopal disaster?

---

### Biohazards

Typically, a *biohazard* is dealt with separately from the other hazardous materials, as it refers specifically to any biological substance that can cause harm to personnel and/or the environment, such as bodily fluids, medical waste, biological toxins, bacteria/viruses, and other biologic materials.

The most common source of biohazard for MCO personnel is each other. Viral or bacterial infections coming from bloodborne pathogens may be spread if you're treating a co-worker that is bleeding or has any open wound. Even seemingly innocuous scenarios like cleaning up vomit should be treated with the same care as blood. First aid kits are an inexpensive preventative measure, and providing gloves, antiseptics, coverings, etc., help to prevent it from spreading. For medical research facilities specifically, the sources of biohazard are numerous and will require site-specific training on handling these systems and addressing related casualty situations. In these kinds of facilities, where the biohazards are more serious and severe, the use of PPE may be required.





**Figure 7-11: Medics practice donning PPE before going out into the field to work in medical centers treating the Ebola virus. (Source: Simon Davis/DFID – UK Department for International Development/Creative Commons (CC BY-SA 2.0)/[https://commons.wikimedia.org/wiki/File:Army\\_trainers\\_teach\\_NHS\\_medics\\_how\\_to\\_put\\_on\\_Ebola\\_safety\\_suits\\_\(15650293350\).jpg](https://commons.wikimedia.org/wiki/File:Army_trainers_teach_NHS_medics_how_to_put_on_Ebola_safety_suits_(15650293350).jpg))**

## Nuclear Materials

The term *nuclear material* technically refers to two types of materials: it can be any substance that possesses radioactive properties (such as cobalt or cadmium metals), or any substance with fissionable properties that can sustain the chain reaction that creates energy (commonly including uranium, plutonium, and thorium metals). The presence and use of nuclear materials is not limited to power plants alone; medical imaging equipment and other industry-specific test equipment, for example, uses radioactive sources. However, nuclear material should always be clearly marked and only trained personnel should be allowed to interact with these systems.

Regardless of the type or use, nuclear materials present obvious safety risks. Nuclear hazards can come from exposure to radioactive fluid (liquid or airborne leaks), contamination, or radiation energy. Once you have ingested radioactive material (whether through breathing, swallowing, or entry into open wounds), it is difficult to treat and may be life-threatening as the radiation will now exist inside your body. In the case of contamination, special showering/scrubbing stations and procedures will help to mitigate the hazard. In both cases, it is not the material itself that is dangerous, but exposure to the resulting energies from radioactive decay of its particles that damages your cells. The same holds true for emergencies where radiation shields for equipment or material have failed. For all nuclear safety incidents, it will be vital to seek medical attention from providers specifically trained in radiation sickness. In the event of a nuclear emergency, evacuation is a common response, although there may be limits as to where you may go if there is concern for further spreading contamination until all personnel can be evaluated for it.

The storage of nuclear waste is a concern for industries outside of nuclear power, although generally on a much smaller scale. Regardless of the amount of waste, though, the proper transportation and storage of nuclear waste is incredibly important. These waste materials continue to be hazardous because they remain radioactive long after their commercial/industrial use is finished. When

transporting and storing these materials, proper care must be taken to ensure the source is shielded to the best extent possible to prevent radiation exposure to personnel.

# ACTIVITY 7-5

## Identifying Proper Emergency Responses

### Scenario

In this activity, you will identify the proper response to take for a variety of emergency situations.

- 1. When documenting an emergency event and your response to it in an incident report, which of the following steps do you need to take to ensure you have the most complete information about the incident?**
  - Attempt to recreate the event.
  - Gather all the available details about the event.
  - Speculate about the potential cause.
  - Thoroughly describe the event, as it happened.
  - Recommend corrective actions.
  - Recommend punitive actions.
- 2. To notify facility personnel and anyone occupying an affected space of an emergency, you should use a method of mass notification such as an automated call or text service or public announcement over a broadcast system.**
  - True
  - False
- 3. During the initial preparation of an Incident Action Plan, what tasks should the key stakeholders complete to make the most comprehensive plan?**
  - Brainstorm all of the various incidents that could possibly occur at the facility.
  - Research incidents that have taken place at other similar facilities.
  - Develop an action-centered response plan for each possible incident.
  - Practice a drill of each response to ensure that it works as planned.
  - Determine how to communicate the plan to the necessary parties.
  - Decide when and how to evaluate and revise the plan, as needed.
- 4. Nuclear materials should always be clearly marked and only trained personnel should be allowed to interact with them.**
  - True
  - False
- 5. Regardless of the type of emergency event, what should always be the priority action in your response?**
  - Finding and stopping the cause.
  - Preventing it from spreading or getting worse.
  - Attending to any injuries.
  - Evacuating non-critical personnel.
  - Fixing the issue causing it.

6. **Aside from making sure that personnel are safe or their injuries are being attended to, what is the first action you should take in response to a utility outage at your facility?**
- Evaluate the infrastructure to check that critical equipment successfully connected to backup power sources.
  - Determine the cause of the utility outage.
  - Communicate the outage with the necessary parties via the appropriate notification method.
  - Consider evacuating non-essential personnel to prevent unnecessary usage or further injuries.
  - Communicate with the utility provider to determine outage duration.
7. **Regardless of the size or severity of the fire, you should always attempt to put it out yourself.**
- True
  - False
8. **Aside from making sure that personnel are safe or their injuries are being attended to, what is the first action you should take in response to a gas leak in your facility?**
- Detect and determine the source of the gas leak.
  - Evacuate the area around the gas leak.
  - Discontinue use of any device that could ignite the gas fumes.
  - Contact emergency personnel and outside emergency responders.
9. **When dealing with a spill or leak of a hazardous material, once you have attended to any injuries resulting from the accident, you should attempt to fix the source of the contamination immediately.**
- True
  - False
10. **Which of the following would be considered a biohazard? Choose all that apply.**
- Blood
  - Used hypodermic needles
  - Used biofuels
  - Vomit
  - Used facial tissues
-

## Summary

In this lesson, you identified and applied personal safety and emergency response protocols and procedures. As an MCO operator, you need to know the kinds of hazards that could pose a threat to you, your colleagues, and any other people within your facility and know the proper protocols to follow to help keep all of you safe. In the event that an emergency does occur, where any of these hazards become a true threat, you need to be aware of the appropriate emergency response actions to take to attend to any injured, address the situation to prevent it from getting worse and hopefully eliminate the threat, and prevent it from happening again. By following these protocols and procedures, you can keep your MCO facility as safe and secure as possible.



# 8

# Facility Security

## Lesson Objectives

In this lesson, you will identify and apply best practices, strategies, and techniques for establishing and maintaining security for a mission critical facility. You will:

- Identify and apply best practices and standards to ensure physical security of a mission critical facility.
- Identify and apply best practices for controlling access to a mission critical facility.
- Identify proper protocol and procedures for maintaining security at a mission critical facility.

## Lesson Introduction

In a Mission Critical Operations (MCO) facility, it is highly likely that there is very specialized work being done using equipment and materials that only knowledgeable, authorized personnel should have access to. Worse still, as both foreign and domestic terror threats change in nature, MCO facilities are more likely to be the target of unauthorized access with the intent to harm people or damage the facility. Therefore, it is imperative that security protocols are in place, for all aspects of the MCO facility, to ensure that the people and equipment at your facility are safe and operations can proceed without interruption.

As an MCO technician, you need to be aware of the security needs for your particular facility and know what security protocols should be in place to provide a level of security that matches those needs. In this lesson, you will identify and apply best practices, strategies, and techniques for establishing and maintaining security for a mission critical facility.

# TOPIC A

## Physical Security

As a facility where critical—and, depending on the product or service that the facility creates, potentially hazardous—operations are being conducted on a daily basis, your MCO facility needs to be as secure as possible. Implementing all of the available aspects of physical security helps ensure that your facility is protected from any unauthorized access that could pose a threat to the safety and security of the facility and the people inside. As an MCO operator, while you may not be involved in the day-to-day operations of these security components—that would be left to the security personnel at your facility—you are likely to be involved in the design and implementation of the security programs. In this topic, you will identify and apply best practices and standards to ensure the physical security of a mission critical facility.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Deterrent
- Access prevention
- Barrier

### Deterrents vs. Access Prevention

Safeguarding the facility, assets, people, and the property are the first priority in a sound physical security program. Every facility is unique in physical design and architectural layout, which presents various challenges when developing an adequate security design. In theory, there are two "kinds" of physical security programs: those that deter access in the first place and those that prevent access from occurring.

The goal of a security *deterrent* is to physically or psychologically demonstrate to potential attackers that an attempt to breach security will be difficult or even impossible, due to safeguards that may be in place. This can be accomplished by even the most basic means, including warning signs, fences, gates, restricted access points, security lighting, landscaping barriers, vehicle barriers, window decals, height restriction points, and orientation of the facility access points.

*Access prevention* is used to control and monitor traffic flow within certain points of the secured facility. This is accomplished by physical means such as key and locking mechanisms, camera and closed circuit TV systems, access card readers, identification cards, turnstiles, mantraps, reception area design, alarms, biometric scanners, zone controls, security guards, and patrols on site.

### Matching the Necessary Level of Security

A physical security risk assessment must be completed to determine the necessary level of security that must be incorporated and maintained. Based on the level of necessary security, you will need to have a security plan that includes physical security measures that can meet these security needs. A huge part of this planning will include an assessment of the amount and type of information that is within the facility, the types and qualities of physical security assets needed and available, and the ability to secure the safety of building occupants. Security levels may need to be tailored to the individual business based on risk due to physical location, neighboring activities, and the general environment.

Physical security measures may be more expensive to implement and less effective as part of a post-construction effort versus establishing the requirements at the earliest stages of design and planning of the facility. As part of an ongoing risk assessment effort, MCOs must continuously assess whether or not the physical environment is acceptable and if enhancements are needed based on



current conditions and the level of physical security risk. Whenever possible, scalable security solutions should always be considered as part of the design.

## Barriers

A *barrier* is any device or structure that creates a physical (or, in some cases, mental or psychological) impediment to entrance, passage, or movement forward within a specific space or location. When discussing the physical security programs in place for a facility, there are many different types of barriers that can help provide physical security and deter and/or prevent access to your facility by unauthorized or threatening persons.

## Gates, Walls, and Fencing

There are three major types of physical barriers that provide access prevention and deterrence, in the form of gates, walls, and fencing. These serve as the first physical barrier or boundary that indicates that access needs to be (and is being) controlled, and the type and design of the constructed barrier may provide a visual indicator that helps communicate the level of intended security for the space and/or indicate that the space is off limits. Gates, walls, and fences should never be considered an avenue to completely stop a motivated intruder, but rather to deter or significantly delay the progress of an intruder or unauthorized person from entering a location that needs to remain secured.



**Figure 8-1:** Both the sign and the spikes on this barrier wall indicate that unauthorized persons should not attempt to enter the secured space. (Source: Edward/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Security\\_spikes\\_1.jpg](https://commons.wikimedia.org/wiki/File:Security_spikes_1.jpg))

## Manual vs. Automatic Gates

There are two types of gates that can serve as a form of access prevention or deterrence, each with its own valuable security characteristics: manual gates and automatic gates. Manual gates must be opened by a human being and are generally intended for minimal entry and access. Manual gates can be secured by various methods such as padlocks, chains, key and core locks, and locking latch assemblies. Manual vehicle control gates may come in the form of a barrier arm which must be physically raised and lowered, as well as a manual sliding gate that must be pushed open and pulled closed.

Automatic gates may be of the same basic structure and type as manual gates, but have the added benefit of automatic or remote control from an alternate or geographically separated location. Much like a common household automatic garage door opener, automatic gates can be electrically and mechanically controlled to open or close either upon command by an operator, a timing device, an electronic access card reader, or by various types of sensors. In most cases, the physical mechanical and electrical design of the gate operating system serves to physically lock the gate in a desired position upon conclusion of operation.

## Fencing

Fencing is designed to deter or slow down a potential intruder, not just to simply provide a physical or impassible barrier. There are multiple purposes for fencing based on its physical design and intended function or usefulness. Fencing such as chain link serves the purpose of identifying property boundaries and prevents casual trespassers from entering the property as well as imposing vehicle control. The mesh wire of a chain link fence does provide the opportunity to place signage with warnings, instructions, caution statements, and other information intended for those who may approach the fence. Adding the element of barbed wire or razor wire to the same chain link fence enhances a physical barrier to further slow-down or deter a potential intruder.



**Figure 8–2: Fencing with the addition of barbed wire deters entry on to the property surrounding Raleigh–Durham International Airport. (Source: Ildar Sagdejev/Creative Commons (CC BY 3.0)/ [https://commons.wikimedia.org/wiki/File:2008-07-30\\_Fence\\_along\\_Commerce\\_Blvd\\_at\\_RDU.jpg](https://commons.wikimedia.org/wiki/File:2008-07-30_Fence_along_Commerce_Blvd_at_RDU.jpg))**

Other types of fencing may be decorative in nature and can be required for aesthetic purposes per local regulations, established regulations of surrounding homes or businesses, or simply a personal choice of the facility owner or operator. These types of alternative fencing may be incorporated with security fencing for enhanced security purposes, by utilizing a design that obstructs views into the facility or other buildings on the property's boundaries to protect sensitive information that is housed or activities that take place within them.

## Electrical Fencing

The intent of electrical fencing is to conduct a significant and very uncomfortable electrical shock to anyone who comes in contact with the fence, in order to deter the entrance or hinder the progress of a potential intruder and reduce the chances of a second attempt. Electrical fencing may be either added to an existing fence or it can be a complete fencing system designed solely for the purpose of increased deterrence. Any installation of electrical fencing must be clearly marked per regulatory requirements with warning or caution signs to prevent accidental contact by someone who has no intention of breaching the property line.

This type of fencing is generally a visual reminder that the enclosed area is intended to be secured at a higher level, and visually indicates that physical harm may occur if there is an attempt to breach the boundaries. The physical appearance of most electrical fences coupled with the posted warning signs referencing an electrical shock hazard, can definitely be a deterrence to potential trespassers.

Additionally, electrical fencing may be wired to alarm by vibration, motion, or a break in the integrity of the fence or the alarm wiring and related sensor components. Alarming mechanisms on a fence are designed to alert those that are monitoring the security systems to indicate a potential breach of the security perimeter is either in progress or has already occurred. These alarms may be configured to be silent or audible to the intruder, depending on the needs or desires of the facility.

While not as commonplace across all industries, highly sensitive and secure MCO facilities like nuclear sites or sensitive government installations have long relied upon electrical fencing for the impact it has on deterring intruder access.



**Figure 8-3:** A multi-zone electrical fence installed on top of other fencing serving as a physical barrier to entry. (Source: PaktonDale/Creative Commons (CC BY-SA 4.0)/[https://commons.wikimedia.org/wiki/File:Security\\_Electric\\_Fence.JPG](https://commons.wikimedia.org/wiki/File:Security_Electric_Fence.JPG))

## Multi-Layered Fencing

Multi-layered fencing can provide additional physical barriers in the deterrent element of physical security. Multi-layered fencing creates entrapment zones by placing one fence behind another, designed to give the security team the time and opportunity to react and respond to the alarm and physically mobilize to address the security breach. Each layer of fencing may have a combination of various deterrents and physical barriers, such as razor wire, barbed wire, motion alarms, or electric apparatuses to slow the intruder, assuming the individual is able to break through or cross one or more of these protective layers of fencing.

## Vehicle Security

Addressing vehicle security measures is a key component of ensuring physical security is maintained at the facility. Historically, vehicles have been utilized in security breach events, whether as battering rams to gain entry to a facility or equipped with bombs or other explosive devices that result in damage or harm. Both foreign and domestic terrorist events within the last two decades involving vehicles have prompted facilities of all kinds to be engineered and planned with vehicle security measures in mind to deter or minimize a successful attack.

Various engineering designs have been developed and deployed to improve security measures related to vehicles and vehicle traffic control. Utilizing natural or man-made landscaping around the facility to prevent vehicle approach and proximity, designing unique entry access roads to control vehicle speeds, and installing barrier arms, gates, road spikes, and short posts (called bollards) have all been effective in supporting physical security against the potential threats posed from vehicles.



**Figure 8–4: Boom barriers prevent vehicles from entering a restricted area without permission.**  
(Source: Bidgee/Creative Commons (CC BY-SA 3.0)/[https://en.wikipedia.org/wiki/File:Bourke-Docker\\_Street\\_level\\_crossing\\_boom\\_gate.jpg](https://en.wikipedia.org/wiki/File:Bourke-Docker_Street_level_crossing_boom_gate.jpg))

## Vehicle Barriers

Vehicle barriers are an excellent means of providing both a physical and psychological deterrence for physical security. Much like the concrete walls used on roads and highways during construction, jersey barriers prevent vehicle access to zones or areas where vehicle traffic or access must be physically restricted. Additionally, the use of steel and concrete bollards, large concrete planters, and natural or man-made berms (a flat or raised strip of grass or landscaping), creeks, and culverts, are effective means of providing desired separation of vehicles (whether moving or parking) and access control.



**Figure 8–5:** Large concrete planters act as a vehicle barrier to passing traffic in front of the Canadian Embassy in Washington, D.C. (Source: Gryffindor/Creative Commons (Public Domain)/ [https://commons.wikimedia.org/wiki/File:Canadian\\_Embassy\\_DC\\_2007\\_002.jpg](https://commons.wikimedia.org/wiki/File:Canadian_Embassy_DC_2007_002.jpg))

## Location of Parking Areas

Assessing the physical risk as it relates to the location of vehicle parking areas is a critical element in the vehicle security planning process. Ideally, for a higher risk structure, a parking location will be designed to accommodate employees only, and a separate area constructed for visitors, vendors, and others who may have a need to frequent the site. Where applicable and physically possible, a separation distance or buffer zone should be maintained between the structure walls and the parking areas to minimize the effects of a vehicle explosion or fire as it relates to the proximity of the structure.

Parking areas designed below a critical facility is not advisable and should be avoided whenever possible. Parking of this type leaves the facility susceptible to a catastrophic event created by a vehicle explosion or fire. This is especially true if the parking area is beneath an administrative area, under the critical environment space, or simply underneath the support structure of the entire facility.

## Points of Entry

Minimizing and consolidating points of entry is important to allow security to focus on key areas of entry and exit into parking areas and into the facility itself. As multiple entry areas increase, so does the vulnerability of a successful breach of security. Additionally, it is important to assess the level of security that needs to be maintained, as well as the type and quantity of deterrence mechanisms required at each point of entry. For example, access points for badged employees from the entry of the property into the main facility would probably be less restricted than access points reserved for contractors or visitors.

Points of entry into a parking area must be clearly defined and identified to direct vehicle operators to the appropriate parking area that is consistent with the purpose of their visit. Upon entry to the property boundary, vendors and other visitors should identify themselves to security personnel either in person or via intercom devices to state their identity and purpose of visit. This initial contact usually occurs at the first line of deterrence, generally consisting of a gate, barrier arm, or other physical barrier apparatus. If granted access, they should be escorted by security personnel or monitored by camera to ensure they park in the appropriate designated area as directed.



**Figure 8-6:** A sailor, acting in a security role, checks the identification of a visitor before granting her entry to a naval base. (Source: United States Navy/Creative Commons (Public Domain)/ [https://commons.wikimedia.org/wiki/File:US\\_Navy\\_050308-N-2385R-029\\_Master-at-Arms\\_Seaman\\_Carly\\_Farmer\\_checks\\_an\\_identification\\_card\\_\(ID\)\\_before\\_allowing\\_a\\_driver\\_to\\_enter\\_the\\_gate\\_at\\_U.S.\\_Fleet\\_Activities\\_Sasebo,\\_Japan.jpg](https://commons.wikimedia.org/wiki/File:US_Navy_050308-N-2385R-029_Master-at-Arms_Seaman_Carly_Farmer_checks_an_identification_card_(ID)_before_allowing_a_driver_to_enter_the_gate_at_U.S._Fleet_Activities_Sasebo,_Japan.jpg))

Preferably, access into the main facility should be limited and consolidated to one point of entry and exit, and there should be multiple layers of physical security to ensure an unauthorized individual is not able to gain access to restricted or interior areas of the facility. Adequate measures usually require an individual to enter a lobby area in plain view of security personnel. Personnel not displaying an employee badge or access card will be challenged by security to produce the proper credentials to initiate the entry process. In order to gain access, multiple levels of approval will need to be obtained prior to entering the facility past the security checkpoint.



**Note:** The types of access control systems used to limit and verify authorized access to facility spaces will be covered in detail in the next topic.

## Security Checkpoints

Upon entering a secured facility, a security checkpoint should be the first visual barrier or deterrent to an individual with the intention of gaining unauthorized access. A security checkpoint consist of at least one security officer who has full control of the primary access area(s) of the facility, as well as visual monitoring of camera equipment, communications, and key control responsibilities. The

primary purpose of a security checkpoint is to ensure that no one enters the facility without authorization. In some cases, additional security checkpoints may be established within the facility to secure access to other restricted or sensitive areas requiring a higher level of security.

## Locking Mechanisms

Appropriate locking mechanisms, whether mechanical or electrical, are the foundation and staple of a physical security program. Just as we lock the doors to our homes to prevent an unwanted individual from entering, the same is true with an MCO facility in an effort to ensure the safety of building occupants, secure equipment and materials, and to prevent access to unauthorized areas.

Locking mechanisms are designed in a vast variety of styles and purposes, depending on the type and level of security desired. As with other electrical and mechanical devices, locks must be maintained and tested to ensure operational integrity and to ensure proper function. Strict oversight and control of keys, codes, combinations, and electronic access cards is imperative to ensure the functionality and integrity of the locking mechanism element of the physical security program.



**Figure 8-7:** A multiple-deadbolt lockset on a door handle is one type of locking mechanism. (Source: richterfoto/iStock/Thinkstock)

## Lock Functions

Locking mechanisms—of any kind and level of implemented security—are vulnerable when an attacker has the time, tools, and opportunity needed to breach or bypass the function of the lock. Therefore, the function and type of lock must be commensurate with the level of access and the level of protection desired. Some areas of higher risk and vulnerability require a more advanced and sophisticated locking mechanism, while other lower-risk locations or assets require a simple locking device such as a padlock or door handle key and lock mechanism.

The following are a few different types of locking mechanisms that you are likely to encounter in an MCO facility and how they function as part of the physical security program.



<b>Type of Locking Mechanism</b>	<b>Description and Function</b>
Storeroom	A storeroom lock provides the lowest level of security protection and therefore should only be used for the lowest level of risk. It is typically a door lever-type lock, where the outside door handle is always in the locked position unless manually opened with a key. Once the key is removed and the door is closed, the door lock reverts back to the locked position. The inside handle operation is always free to open the door.
Key In/Key Out	Key In/Key Out locks are any types of security locks that must be operated with a key, and cannot be locked or unlocked by any other mechanical means. These may be a door handle lever type, a door knob, or a lockbolt and tumbler set.
Industrial and Institutional use	Industrial and institutional use locks are designed to withstand heavier use applications and are designed with both security and safety in mind. Locking mechanisms of this type include heavy duty lever locks, panic door hardware, and intruder lever locks—all of which are more difficult to damage or bypass.
Fail-Safe and Fail-Secure Electronic Locking Systems	Fail-safe refers to electronic-actuated locking mechanisms that are designed or programmed to be in the unlocked position if power was to be removed from the actuating components of the lock. These are proper locking mechanisms on fire-rated doors where life safety for emergency egress is a consideration. Conversely, fail-secure locks will remain in the locked position when power is removed from the device. These may be utilized on non-fire rated external doors, or other doors that are designed to be remotely released or electronic access controlled.

## Penetrations and Building Integrity

In order to allow for necessary air exchange criteria to be met within the facility, it may be necessary to have penetrations to the interior or exterior walls of the facilities to accommodate proper air circulation for both supply and return air. To maintain the proper level of security, it is vital that these areas are designed to have grated cover plates or other such devices near the louvers or vents that will prevent a potential intruder from entering the facility through these openings.

## Video Surveillance Systems

Cameras and video surveillance equipment provide real-time visibility into structures, restricted areas, parking lots, and across the entire site. Systems that are actively monitored can provide visual evidence of an intrusion or emergency event, and verify if there is truly an intrusion threat or if it is simply a false alarm. This type of electronic advancement can reduce the physical amount of security personnel required to be on site, and can effectively cover more area instead of utilizing patrols to conduct verification checks in key areas of the facility and property. Additionally, cameras are a very effective means of deterrence since just the presence of cameras induces the thought that you are being watched and monitored.



*Figure 8–8: Surveillance cameras monitor and record the actions happening outside of a facility. (Source: Hustvedt/Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:Three\\_Surveillance\\_cameras.jpg](https://commons.wikimedia.org/wiki/File:Three_Surveillance_cameras.jpg))*

## Intrusion Detection

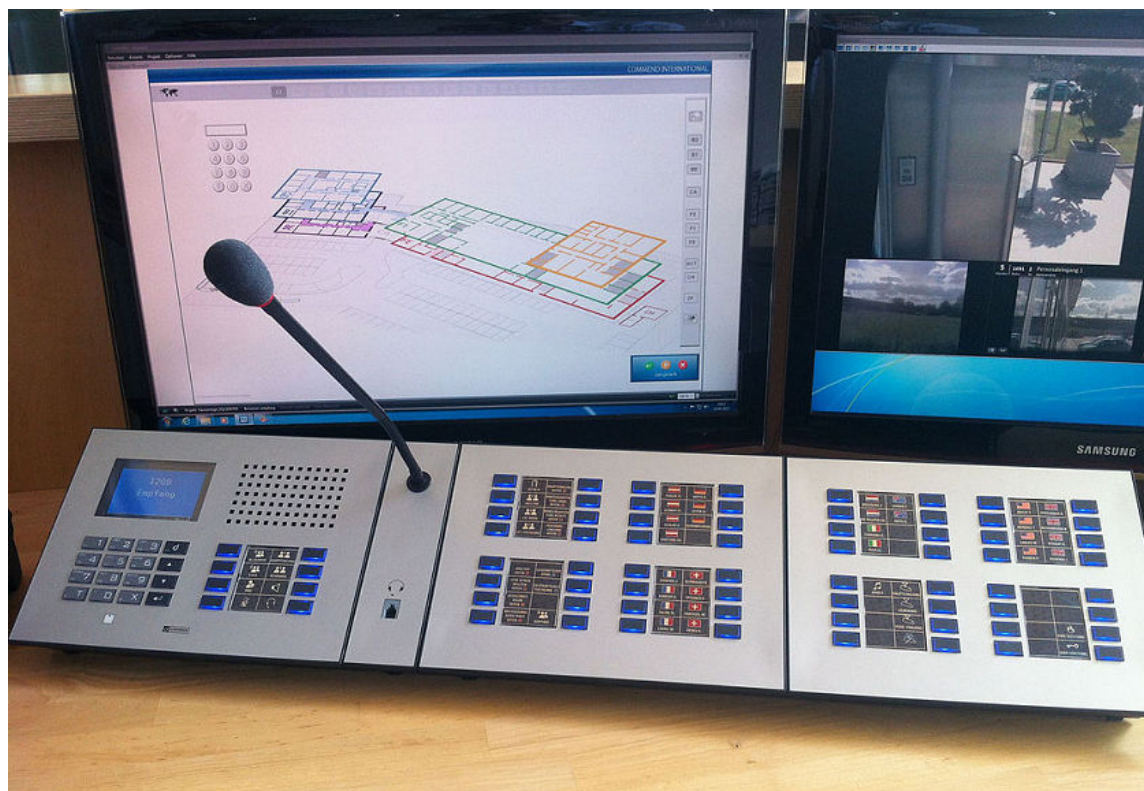
Intrusion detection systems can be the eyes and ears of security personnel, by detecting that a potential security breach has occurred, identifying the location where it took place, and notifying security personnel of the breach. Most utilize some variety of sensors such as motion detectors, heat sensors, door contact sensors, laser beam barriers, touch sensors, and vibration sensors. Activation of these sensors will create an alarm signal to report back to a centralized security location. Intrusion detection alarms may be audible or silent at the location of the event depending on the preference of security personnel and whether or not they want a perpetrator to know an alarm has been activated.



**Figure 8–9:** Motion detectors sense when there is movement in a protected area and can trigger an alarm to notify personnel of a possible security breach. (Source: MileA/iStock/Thinkstock)

## Intercoms, Radios, and Other Security Communications

Proper security communication equipment is vital to the success of security personnel to deliver the physical security program in its entirety. Intercoms are utilized for direct communication to and from various points of the property and facility such as at entry gates or entry lobby areas, and at key points of entry and exit throughout facility zones. Radios provide the ability for security personnel to communicate while being mobile. The ability to be mobile improves response times to emergencies while enhancing life and safety elements as communication can flow simultaneously to multiple locations of the facility.



**Figure 8-10:** An intercom communication system allows security personnel to remotely monitor the facility and communicate any potential breaches immediately. (Source: H.stadler/Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:Intercom\\_Control\\_Desk.jpg](https://commons.wikimedia.org/wiki/File:Intercom_Control_Desk.jpg))

## Placement of Critical Security Equipment and Systems

Depth of security is an important aspect when planning where to place critical equipment and other systems that are vital to the operation of the facility. With critical equipment being the heart of the facility operation, you want to place your equipment in an inner area where it is not only protected by its own security devices, but also those of the surrounding environment. In most cases, this will be the center of the facility, away from exterior walls, doors, or other vulnerable points. Any breaches of an outer security area can be met with another access challenge prior to gaining access to the critical equipment. Security systems and devices that monitor and report on the safe, continued operations of your critical equipment should be implemented and installed in areas with unobstructed views and at a safe distance from any potentially hazardous conditions that could affect the proper functioning of the components.

You also need to take proper precautions to place your critical security equipment and systems in a location where services are least likely to be interrupted or affected by outside factors, such as a common hazard or emergency event. These systems are almost just as vital as the critical equipment that they are designed to monitor and protect, for the simple fact that they provide these necessary security services. Therefore, they need to be functioning properly all the time, making it imperative that they are located in a space that is protected from—or at least separated, either physically or logically, from other systems that could be affected by—emergency events such as loss of power, a fire or flood, or even damage from an intruder.

# ACTIVITY 8-1

## Ensuring Physical Security

### Scenario

In this activity, you will identify the various components that provide physical security for an MCO facility.

1. **For an MCO facility that requires high levels of security, security checkpoints only need to be placed at the points of entry into the facility.**
  - True
  - False
  
2. **Which of the following descriptions accurately describes the purpose of a deterrent?**
  - It is used to physically control and monitor traffic flow within certain points of the secured facility.
  - It is used to physically prevent any attempt to breach the security in place and enter the facility.
  - It is used physically or psychologically to demonstrate that an attempt to breach security will be difficult or even impossible.
  - It is used to physically deny any users, authorized or unauthorized, access to certain points of the secured facility.
  
3. **Which of the following descriptions accurately describes the purpose of access prevention?**
  - It is used to physically control and monitor traffic flow within certain points of the secured facility.
  - It is used to physically prevent any attempt to breach the security in place and enter the facility.
  - It is used physically or psychologically to demonstrate that an attempt to breach security will be difficult or even impossible.
  - It is used to physically deny any users, authorized or unauthorized, access to certain points of the secured facility.
  
4. **Which of the following physical security components are typically placed on the outside of the facility and act as a first-line of defense to deter or prevent unauthorized access to the property?**
  - Gates
  - Berms
  - Surveillance cameras
  - Walls
  - Intrusion detection
  - Fences

5. Which of the following physical security components can be placed outside of the facility and direct vehicle traffic to approved entrances or control/prevent vehicles proximity to the building?
- Gates
  - Berms
  - Barrier arms
  - Walls
  - Bollards
  - Fences
6. To make more use of an MCO facility's space, parking lots could be safely constructed underground, as part of the facility's infrastructure.
- True
  - False
7. Which type of locking mechanism would be best suited for a shared space in a facility that many people would access and has a low level of security risk, such as a bathroom?
- A storeroom lock
  - A key in/key out lock
  - An industrial or institutional lock
  - A fail-safe lock
  - A fail-secure lock
8. Which type of locking mechanism would be best suited for a space that has a very low level of security risk but needs to have limited access, such as a storage closet housing janitorial products?
- A storeroom lock
  - A key in/key out lock
  - An industrial or institutional lock
  - A fail-safe lock
  - A fail-secure lock
9. Which type of locking mechanism would be best suited for the interior door to a production space where personnel works with flammable materials?
- A storeroom lock
  - A key in/key out lock
  - An industrial or institutional lock
  - A fail-safe lock
  - A fail-secure lock
10. Which type of locking mechanism would be best suited for the interior doors used to access a research lab where sensitive materials and data are being developed and housed?
- A storeroom lock
  - A key in/key out lock
  - An industrial or institutional lock
  - A fail-safe lock
  - A fail-secure lock

---

**11. Which type of locking mechanism would be best suited for the exterior doors of a facility where sensitive information is stored?**

- A storeroom lock
- A key in/key out lock
- An industrial or institutional lock
- A fail-safe lock
- A fail-secure lock

**12. Which of the following physical security components monitors for potential security breaches and notifies security personnel if and when a security breach occurs?**

- Security checkpoints
- Video surveillance
- Intrusion detection
- Intercoms and radios

**13. Which of the following physical security components allows security personnel to validate the identification and authorization of people entering or moving about the facility?**

- Security checkpoints
- Video surveillance
- Intrusion detection
- Intercoms and radios

**14. Which of the following physical security components allows security personnel to remain in constant communication about the general security throughout the facility?**

- Security checkpoints
- Video surveillance
- Intrusion detection
- Intercoms and radios

**15. Which of the following physical security components allows security personnel to remotely view, monitor, and capture the activities going on inside the facility or in secured locations outside the facility?**

- Security checkpoints
  - Video surveillance
  - Intrusion detection
  - Intercoms and radios
-

# TOPIC B

## Access Control Systems

A key component of facility security is limiting and controlling who can access the site in general and where within the facility they can access and move about. Overseeing this access helps ensure that only those people who should be are entering or occupying a specific or secured space, and prevents anyone who shouldn't be in those places from getting in—especially if their presence could be a potential threat that could cause injury to themselves or others or damage the equipment or property, even accidentally. As an MCO operator, you will need to know which of the site access control options is best suited for certain security needs, and include them in the security implementation at your site. In this topic, you will identify and apply best practices for controlling access to a mission critical facility.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Biometrics
- Keypad

### Biometrics

*Biometrics* refers to a specific kind of access control system that uses the unique biological "signatures" of individual people to restrict or grant access to protected spaces and/or information.

Most traditionally, we think about fingerprints as being our unique human identifiers, which indeed have been used from some time now in security systems via fingerprint scanners, where a fingerprint scan matching an approved, authorized person will grant access to the secured space. Moving beyond a single fingerprint, palm print scanners are also in use in many industries, although there is some debate as to how much more security they provide. Either way—despite what you see in the movies—fingerprint/palm print scanners are difficult to defeat without bringing a lot of attention to the unauthorized person attempting to breach the security at the access point.

Optical scanners that read highly unique patterns in the iris of your eye provide another biometric security option. The intricacies of the iris provide a much more enhanced level of security than fingerprints, but these systems are notably more expensive to install.

There are audio options as well, most commonly referred to as voice recognition. While voice recognition access systems have become viable options (similar to fingerprint readers), the level of technology and cost to install them is directly related to the level of security provided. Most of us have voice recognition features on our smartphones, but in order to support ease of use and deal with background noise, the sensitivity to detect differences in vocal signatures is low. Thus, in order to get a vocal-biometric system with the level of security needed for a highly sensitive facility, the cost would be incredibly high; for the same cost, high-end fingerprint readers or iris scanners can provide a much higher level of security.





**Figure 8–11:** A fingerprint scanner allows access to a space to authorized personnel. (Source: Tatom/iStock/Thinkstock)

## Access Control Vestibules

Access control vestibules—such as mantraps and turnstiles—are used to create an area that can delay or prevent an unauthorized individual from entering a facility or secured space. Additionally, access control vestibules create a containment area to enable security personnel to respond to an attempted breach of security by virtually trapping an intruder between barrier zones. In most cases, one form of access approval, such as an electronic access card, must be verified to enter the mantrap; then, another form of access approval, such as a biometric hand scanner, must be verified to exit it, and allow the authorized person to enter the secured area beyond the vestibule.

## Security Badges and Readers

Security badges serve two purposes: identify personnel (and possibly their work group or access group) visually and digitally and serve as electronic keys to access spaces. A card reader is the receiver that controls door locks. Traditional card readers typically work like credit card readers, swiping a magnetic strip to operate. Technologies such as radio-frequency identification (RFID) have replaced magnetic readers in many MCO installations, in which simply touching your security badge to the card reader authenticates your identity and access permission, and restricts or grants access.

Proximity readers work on the same principle as the card/badge reader, but with a stronger signal. This allows you to unlock spaces and open doors without having to place your badge immediately adjacent to the reader/receiver, but rather just by being near it—hence, the name. Proximity readers work great when personnel transit often with their hands full of materials/tools, and have specialty applications. In a biotech facility, or any MCO facility regularly dealing with hazardous materials, the spread of contamination can be limited by not having to use your hands to access controlled spaces.

Anti-pass back refers to the digital interlocks between multiple or multiple sets of digital access points. This feature may be utilized when “badging out” of spaces is required: namely, if you badge

into an area, you must badge out of that area or the system will not let you access any other areas. This creates a very detailed record of who has accessed which spaces, when, and for how long—a common requirement in tightly controlled MCO facilities. Additionally, this prevents a common security threat called “tailgating,” where an unauthorized person walks through a secured door behind an authorized user that has used their approved security credentials to gain access.



**Figure 8-12:** An employee swipes a security badge to access a secured space. (Source: Keith Brofsky/Photodisc/Thinkstock)

## Keypads

A *keypad* is a digital or mechanical lock set that operates by entering an alphanumeric code to unlock the mechanism and access a secured space. Mechanical keypads usually just have numbers on them and entering the code in the right sequence releases the tumbler in the lock, just like a key. Digital keypads may be numeric like the pin pad on an ATM, or have full lettering to enter a password or code. The benefits of keypads include not having to hassle with physical keys (include having to issue and reissue keys, change locks if keys are lost, etc.) and not having a cylinder that can be picked, although some keypads do have a keyed tumbler as a backup.



*Figure 8-13: A keypad restricts or grants access to a secured space. (Source: D4m1en/Creative Commons (CC BY-SA 3.0)/<https://commons.wikimedia.org/wiki/File:Digicode.JPG>)*

## Keyed Locks

Keyed locks are traditional locksets that require a specific key to release the tumblers inside the lock and open the door. Keyed locks still have a place in MCOs, but many MCO operators prefer to have the record-keeping abilities of digital lock systems. Commonly, storage rooms, closets, emergency exits, and other less critical, less frequently-accessed doors may still use a traditional keyed lock.

# ACTIVITY 8–2

## Controlling Facility Access

### Scenario

In this activity, you will identify the various security components that can be used to control facility access.

---

- 1. Which type of access control component might be implemented to secure and limit the access to a storage closet where chemicals are stored?**
  - Biometric device
  - Mantrap
  - Proximity reader
  - Keypad-locked door
  - Key-locked door
- 2. Which type of access control component might be implemented to create a containment area outside of a research lab where personnel are working with hazardous biological materials?**
  - Biometric device
  - Mantrap
  - Proximity reader
  - Keypad-locked door
  - Key-locked door
- 3. Which type of access control component might be implemented to permit access in and out of a storage closet within a research lab where personnel are working with hazardous biological materials?**
  - Biometric device
  - Mantrap
  - Proximity reader
  - Keypad-locked door
  - Key-locked door
- 4. Which type of access control component might be implemented for a highly-secure area of a nuclear reactor facility, where unique identification of the authorized user is required to gain access?**
  - Biometric device
  - Mantrap
  - Proximity reader
  - Keypad-locked door
  - Key-locked door

5. Which type of access control component might be implemented on the exterior doors of a production space, near the loading docks, where there have been attempts to breach the security by picking the locks?
- Biometric device
  - Mantrap
  - Proximity reader
  - Keypad-locked door
  - Key-locked door
-

# TOPIC C

## Security Procedures

With the proper security in place to deter or prevent unauthorized access to the facility and control access within the facility, both for authorized personnel and visitors, you can then turn your attention to implement protocols for maintaining security for the entire organization as a whole. This includes establishing security protocols for other aspects of the organization, such as determining who is authorized and for what or protecting sensitive information. As an MCO operator, you will need to know the protocols that will apply to your facility and the proper procedures you should follow to make sure the facility is secure to those standards. In this topic, you will identify proper protocols and procedures for maintaining security at a mission critical facility.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Fire watch
- Confidentiality

## Authorization Procedures

When it comes to permitting people, deliveries, or any other "outside element" to enter an MCO site, there should always be authorization procedures in place that will be followed to assess the person or item attempting to enter and either approve or deny access to the site. According to best practices, the security and operations teams control who and what gets into the facility and are charged with enforcing the authorization procedures that evaluate each entry. There may be multiple levels of approval required to get visitors onto an access list or specific procedures for cross-checking shipping documents with logistics programs before accepting deliveries. The authorization procedures for allowing these outside elements to enter your site should be documented and followed to the letter; if there is ever any gray area, you should default to refusing entrance or delivery until someone from the management team can help sort things out.

## Background Checks

Permanent and semi-permanent MCO personnel are commonly required to submit to background checks before being granted regular access to the facility. Background checks can range from general review of legal records and credit checks, to full government-issued security clearances. Some organizations and security records have effective dates that may expire from time to time, requiring personnel to go through background checks on a periodic basis (often every 5 or 10 years), even if they've held the same job at the same location throughout that time.

## Entry Credentials

All MCO locations, even with nominal security needs and/or staffing, should practice verifying identification of the personnel coming onsite. This is particularly important for guests or other people visiting the site or vendors coming in to work on equipment. Generally, a government-issued ID card is sufficient, but some MCO facilities with heightened security might require a second document to prove identification. Entry credentials may also include some sort of site-specific approved access document.

Validating identification credentials should be enforced for *all* non-resident personnel, even if someone onsite personally knows the visitor—checking for a current and valid identification card can find potential red flags that the visitor could pose a threat to the facility, preventing them from even entering the site where they could possibly do harm or cause damage.

## Site Access Control

Security protocols and restrictions for site access extend beyond simply who or what is allowed through the gates; once onsite, it is still important to maintain awareness of where people are going and control which areas of the site they can access. There are a few common security measures that can be implemented to oversee access to spaces within the site.

<b><i>Access Control Measure</i></b>	<b><i>Function and Description</i></b>
Visibility of waiting areas	<p>Most MCO facilities will have some sort of waiting area where visitors check in and meet site personnel. This area is generally secured from the rest of the facility by at least a locked door, if not more elaborate electronic security measures like mantraps and biometric devices. For security purposes, these areas should remain as highly visible as possible: large windows, glass doors, or (at the very least) video surveillance that allows security personnel to view the visitor at all times. This provides several key benefits: you'll always know who is entering the facility and when, recorded in memory by witnesses or preferably video and other electronic records; you can keep an eye out for anyone attempting to defeat installed security measures; and, it provides a safe, controlled place for site personnel to greet guests, visitors, vendors, etc.</p>
Physical escorts	<p>Depending upon actual site access rules, physical escorts may be required of some or all non-resident personnel as they move about the facility. If escorts are deemed necessary by site protocol, MCO personnel must adhere strictly to the process—yes, that even means walking a visitor to and from the restroom. Think about it in terms of the potential repercussions of leaving any visitor alone, for even two seconds; it only takes those two seconds for them to flip a switch that could have catastrophic consequences.</p> <p>Physical escorts have an even greater level of importance as it relates to today's concerns with cybersecurity, far beyond simply being aware of what equipment visitors or vendors are touching and what they've done to it. While it may seem very James Bond-esque, casually slipping a thumb drive into a random USB port can infect systems with viruses. Worse yet, even equipment that seems to pose little cybersecurity threat (such as a chiller or air compressor) is often connected to networks for performance monitoring, and could be used as a gateway to gain entrance into an organization's confidential data.</p>
Vendor policies and procedures	<p>While in-house MCO maintenance and operations teams tend to do the lion's share of the work to support the facility, vendors and subcontractors are a regular part of our lives: working on proprietary systems, completing major repairs, installing new equipment, etc. The best MCO programs have detailed and refined policies and procedures for working with vendors in these scenarios which include site orientation, safety training, non-disclosure agreements (NDAs), and more. And that's just to get in the door! While onsite, some vendors may need to be fully escorted. In many cases, an alignment of plant equipment, electrical switching, LOTO, etc., should be performed by onsite technicians to prepare for outside vendors accessing these specific facility systems.</p>

<b>Access Control Measure</b>	<b>Function and Description</b>
Visitor policies and procedures	Visitors are also fairly commonplace in MCOs, and the facility should have detailed protocols for them as well. Most importantly, rules for how access is approved, security check-ins, badging, and escort requirements top the list. Depending upon the purpose for the visit, and to what parts of the facility the visitor will enter, some abbreviated site orientation or training may be required. You should also keep in mind that visitors may not be accustomed to working in critical industrial environments, so additional Personal Protective Equipment (PPE) should be made available for them to borrow as required.

## Materials and Inspections

While they are probably most top-of-mind when it comes to security, you need to be concerned about more than just the people visiting your MCO facility; the goods and materials coming in and out require an equal amount of scrutiny. Protocols should be in place for standard locations (typically at a loading dock or main entry area) and processes by which materials are received, including keeping detailed logs of the date and time, the carrier, the recipient, and any other pertinent tracking information. Certain high-security environments may also have additional screening requirements like x-ray. You must also keep track of what leaves the facility: sensitive information and potentially hazardous materials are part of daily MCO life, so the best practice is to just as tightly control any materials leaving the facility using the same protocols as you would use for those coming in.

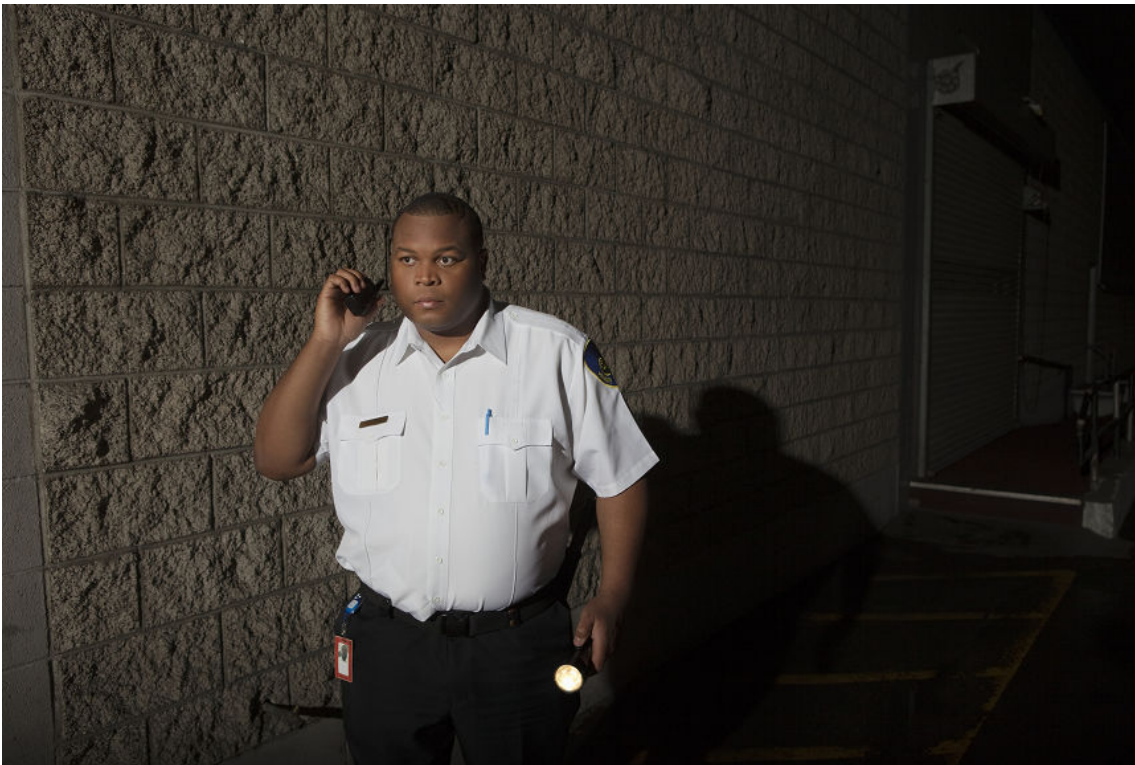


**Figure 8-14:** Authorized personnel checks a delivery at a loading dock before it is allowed into the facility. (Source: Cameron Whitman/iStock/Thinkstock)



## Security Patrols

MCO facilities are typically large in size (sometimes, huge), and there are only so many people on shift and only so much that can be monitored via video. It is therefore important to consider the frequency of additional security patrols around the grounds—particularly during off-hours shifts when there are less people onsite. Security patrols should focus on areas not well-covered by other security and monitoring systems, as well as remote areas where there may be the chance that people could have been working alone (which is never advised) and might be in distress. Patrollers should be alert for any abnormal sights, sounds, and smells from facility equipment that could point to a potential malfunction or damage to critical devices. Throughout these security patrols, patrollers should maintain constant communication with either the operations team or other security personnel to keep them apprised of the general security conditions at these far reaches of the MCO facility.



**Figure 8-15:** Security personnel patrols a facility during a late-night shift. (Source: moodboard/moodboard/Thinkstock)

## Manual Logs

Just as rounds and readings are part of regular equipment maintenance in an MCO facility, maintaining different types of manual security logs are common best practices. Electronic access logs from badge systems, video surveillance, and other forms of digital security are wonderful modern tools to have at our disposal, but computers are only as smart as the information we provide them. Simple handwritten logs of vendors/visitors, guest badge issuance, shipping/receiving, etc., provide an extra layer of security by allowing a person to make a judgement call as to whether or not it makes sense that John Smith is coming in alone at 2 A.M. or this large strange package arrived without any warning. Some may argue that paper logs are wasteful given our ability to digitize so much information, but the benefit of using manual logs as a standard practice lies in the potential for electronic systems to go down and all that data to be lost. Think about it this way: in a power outage, the backup power needs to go to the critical equipment, not necessarily to a backup log—and coming up with a process for capturing this information is the least of your

concerns if you're truly in an emergency situation. Better to have those paper logs available in a case like this!

## Fire Watches

A *fire watch* refers to the practice of assigning MCO personnel to a system, space, or specific facility for a prescribed period of time to physically observe for and report signs of fire. The fire watch should have a portable fire extinguisher with them, a means to communicate (radio, phone, etc.), and no other assigned tasks for the duration of the work and a cool-down period. Assigning a person to a fire watch is common under two conditions. The first condition is when there is hot work such as welding, cutting, or brazing taking place that creates obvious and immediate fire hazards. The second condition is when fire monitoring and/or suppression systems are down for maintenance and repair. In this case, the fire watch may be assigned to patrol the affected areas on a continuous loop, as opposed to being fixed in one spot.

## Confidentiality

As you probably know, *confidentiality* refers to the implicit or explicit promise that certain types of information will be protected from unauthorized access and will not be viewed or shared inappropriately. Almost all MCO installations deal with sensitive matters where confidentiality is key to operational success. This could be proprietary corporate data, hazardous materials, research and development (R&D) data, information regarding national or public security, and more. MCO security groups are often the front line of protection for digital, physical, and intellectual aspects concerning sensitive data. In many cases, an MCO organization will require that employees sign non-disclosure agreements (NDAs) so that even if some organizational damage has been done due to a security breach, the organization has legal means to go after reparations.

## Equipment, Information, and Mission Sensitivity

Mission Critical Operations are named as such for the purpose they serve: the equipment that is housed and the operations that take place at an MCO facility are crucial to the success of the organization. It would no doubt be a tragedy if an office building was burglarized or damaged in a disaster, but the organization could likely pick up the pieces and get things back in working order fairly easily. On the contrary, if a mission critical facility were affected by the same events, a great risk is posed to the organization or even the public at large, from which recovery could be a huge challenge, if not impossible. MCO personnel must take this mindset one step further and be aware of the incredibly sensitive equipment, information, and activities at their facility that make up the most vital building blocks for the organization.

## Common Types of Sensitive Equipment

Sensitive equipment can include the most critical pieces of the infrastructure and/or hazardous equipment—think nuclear reactor, high voltage switchgear, microwave transmitter, etc.—or special proprietary technology in use or in development. Sensitive equipment also includes items that are actually delicate, such as laboratory equipment or one-of-a-kind, specialty devices specific to the MCO activities.

## Common Types of Sensitive Information

Sensitive information encompasses the common categories familiar to the public—personally identifiable information, or PII (which includes names, addresses, birth date, credit card information, and identification numbers, among other things), protected health information or PHI (which includes healthcare records, health plan account information, and possibly even biometric identifiers, among other things), and financial data. It also includes certain types of information that

could pose a risk to organizational or public security or safety if disclosed to parties with malicious intent, such as research data related to a specific (possibly controversial) medical procedure or the steps for creating a hazardous compound that could be used inappropriately to cause damage or harm.

Information may also be considered sensitive simply due to the network on which it resides. Enhancements in cybersecurity over the last decade or two have made direct attacks highly visible and very difficult, so many of our concerns now revolve around indirect "backdoor" attacks. For instance, someone might decide to store the maintenance history for the facility's emergency generators on the same server as financial data or patent-pending production related designs (clearly a practice that would never truly happen because it is a terrible idea, but imagine it for the sake of illustration). In this scenario, you would need to treat access to maintenance information with the same heightened sensitivity as accessing the designs themselves.

## Visibility of Sensitive Equipment or Information

Sensitive equipment or information should be appropriately hidden, obscured, or otherwise stored to prevent unauthorized individuals from accessing it and/or viewing it. Otherwise, sensitive items should be clearly marked as such, with warnings that they should not be accessed unless authorized to do so, and preferably should be located within visibility of security personnel or systems.

Additionally, since cybersecurity threats come in many forms today, it is important for MCO teams to work closely with IT leadership when planning new projects, changing access levels, etc. As an MCO technician, you know that most of the infrastructure is critical, but based on your job responsibilities or areas of expertise, you might not always know which components and systems carry the highest digital risks. A particular stack of communications switches may have been labeled as "core network - special permissions required" when it had only limited access, but if facility construction or operations changes permitted more personnel access to that area, you would want the technology owners to weigh in on the cybersecurity ramifications of more traffic in the area. In this case, you might want to remove all signage so as not to draw unwanted attention or introduce the need for additional enclosure or cage locks.

## Classified Projects and Access Levels

Even within already sensitive and secure MCO facilities and operations, specific projects or systems may be further compartmentalized to tightly limit the number of individuals with access. While operators and technicians may be charged with maintaining the entire physical infrastructure of a facility, it is a faulty assumption to think you can access everything. The old adage of "need to know" rings true across all mission critical industries. If you're ever in doubt whether it's appropriate that you see something you have access to, given the currently implemented security protocols, ask yourself whether you need to know that information to carry out your normal job. Any hesitation in answering "yes" is a warning sign to stop. The same holds true for site personnel that see someone or something out of place: if there is not proper access authority and a need to know, it's your duty to stop and question it.

# ACTIVITY 8–3

## Establishing Security Procedures

### Scenario

In this activity, you will identify the various protocols and procedures that should be followed to establish a secure facility.

1. Which type of security protocol should be in place to verify the identity of any person coming onsite, from every-day personnel, to visitors, to authorized vendors?
  - Authorization procedures
  - Background checks
  - Entry credentials
  - Site access control
  
2. Sensitive items that you might find in your MCO facility range from equipment that is incredibly intricate or even dangerous, to personal or organizational information that could be used with malicious intent.
  - True
  - False
  
3. Which type of security protocol should be in place to assess the security of any items that are received into or even delivered from the facility that could pose a potential threat?
  - Materials and inspections
  - Security patrols
  - Manual logs
  - Secure storage of sensitive items
  
4. Which type of security protocol should be in place to assess any person or item coming into a facility to verify that they are not a security threat to the people or property within the facility?
  - Authorization procedures
  - Background checks
  - Entry credentials
  - Site access control
  
5. Which type of security protocol should be in place to capture and track important facility information, such as delivery receipts, in a non-electronic form, in case digital data is lost or otherwise unavailable?
  - Materials and inspections
  - Security patrols
  - Manual logs
  - Secure storage of sensitive items

6. Which type of security protocol should be in place to remain aware of who or what has entered the facility and limit or otherwise control which areas of the facility they can enter or move about in?
- Authorization procedures
  - Background checks
  - Entry credentials
  - Site access control
7. Which type of security protocol should be in place to assess the security of remote areas of the facility or any areas where other security system implementations are limited, especially during off-hours?
- Materials and inspections
  - Security patrols
  - Manual logs
  - Secure storage of sensitive items
8. A fire watch would only be assigned during a period of time when fire monitoring or suppression systems are unavailable, such as during maintenance or repair.
- True
  - False
9. Which type of security protocol should be in place to vet the people that are selected as permanent or semi-permanent MCO personnel before (or sometime during) their employment?
- Authorization procedures
  - Background checks
  - Entry credentials
  - Site access control
10. Which type of security protocol should be in place to protect the confidentiality of public data that is being housed within an MCO facility?
- Materials and inspections
  - Security patrols
  - Manual logs
  - Secure storage of sensitive items
-

## Summary

In this lesson, you identified and applied best practices, strategies, and techniques for establishing and maintaining security for a mission critical facility. As an MCO operator, you need to know the kinds of security breaches that could pose a threat to the people, equipment, property, and continued operations within your facility and you need to know the proper protocols to follow to help keep all of those elements secure. By following best practices and industry-standard strategies and techniques, you can help ensure that your MCO facility is as secure from potential threats as possible by deterring or preventing unauthorized access to the site, controlling who and what gets into and where they can go within your facility, and following other security procedures to maintain a safe, secure facility location.

# 9

# Critical Production Spaces

## Lesson Objectives

In this lesson, you will identify and apply industry best practices, strategies, and techniques for the proper design and configuration of critical production spaces. You will:

- Identify and apply best practices for configuring and operating a data center.
- Identify techniques and strategies for proper air flow management in a data center facility.
- Identify and apply best practices for cable management in a data center space.
- Identify other common mission critical production environments and their associated equipment.

## Lesson Introduction

In addition to the critical products or services that Mission Critical Operations (MCOs) provide, there are a number of other services that are imperative for the optimal operation of the organization itself or that its consumers rely upon, ranging from the organization's data center to its communications services. These critical production spaces can be just as important as the critical operations, and should be addressed with the same sensitivity and urgency as the critical operations themselves.

As an MCO technician, you need to have a strong understanding of the various critical production spaces, from the data center to the manufacturing warehouse, that keep the critical operations of your MCOs running smoothly. In this lesson, you will identify and apply industry best practices, strategies, and techniques for the proper design and configuration of critical production spaces.

# TOPIC A

## Data Center Best Practices

Depending on the size, scope, and services it provides, a data center can be an important ancillary space within an MCO organization, such as the data center that houses patient data for a hospital; or it can be the MCOs themselves, such as the giant facilities that handle the data for large technology corporations like Google™ or national telecommunications companies like Verizon. Regardless of its size or purpose, though, the continuous, reliable operations of the data center and the accessibility and security of the information it stores is a top priority for any organization. This means following all of the industry standards and best practices available to help ensure that your data center is functioning at its most efficient. As an MCO operator, you need to have a working understanding of these best practices to help design, construct, and maintain the data center as a critical space for your facility. In this topic, you will identify and apply best practices for configuring and operating a data center.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Power load balancing
- Phase balancing
- Distribution redundancy
- Load shedding
- Power Usage Effectiveness (PUE)
- Data Center Infrastructure Efficiency (DCiE)
- Raised access flooring
- Vented access flooring
- Loading
- Bridging

## Site Selection

As discussed previously, site selection is a key (if not primary) factor in establishing the mission critical footprint of an organization. This is particularly true of data centers that derive benefits from the convenient intersections of people, resources, and technology.

Aside from macro-geographic considerations discussed previously (such as the location's susceptibility to natural disasters, proximity to transportation, availability of government subsidies, etc.), the actual location of the property itself is important for a given facility. Many data centers have strategic importance for the organization beyond other mission critical facilities and/or are involved in confidential operations—in either case, staying out of the immediate public eye is often a desirable trait. Data center properties may be located deep within an industrial park or in remote rural areas, which is actually fairly easy to accomplish since most high-power utility transmission lines and high-bandwidth communication paths don't run through the middle of highly populated residential or commercial areas.

If a data center is not the sole occupant of a mission critical facility, special consideration should also be given to what area of the facility it occupies. From a security standpoint, mission critical infrastructure should be located away from main entrances, parking garages, etc. Another consideration, especially in multi-story structures, are the functions of the adjacent spaces to the data center. Particularly in older buildings that have been retrofitted to include data centers, you may run into situations where the data center or its support spaces are located underneath other tenants. Gaining access to overhead space for the data center can be difficult, but the biggest concern is water systems residing above the critical gear. It won't take long in the industry until you run across



stories about—or worse, experience firsthand!—an upper-floor restroom or water closet flooding and causing damage to the critical equipment housed below.

## Component Redundancy

Perhaps more than any other MCO installations, data centers need as much redundancy as the design and budget will allow for. This extent of component redundancy is really necessary, given that component failures within the data center infrastructure or the cascading faults that may accompany them can impact the organization pretty much immediately.

Take, for example, component redundancy for backup cooling systems: in general, these systems don't always get the forethought they deserve—or that the facility needs. While power backup and redundancy are becoming more commonplace with the prevalence of uninterruptible power supply (UPS) designs, it can be difficult to build in backup sources for cooling systems due to the size and volume of their components. But what good does 10 minutes of backup battery power do if the data center floor will overheat in 8 minutes given a loss of cooling? When possible, then, at least minimum portions of the mechanical plant should be supported by UPS protected power. Roll-up or spot coolers (basically, portable air conditioners) can also be hooked up to emergency power, and industrial size fans are great to keep on hand if you need to prop doors open to circulate what air you can.

## Supply Voltage

The supply voltage to the data center tends to be driven by the technology installed, but is affected by any number of design considerations such as utility sources, the types and/or amount of equipment redundancy desired, or even owner preference. Direct Current (DC) supply is less efficient at the low voltages used by equipment, so it is not as common as Alternating Current (AC). Typical floor-level AC supply voltages are 208V, 240V, 415V, and 480V.

## Power Cabling

Power cabling for data center equipment is not only the lifeline for the gear, but an enormous expense due to the cost of copper as the primary conductor component. With costs of cabling alone regularly running from hundreds of thousands to millions of dollars, you'll want to have just enough power circuitry to meet your data center's design requirements without being wasteful. This is particularly true for the fully redundant designs previously discussed, such as dual-feed power supplies. Consider this: if there are two power runs to each piece of technology and a thousand of these assets in the facility, an extra six inches of unnecessary cabling adds up quickly.

In addition to having a dedicated power system as part of the critical infrastructure, data center designs often include further breakdowns of dedicated circuitry to isolate sections of technology from one another. This allows for flexibility in repair and maintenance so the entire production space doesn't need to be de-energized and isolates highly sensitive equipment from other sections on the floor to prevent potential faults from spreading.

## Grounding for the Data Center

As with MCO facilities as a whole, grounding within a data center is particularly important due to the sheer volume of electronic components that are increasingly more sensitive to faults. While there are no standard best practices for providing grounding within the data center (aside from making sure something is in place), there are a few common techniques that could be applied.

<b>Grounding Technique</b>	<b>Description</b>
Signal reference ground grid systems	Typically utilizes large plates and/or structural steel as much as possible with limited length conductors to maximize absorption. This technique is used in high-frequency electrical source systems where the grounding system needs to be able to accept large surges of varying potential and frequency.
Rack grounding	Connects a ground conductor to the frame of each rack, which ties back into some common ground grid.
Cable tray grounding and bonding	While the cables in a data center are typically insulated, the moving current through them creates fluctuating magnetic fields. Therefore, cable trays containing multiple runs of power need to be grounded; to do so, this approach directly bonds them to the structural components to which they are attached.
Master ground bus bars	Utilizes bus bars, which are metallic strips or bars that are directly grounded to the earth or structural steel, as a collective attachment point for bonding ground cables coming from racks, trays, etc.

## Power Load Balancing

*Power load balancing* refers to distributing power throughout the data center in such a manner that it provides equal load to and wear on the associated infrastructure. Additionally, the heat density differences created by imbalanced loading throughout the data center floor will create significant inefficiencies in cooling demands. If hot spots cannot be avoided due to specific technology requirements, using additional spot cooling should be considered to prevent having to excessively cool the rest of the space just to keep one area within acceptable temperature specifications.

## Phase Balancing

*Phase balancing* refers to the more detailed practice of balancing the power draw from different phases of power delivered to individual cabinets. Typically, three-phase power is split at the cabinet level to provide a single phase to each rack or a set of racks; unfortunately, three-phase breakers can develop hotspots if the power draw is not somewhat balanced across the terminals of each phase.

## Distribution Redundancy

Just as redundancy in the design of the electrical infrastructure at a system level is imperative, strong data center designs incorporate distribution redundancy as well. *Distribution redundancy* refers to the practice of overlapping, interlacing, or otherwise mixing up distinct power supply paths to critical equipment throughout the data center in order to vary the diversity of power supply sources to the greatest extent possible.

If there are more than two (UPS-backed) critical power paths, overlapping or interlacing them throughout the floor is a best practice because it can provide an extra layer of redundancy, especially for devices installed in adjacent cabinets with different sets of power supplies. Then, any critical power path faults would be less likely to interfere with continuity of operations.

## Load Shedding

*Load shedding* is the practice of simultaneously or sequentially de-energizing certain non-critical loads during utility events in order to conserve emergency power sources. When a utility loss occurs, general facility loads—from non-essential spaces, like administration locations—may be immediately shed. If the generators fail to start and your facility is relying on UPS battery power only, portions of

the critical cooling system may be shed in order to maintain only the data center power and nominal air circulation.

## PUE

*Power Usage Effectiveness (PUE)* is a common industry term used to measure and track the efficiency of how a data center utilizes power to operate installed technology. Very simply put, it is the ratio of the power consumed by the total critical infrastructure to the power consumed by the critical load of the data center, represented by the following equation:

$$PUE = \frac{\text{Total Critical Infrastructure Load}}{\text{IT Critical Load}}$$

(Source: Logical Operations for NCMCO)

The higher the PUE calculation, the less efficient the power utilization; the lower the PUE calculation, the more efficient the power utilization. For example, consider a facility that uses 200,000 kw of total power, 120,000 kw of which is used by the data center. Using the equation for PUE, (in short, 200,000 divided by 120,000) gives you a PUE of approximately 1.7 which falls somewhere between average and efficient power utilization.



**Note:** As PUE gets closer to 1, it means that more of the power is being consumed by the technology equipment. Achieving a PUE of 1 would mean that all power is being consumed by the technology equipment, which is actually impossible to attain due to inherent power transmission losses and support system consumption (such as cooling, controls and monitoring, etc.).

In general, there is a lack of consensus within the industry on exactly how to calculate PUE, primarily due to disagreements on what systems support the critical load vs. general building load, especially when these may be combined services. The best practice is to track PUE locally and measure your own usage against past performance.

## DCiE

*Data Center Infrastructure Efficiency (DCiE)* is another metric used to measure the effectiveness of the power usage for a facility, but it measures the inverse of PUE. Also simply put, it is the ratio of the power consumed by the critical load of the data center to the power consumed by the total critical infrastructure, represented by the following equation:

$$DCiE = \frac{\text{IT Critical Load}}{\text{Total Critical Infrastructure Load}}$$

(Source: Logical Operations for NCMCO)

The lower the DCiE calculation, the less efficient the power utilization; the higher the DCiE calculation, the more efficient the power utilization. Take the same facility that uses 200,000 kw of total power, 120,000 kw of which is used by the data center. Using the equation for DCiE, (in short, 120,000 divided by 200,000) gives you a DCiE of approximately 60%, which again falls somewhere between average and efficient power utilization.

In short, PUE and DCiE give you pretty much the same measurement of energy usage effectiveness, just derived in a different manner with a different measured result. Some MCO organizations will remain fixated on one particular aspect of their data center operations, like PUE, but this is where operators and technicians can prove tremendous value: experiment with different measurements,

find ones that track your biggest goals, then trend them as you fine tune your infrastructure systems. The important takeaway is that these metrics exist, and you should use them to measure your facility's effectiveness—at least once, if not more often.



**Note:** While PUE/DCiE are used almost exclusively within the data center industry, any MCO organization can think about the same approach by identifying what the critical loads are that directly provide the MCOs' purpose, and which loads are simply required to support it.

## Rack Placement, Layout, and Installation

The placement of IT equipment racks throughout the data center space is key for both installation and operational efficiency. Pre-planned floor layouts significantly decrease capital costs by allowing data center management to minimize the length of power and communication cabling, as well as establish systems for installing new equipment in a neat and orderly fashion. Additionally, MCO technicians should weigh in on the planning process to make sure that cooling systems are being utilized in the best way possible. For instance, simply installing racks and cabinets because there is enough room in a given footprint can create serious problems, such as the intake of one set of servers being adjacent to the hot air exhaust of another set of equipment.



**Figure 9–1:** Server racks, which can be numerous, need to be well-placed in the data center. (Source: Derrick Coetzee/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Rows\\_of\\_Franklin\\_Cray\\_XT4\\_racks.jpg](https://commons.wikimedia.org/wiki/File:Rows_of_Franklin_Cray_XT4_racks.jpg))

## Rack Power Distribution

The distribution of power to and between racks on the data center floor is almost as much of an art as it is a science. Design requirements will dictate how much power needs to be delivered, to what systems, and the levels of redundancy and reliability that are necessary for business continuity.

There are a few considerations regarding rack power distribution that you should keep in mind:

- Dedicated circuits should be implemented for sections of the floor, for individual cabinets, or both.

- Circuit size will be generally dictated by design, but a good rule of thumb is the maximum expected load should be less than 80% of the circuit size. For instance, a 20A circuit should not have more than 16A of load installed.
- Rack flexibility, which is the ability to install different-sized gear with varied power and networking requirements, is important for enterprise data centers that have all sorts of IT setups installed.
- Growth potential is very hard to determine in the rapid evolving IT/data industry, but all efforts should be made to provide design allowances for growth in scale, connectivity, and power density. It is extremely expensive and invasive to attempt to retrofit a live data center with new infrastructure requirements.

## High-Density Server Cabinets

High-density server cabinets are those generally designed to operate above 15 kilowatts per cabinet. While the computing power is certainly greater, this does mean more infrastructure costs associated with each deployment. With the increase in power and density of these types of computing devices, more heat is generated, requiring more cooling functions.

## Floor Systems

Floor systems refer to the different flooring components and designs within a data center space. This is often further characterized and referred to as “whitespace,” since most flooring systems are white or light-colored. There are two common types of floor systems: raised access flooring and vented access flooring. With *raised access flooring*, the floors are elevated typically from 18 to 48 inches above the slab, which allows for under-floor cooling and/or space to run power conduits or other piping. With *vented access flooring* (which is a modification of a raised floor system), the entire underfloor is not treated as a cooling supply plenum; instead, ducting is run under the floors and vented into the space at specific locations within the infrastructure design, much like in residential construction. Regardless of the type of floor system installed, ramps into and out of data center spaces with elevated areas are necessary, since most technology infrastructure needs to be rolled around on pallets.



**Figure 9–2: A floor tile is lifted out of the raised access flooring system to access the components below. (Source: Jonathan Lamb/Creative Commons (Public Domain)/<https://commons.wikimedia.org/wiki/File:Tile-lifter-in-use-raised-floor.jpg>)**

When it comes to floor systems, there are a few key design considerations that you should also keep in mind. *Loading* refers to the weight limits of the flooring system. Raised floors have limits depending upon the stanchion design and floor tile construction, but even concrete slabs have limits to the weight of equipment that can safely rest on them. *Bridging* is the practice of installing angled covers over cabling or other components running across floors to allow for equipment, carts, etc., to be easily and safely rolled over them and to eliminate trip hazards.

## Rack Cooling

No two data centers are alike, and not all of them are pre-planned and well laid out—some just grow organically, out of need or use. Some designs and implementations may require the use of rack-level cooling to counteract the heat generated by the specific equipment utilized. There are three commonly used applications for rack cooling:

- Above floor: cool air is ducted specifically from overhead towards a single rack or section of cabinets.
- Below floor: cool air is ducted up from below, into a cabinet or towards standalone perforated tiles.
- Spot coolers: small lines of refrigerant or chilled water are piped directly to heat exchangers with fans installed at the top, bottom, or sides of individual racks.



**Figure 9–3:** The fans on a server rack are used to moderate the temperatures of the servers on the rack. (Source: Annagen, LLC dba Netrepid/Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:Colocation\\_Cooling\\_Rack.png](https://commons.wikimedia.org/wiki/File:Colocation_Cooling_Rack.png))

## Fluid-Cooled Processors

Though not widely adopted anywhere in the industry at this time, it is worth noting that there have been many successful implementations of liquid submersion or fluid-cooled techniques to provide cooling for data center components. In this design, the server's components, including the processors and motherboards, are directly submerged in a non-conductive fluid like mineral oil to provide the means of heat transfer. The heat can then be removed from the liquid via cooling coils, circulating air, etc.

## Cleanliness

Cleanliness is important in all MCO environments, but especially so in data centers. The design of most technology in the center is to pull air through the device to cool its internal components. The airstream and any potential pollutants contained within it, therefore, comes into direct contact with highly sensitive electronic components. There are a variety of substances, then, that should be addressed or avoided to maintain cleanliness within the data center.

Dust is ubiquitous and very difficult to completely eliminate, but isn't itself generally harmful to technology devices. Buildup of dust layers can impede heat transfer from the components being cooled and potentially cause damage; therefore, you need to make sure that all sources of air flow are cleaned often to remove any dust that could become an impedance. Dust that contains metallic/conductive particles, however, can be very dangerous, causing shorts or other faults at the micro-level; this requires a greater level of component cleanliness.

The fibrous construction of cardboard makes it highly susceptible to brushing or flaking off. These little fibers can build up in the airstream quickly, particularly since the data center floor is downstream of the filtration media in air handling equipment. Therefore, cardboard should be prohibited from being placed anywhere on (or near) the data center floor whenever possible.

Pallets are a similar concern to cardboard since wood is also a fibrous material. Moreover, placing large amounts of combustible fuel near critical and expensive technology is generally a bad idea.



**Figure 9-4:** Dust has built up inside of a computer that has gone far too long without cleaning, and has led to some component failures. (Source: Arvutistuudio/Creative Commons (CC BY-SA 4.0)/[https://commons.wikimedia.org/wiki/File:Dusty-dirty\\_PC.jpg](https://commons.wikimedia.org/wiki/File:Dusty-dirty_PC.jpg))



# ACTIVITY 9-1

## Identifying Data Center General Best Practices

### Scenario

In this activity, you will identify data center best practices.

- 1. Which measurement calculates the efficiency of the power usage of a data center using the ratio of the power consumed by the total critical infrastructure to the power consumed by the critical load of the data center?**
  - Data Center Infrastructure Efficiency
  - Energy Reuse Effectiveness
  - Power Usage Effectiveness
  - Energy Consumption Intensity
- 2. Which measurement calculates the efficiency of the power usage of a data center using the ratio of the power consumed by the critical load of the data center to the power consumed by the total critical infrastructure?**
  - Data Center Infrastructure Efficiency
  - Energy Reuse Effectiveness
  - Power Usage Effectiveness
  - Energy Consumption Intensity
- 3. Which power distribution and usage best practice should be followed to distribute power to and between the main components of the data center in a manner that provides redundancy and reliability?**
  - Power load balancing
  - Load shedding
  - Rack power distribution
  - Phase balancing
- 4. Which power distribution and usage best practice should be followed to distribute power throughout the data center in a manner that equally shares the load to and the wear and tear on the infrastructure?**
  - Power load balancing
  - Load shedding
  - Rack power distribution
  - Phase balancing
- 5. Which power distribution and usage best practice should be followed to appropriately balance the power drawn from the different types of power supplies that deliver power to the individual cabinets in the data center?**
  - Power load balancing
  - Load shedding
  - Rack power distribution
  - Phase balancing

6. Which power distribution and usage best practice should be followed to conserve emergency power sources during utility events by simultaneously or sequentially de-energizing certain non-critical power loads?
- Power load balancing
  - Load shedding
  - Rack power distribution
  - Phase balancing
7. With vented access flooring, the entire space under the raised floor is used as a cooling mechanism by providing air flow and a power distribution mechanism by providing a location for conduits or piping to run.
- True
  - False
8. What are the common mechanisms that are utilized in a data center to provide cooling for the racks and the equipment housed within them?
- Spot cooling
  - Hot aisle/cold aisle
  - Above floor cooling
  - Below floor cooling
  - Liquid submersion
9. Which grounding technique directly bonds the containers that are used to house and run cables throughout the data center to the structural components that they are attached to?
- Signal reference ground grid
  - Master ground bus bars
  - Cable tray grounding and bonding
  - Rack grounding
10. Which grounding technique attaches the grounding cables coming from the racks or trays to a piece of metal that is directly grounded to the earth or a steel structural component?
- Cable tray grounding and bonding
  - Master ground bus bars
  - Signal reference ground grid
  - Rack grounding
-

# TOPIC B

## Data Center Air Flow Management Techniques and Strategies

Any data center, regardless of size or scope, will consist of numerous electronic equipment that generates a lot of heat and spent exhaust air; unfortunately, these components also rely on a source of clean, cool air in order to operate properly. Therefore, it is imperative that there are mechanisms in place to create and maintain ample air flow in the data center to keep all of your components functioning under optimal conditions. As an MCO technician, you will need to know what the techniques and strategies are for managing the air flow in the data center, and which are the best suited for your design and installation. In this topic, you will identify techniques and strategies for proper air flow management in a data center facility.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Computer Room Air Conditioner (CRAC)
- Computer Room Air Handler (CRAH)
- In-row cooling
- Spot cooling
- Hot aisle/cold aisle (HACA)
- Supply air plenum
- Return air plenum
- Room envelope
- Perforated tile

### Computer Room Air Conditioners vs. Air Handlers

While you have already learned quite a bit about facility air circulation—specifically, the air handlers used for HVAC purposes—there is an important distinction to make in regard to the equipment used for air management in the data center. A *Computer Room Air Conditioner (CRAC)* is a piece of equipment that directly performs the heat transfer functions to cool the supply air. CRACs either have internal compressors or a supply of refrigerant to cool the supply air and then circulate it back throughout the floor. A *Computer Room Air Handler (CRAH)* or simply an air handler/air handling unit (AHU) moves the air across a cooling agent or mechanism (usually, chilled water cooling coils) but does not cool the air via a cooling process itself.

While both types of equipment supply cool air to the data center, some personnel often incorrectly interchange these two terms. Astute MCO operators and technicians understand the difference and how it relates to the execution of the infrastructure design.

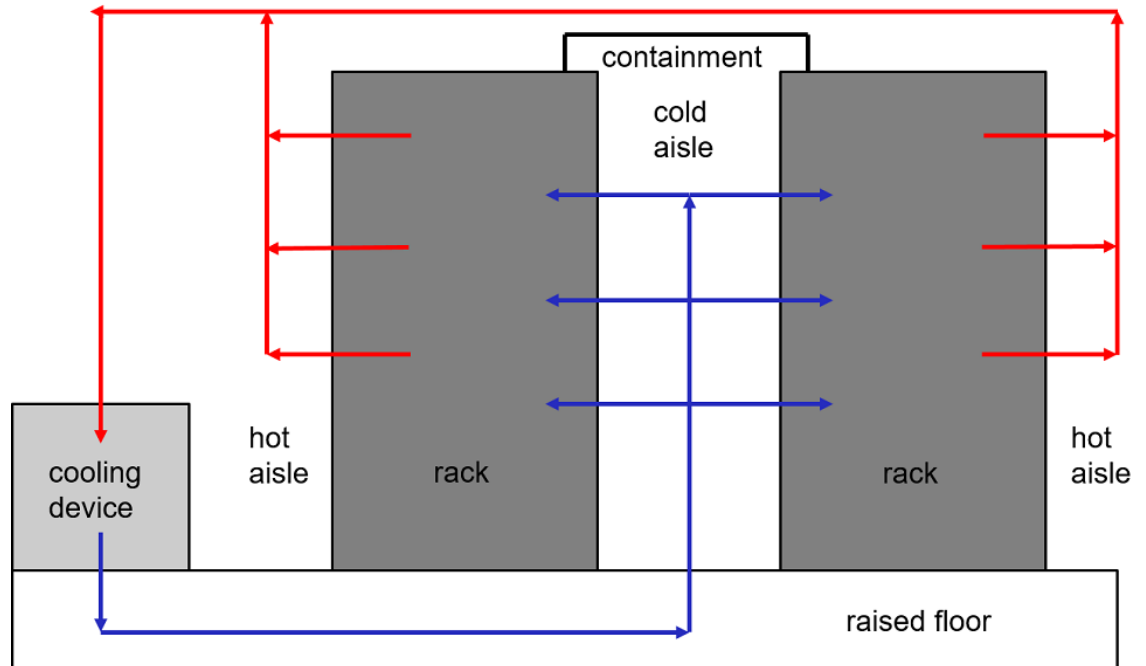
### In-Row Cooling and Spot Cooling

Another set of terms that can be used interchangeably but that have subtle differences are in-row cooling and spot cooling. With *in-row cooling*, a cooling unit is inserted within a cabinet, between cabinets, or mounted to the top or bottom of a cabinet in order to deliver cool air directly to a specific location within a data center row.

With *spot cooling*, small cooling units (usually fan coil units) are installed anywhere in the data center where additional cooling is needed. This could be adjacent to a row, in the corner of a room near power distribution equipment, and so forth. Spot coolers tend to be more feasible solutions when hot spots start developing or when there is difficulty maintaining temperature stability in the space.

## Hot Aisle/Cold Aisle

*Hot Aisle/Cold Aisle (HACA)* is a technique used for air flow in a data center that physically separates the supply air (cold aisle) from the exhaust or return air (hot aisle) for the equipment in the data center, via various containment strategies such as panels or curtains. By segregating these two airstreams to the greatest extent possible, it increases efficiency by preventing cold air from bypassing the IT equipment and travelling straight into the exhaust path and/or preventing hot air from being pulled back in through the equipment. HACA terminology is applicable regardless of which side is more directly contained.



**Figure 9-5:** A diagram of the flow of warm and cool air when a hot aisle/cold aisle design is implemented. (Source: Logical Operations for NCMCO)

## Space Integrity

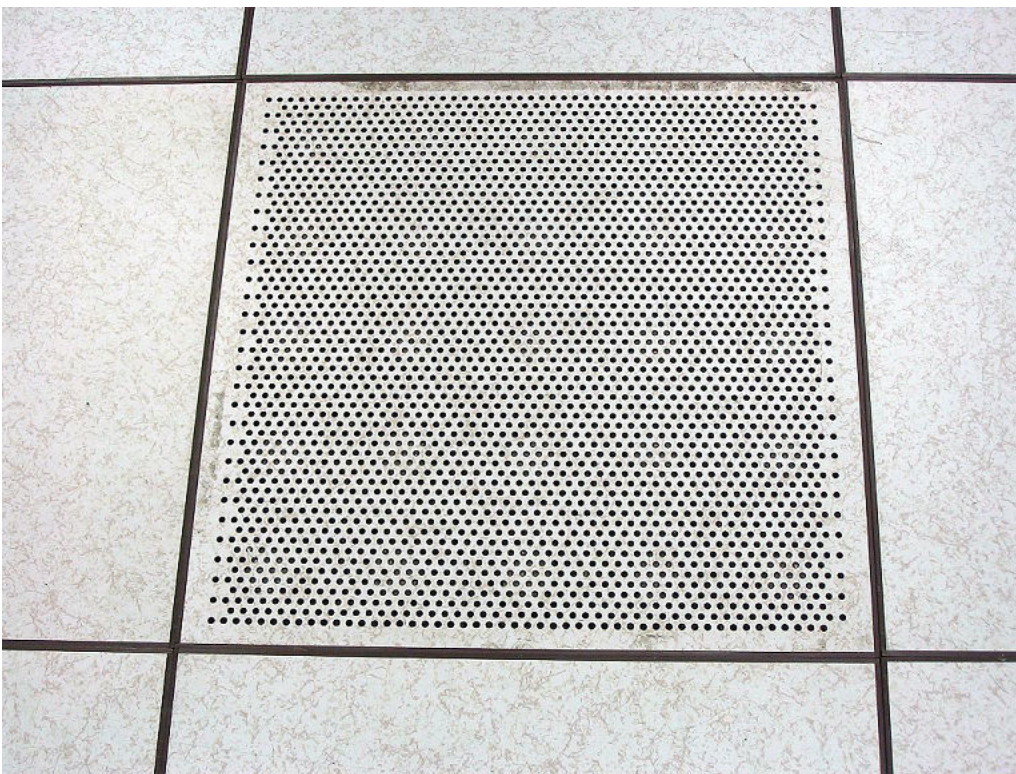
Space integrity is the often elusive target MCO technicians are chasing in data center efficiency. Regardless of the design elements that have been added, if all the components can't complete their individual functions without interference from other parts of the airflow management, you are really just wasting your time and energy in designing for efficiency. Therefore, there are a few common components and associated methodology for maintaining space integrity that results in better air flow within the data center.

Component or Method	Description
Supply air plenums	A <i>supply air plenum</i> refers to the ducting and/or contained space (usually under the raised floor) through which cool air is supplied from the AHUs. Plenums refer more to the common air paths (or headers) than just the individual ducting runs if all of the supply air is not just being pushed into the underfloor, for instance. Air leaks here are especially wasteful, since the energy exerted to cool the air doesn't even have a chance to remove any heat from the IT equipment on the floor.

Component or Method	Description
Return air plenums	A <i>return air plenum</i> refers to the ducting and/or contained space (usually overhead, above the ceiling grid) through which hot air rejected from the IT equipment is collected and exhausted and/or circulated back to AHUs for cooling.
Room envelopes	The term <i>room envelope</i> refers to the overall isolation of the spaces containing the main data center equipment. There are many temperature, pressure, and cleanliness concerns associated with certain designs, but the whole point is to keep the space as contained as possible to allow all of the design elements to function as intended. However, there are many weak spots that can compromise the integrity of this sealed-off space, such as wall penetrations for conduit, cabling, or ducting and access doors that don't have proper weather-stripping, brush guards, etc.

## Perforated Tiles and Tile Placement

*Perforated tiles* are floor tiles with holes in them used to supply cool air from below. Just as with most aspects of data center design, the styles and applications of perf-tiles are countless, but they all perform this same basic function.



**Figure 9–6:** A perforated tile in raised access floor. (Source: Jonathan Lamb/Creative Commons (Public Domain)/<https://commons.wikimedia.org/wiki/File:Perforated-ventilation-tile.jpg>)

MCO facility operators should consider the following if under-floor cooling via perforated tiles is being used.

<i>Consideration</i>	<i>Description</i>
Safety	Although most products are designed to meet similar load-bearing characteristics as the solid tiles in the rest of the space, this should be researched and understood—not assumed. Perf-tiles can also present a trip hazard if proper footwear is not enforced in the data center; most commonly, female guests touring the data center should be advised against wearing high-heels.
Floor integrity	Along the lines of load-bearing characteristics that should be fully understood, integrity of the floor as an air plenum can be compromised if the placement of perf-tiles is excessive or insufficient, causing air pressure control issues.
Regulations	Some design specifications (which may include the organization's insurer) may require that a specific product or category of product be used based upon strength, material composition, or other specification.

## Return Air Methodologies

What to do with the return air? This is a question guaranteed to spur hours of debate among seasoned MCO professionals. By the laws of physics, hot air has more energy than cold air, so it seems pretty wasteful to spend more energy to remove this existing energy via a cooling process. Because you're controlling other space conditions, though, there is more consistency in the atmospheric conditions of the air that would be reconditioned—so there are some efficiencies gained from reusing return air vs. using the outside air in whatever condition it may be.

In many cases, enough heat is generated and available in the exhaust stream of the data center floor that it can be reused, via heat recovery units, to heat hallways and admin spaces during cool months to save energy on standalone means of heat (electric, gas, steam). When reusing return air, however, you may need to consider the addition of fresh air makeup for two main reasons. First, continued cycling of the same air volume tends to dry it out via the repeated heating of the air stream, so using some fresh air makeup to modulate humidity levels can be more efficient than supplemental humidification systems. Secondly, people do need to work in the data center, and there is the potential for the  $O_2$  and  $CO_2$  levels to rise to unsafe levels if you keep using the same air volume over and over again.

## Temperature Control Strategies

There are numerous strategies for controlling temperature in the data center, far too many to detail them all. In general, your primary goal as an MCO operator is to fully understand the design specifications and intent of your facility and then find the strategy that is applicable to your specific design. (Unfortunately, you may need to sort through the various industry publications applicable to help guide your strategic approach).

There are a few common considerations for temperature control, however, such as:

- Supply air temperature measurement: are you controlling based upon the output of the air-handling equipment, or what is measured in the cold aisles/equipment intakes?
- Fixed or swing setpoints: do you control to a single temperature (wherever it is measured) or allow a few degrees of swing to prevent the system from constantly modulating and adjusting to meet an exact point?

## Pressure Control Strategies

Just like with temperature control, there are numerous pressure control strategies in the data center industry that may or may not apply to your specific facility. In general, though, pressure control is

most important for under-floor plenum designs where the pressures above and below the floor (or as measured by the changes in pressures across the floor) are controlled to ensure the proper air flow to the IT equipment. Similarly, you might want to maintain a relatively fixed negative pressure in the exhaust/return plenum to more naturally draw the hot air out of the space as opposed to mechanically forcing it out with fans.

## Humidity Control Strategies

Humidity control is an important consideration within a data center to help protect the equipment from harmful effects: too humid of an environment can cause condensation damage, while too dry an environment increases the risk of electrostatic charge buildup. Much like temperature and pressure, where you are measuring humidity for control purposes will dictate the strategy and components used to modify humidity conditions. In general, though, the closer you measure humidity to the technology being served, the better, since this is much more about equipment safety than comfort.



**Note:** To further explore how to control the operating conditions within your space, you can view the **Use an Operating Envelope to Simplify Control Programs** presentation from the Certified Mission Critical Operator Video Series.

## ACTIVITY 9–2

# Identifying Air Flow Management Techniques and Strategies

### Scenario

In this activity, you will identify data center air flow management techniques and strategies.

1. **A Computer Room Air Handler (CRAH) uses an internal compressor or a refrigerant to cool the supply air and then circulates the cooled air throughout the data center floor.**
  - True
  - False
2. **Which air flow technique utilizes ducting or contained space above the ceiling grid to collect hot air exhausted from the data center equipment and deliver it back to the air handler to be cooled?**
  - Supply air plenum
  - Room envelope
  - Hot aisle/cold aisle
  - Return air plenum
3. **Which air flow technique attempts to isolate the entire data center space in order to maintain air temperature, pressure, and cleanliness at optimal levels and prevent potential fluctuations to them from outside spaces?**
  - Supply air plenum
  - Room envelope
  - Hot aisle/cold aisle
  - Return air plenum
4. **Which air flow technique physically separates the supply air from the exhaust or return air within the data center in order to optimize the airflow in and around the equipment?**
  - Supply air plenum
  - Room envelope
  - Hot aisle/cold aisle
  - Return air plenum
5. **Which air flow technique utilizes ducting or contained space below the floor to move cooled air from the air handler around the data center floor?**
  - Supply air plenum
  - Room envelope
  - Hot aisle/cold aisle
  - Return air plenum



6. An in-row cooling mechanism delivers cool air directly to a specific location within a data center row via cooling units placed directly in, between, or on the equipment where cooling is needed.

True

False

---

# TOPIC C

## Cabling and Cable Management

Think about the number of cables and connectors you have running to your own computer at home or in your office. Now, multiply that by hundreds or thousands, and you still might not have as many cables as are needed in a typical data center installation. Cabling of this magnitude also needs some management techniques to help prevent it from become a tangled mess of cables, with no idea of where they start, end, or what they connect to and what purpose they serve. As an MCO operator, you need to know the various types of cables that you might encounter in a data center space and how to best configure the cables in the space to ensure that the equipment is continuously functional. In this topic, you will identify and apply best practices for cable management in a data center space.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Twisted pair cable
- Coaxial cable
- Fiber optic cable
- Bend radius
- Cable dressing
- Cable tracing/testing

### Cable Types

There are numerous types of cables that you are likely to encounter within critical production spaces, particularly data centers. Even non-IT focused MCO production spaces today have lots of communication cabling as we connect more devices and equipment to local networks or the Internet itself, so being able to identify these various cable types is beneficial to any MCO technician.

Cable Type	Description
Twisted Pair	<p>Most commonly referred to as an Ethernet cable, <i>twisted pair cables</i> consist of four twisted pairs of insulated wires encased in a single sheath and terminated to an Ethernet adapter. The pairs of wires are twisted for the prevention of attenuation (gradual loss of strength) of a data signal. This allows for transfer of data over longer distances. However, the most common types of twisted pair cables you are likely to encounter are limited to 100 meters in length before interference becomes an issue.</p>



(Source: Baran Ivo/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:FTP\\_cable.jpg](https://commons.wikimedia.org/wiki/File:FTP_cable.jpg))

These cables are commonly rated using a category system which indicates the data transmission speed limit of a particular cable. The most common categories you are likely to encounter in a data center include:

- CAT5: An older, but still often-utilized cable type limited to 100 Mbps at 100 MHz data transfer (or throughput) speed.
- CAT5e: The “e” denotes an “enhanced” performance, and as such, this cable has a useable data transfer speed of 1,000 Mbps (or 1 Gbps) at 100 MHz.
- CAT6: A relatively new cable design which greatly improves the speed of Ethernet data transmission. While still utilizing the twisted pair design, it also includes an internal separator of the wire pairs which allows for less attenuation and a higher specific data transfer speed of 10,000 Mbps (or 10 Gbps) at 250 MHz.

#### Coaxial

*Coaxial cables* consist of a single inner conductor surrounded by a tubular insulated layer, then surrounded by a tubular conductive layer and, lastly, surrounded by an insulated outer shield. This type of construction allows for a higher specific throughput, as well as usable transmission length.



(Source: Jamj2000/Creative Commons (CC BY-SA 4.0)/[https://commons.wikimedia.org/wiki/File:Cable\\_coaxial.jpg](https://commons.wikimedia.org/wiki/File:Cable_coaxial.jpg))

Commonly referred to as a “last mile” technology, it is usually the media of choice utilized by cable providers for connection between the modem and the provider termination point. The actual speed limitation of coaxial cable is more closely related to the number of data channels utilized and the limitations of the transmitting/receiving equipment.

Cable Type	Description
Fiber Optic	<i>Fiber optic cables</i> consist of a core made up of optical fibers that is surrounded by glass or plastic strands, which is then surrounded by extra fiber strands or wraps, all of which is surrounded by a protective outer shield. The optical fibers in the core transfer data by utilizing pulses of light.



(Source: Srleffler/Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:Optical\\_fiber\\_cable.jpg](https://commons.wikimedia.org/wiki/File:Optical_fiber_cable.jpg))

### Plenum-Rated vs. Non-Rated Cabling

One important property of cabling is whether or not it is plenum-rated, which focuses mostly on the type of material used for the insulation or jacketing. By definition, plenums are pathways for air to travel, which presents fire hazards pertinent to cabling. Since the air volumes in plenums tend to stoke fires and the air is in one manner or another a supply to spaces occupied by people, flammability and toxicity are concerns for cabling that runs through plenums. In short, plenum-rated cabling is classified as such due to the material being more flame resistant and giving off little or no toxic substances or fumes when burned. You may even find plenum-rated cabling in data centers with limited occupancy, since the same combustion by-products of the insulation that are dangerous to people can be harmful to the electronics in IT equipment.

### Cable Labels

Since cabling is so ubiquitous in MCO facilities today, it is crucial to properly identify what cable serves what purpose and for what equipment. Often, cables have color-coded insulation to create a visual distinction between their purposes. In addition, however, your own specific cable runs should be labeled as much as practically possible. Data cabling, for instance, may have labels identifying network names, IP addresses, IMAC ports, etc. Control wiring should identify what device it is connected to and the control panel it feeds back to. Power wiring should identify the source of the power so electrical isolations can be made safely when working on equipment. Whenever possible, it is best practice to label cabling at least twice—at the origination and termination points—and even at some spots in the middle if it is a particularly long cable run.

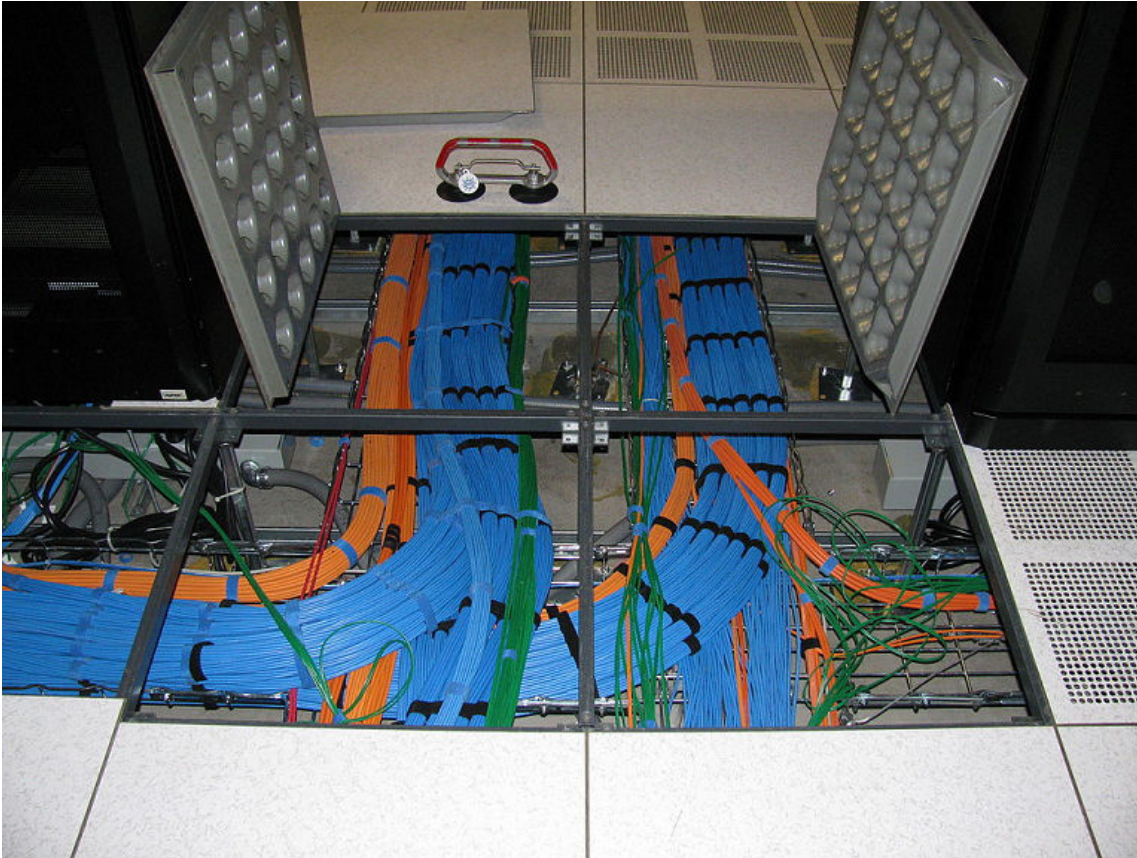
### Cable Segregation

Cabling should also be segregated to the greatest extent possible throughout MCO spaces. First and foremost, after the facility is built, we typically end up only going back to work on certain systems at a time. So if cabling is properly segregated, we do not have to move (or remove!) power wiring just to replace a data cable, for instance. Additionally, there are certain physical properties of cables that can cause interference with other cables; for example, high voltage power cabling can create electromagnetic fields that interfere with data transmission on network cabling.

### Below-Floor Cabling

Depending upon the equipment installed in critical production spaces, power and/or data cabling may be run under the floor—either throughout a raised floor system or in conduits or vaults in the slab. MCO technicians need to know how and where under-floor cabling is run in your facility due

to the risk of disrupting operations by damaging them. Be it for maintenance or just cleaning, it is inevitable that you will end up in or under the floor, and catching your boot on a fiber cable could pull it loose and kill communication to equipment.



*Figure 9-7: Cables run under the raised floor tiles in a data center. (Source: Robert Harker/  
Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/  
File:Under\\_Floor\\_Cable\\_Runs\\_Tee.jpg](https://commons.wikimedia.org/wiki/File:Under_Floor_Cable_Runs_Tee.jpg))*

## Overhead Cable Tray Systems

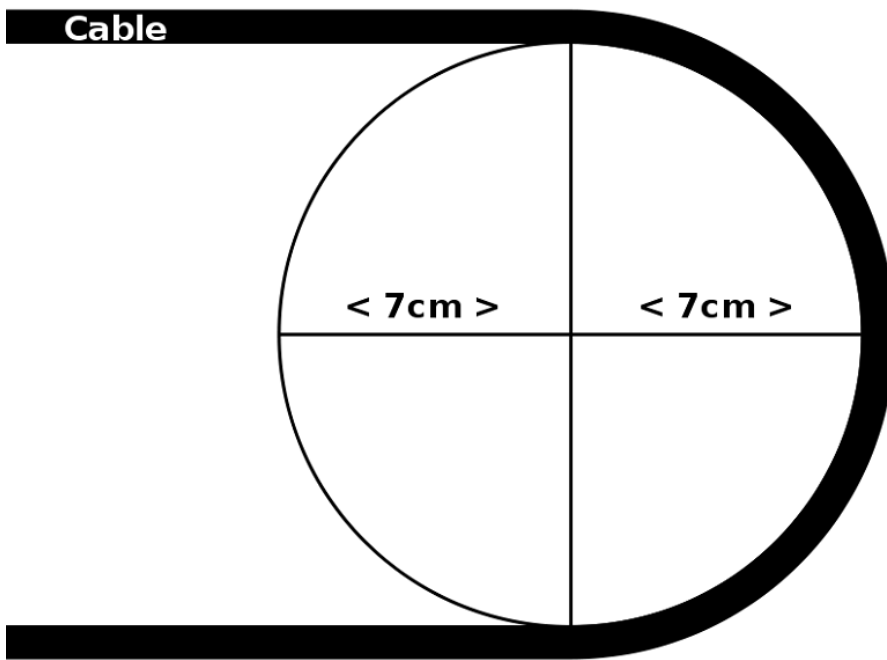
Overhead cabling tray systems use trays, typically made of reinforced metal or plastic, that are mounted to the ceiling or other overhead components in order to run the cables throughout the space. These systems are typically found in data centers or other production spaces if the main space is not on a raised floor system, since it may be impractical to run cabling through or over slab. Second, overhead cabling can be easier to maintain than below-floor cabling if damaged wires need to be pulled or new runs added.



**Figure 9–8:** Overhead cable trays run cables throughout a space. (Source: Leotard/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Wire\\_cable\\_tray02.jpg](https://commons.wikimedia.org/wiki/File:Wire_cable_tray02.jpg))

## Bend Radius Limitations

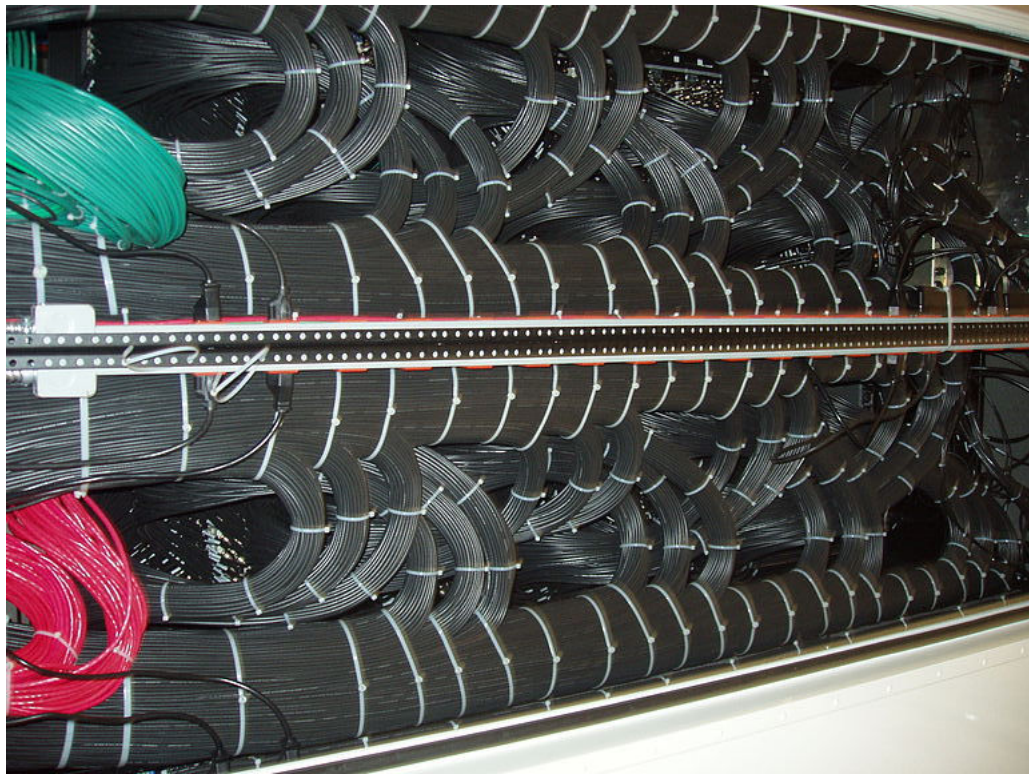
In terms of cabling, *bend radius* refers to the measurement of the minimum amount that a cable can be bent without causing unwanted negative effects (such as damage or a shorter lifespan). Manufacturers establish limits on the bend radius because it can affect transmission capabilities and efficiencies, but primarily because it can damage the cable. If pushed beyond the bend radius, the copper strands in twisted pair or coaxial cables can fray and the strands of glass in fiber optic cables can snap. Bend radius limits are often stamped on the jacketing/insulation of the cable, but can also be found in many industry standards tables based upon the application. If you don't know the bend radius limitation of the cabling you are working with, it's probably best to use as much caution as possible and refrain from bending the cables.



**Figure 9–9:** A diagram illustrating a cable with a bend radius of 7 cm. (Source: Gracenotes/  
Creative Commons (Public Domain)/<https://commons.wikimedia.org/wiki/File:Bendradius.svg>)

## Cable Dressing and Placement

The sheer volumes of cabling in MCO production spaces today is enormous and will only increase as more and more intelligent equipment becomes networked. Therefore, the proper management of cable installation and placement is more than just good housekeeping—it's a necessity. Beyond placement considerations that have already been noted (such as below-floor/overhead and bend radius), you'll want to consider *cable dressing*, which generally refers to arranging adjacent cabling in an organized, orderly manner and making clean connections. That way, when it comes time to repair or replace cabling, you don't end up in the same situation that we've all faced at one point or another: untangling the tangled mess of lights during holiday decorating. It is also best practice to make wiring runs and connections as short as possible so there isn't a tangle of loose wires at the back of a unit (particularly servers and switches where potentially dozens of communication wires are connected) and to leave room to add more cabling in the same area if needed down the road.



**Figure 9–10: Cables that have been neatly dressed and organized. (Source: Pcppeggs/Creative Commons (Public Domain)/<https://commons.wikimedia.org/wiki/File:Patchpanelrear.JPG>)**

## Cable Tracing and Testing

*Cable tracing and testing* refers to any number of techniques used to validate the signal strength, quality, or pathway of installed cabling. This may involve inducing a small amount of voltage at one end to check for continuity or resistance levels. For fiber optic cables, this would be shooting a small beam of light (usually some sort of laser) to see if it comes out unaltered on the other end. When proper care hasn't been taken in system installation, technicians often have to resort to cable tracing to figure out which cable is going where—particularly if cables have been poorly labeled (or not labeled at all!) or if physical, hand-over-hand tracing is not feasible due to the design or arrangement of the equipment.



# ACTIVITY 9–3

## Managing Your Cables

### Scenario

In this activity, you will identify best practices for cabling and cable management.

1. **The bend radius is the amount that a cable can be bent before causing unwanted negative effects such as damage to the cable or a shortened life span.**
  - True
  - False
2. **Which type of cable is made up of a single inner conductor surrounded by a tubular insulated layer, which is surrounded by a tubular conductive layer, all of which is surrounded by an insulated outer shield?**
  - Twisted pair
  - Coaxial
  - Fiber optic
3. **Which type of cable is made up of four interwoven insulated wires that are encased in a single sheath?**
  - Twisted pair
  - Coaxial
  - Fiber optic
4. **Which type of cable is made up of a core of optical fibers that are surrounded by glass or plastic strands, which is then surrounded by extra fiber strands or wraps, all of which is surrounded by a protective outer shield?**
  - Twisted pair
  - Coaxial
  - Fiber optic
5. **Which cable management best practice refers to arranging adjacent cabling in an organized, orderly manner to keep the data center tidy and to easily find and manage connection points?**
  - Labeling
  - Segregation
  - Dressing
  - Tracing/Testing
6. **Which cable management best practice refers to visibly identifying a cable's purpose, the equipment it's connected to, its power source, or other important information at various points along the cable's run?**
  - Labeling
  - Segregation
  - Dressing
  - Tracing/Testing

7. Which cable management best practice refers to using a technique, appropriate to the specific data center design, to validate the signal strength, quality, or pathway of the cabling that has been installed?
- Labeling
  - Segregation
  - Dressing
  - Tracing/Testing
8. Which cable management best practice refers to physically separating and isolating different types of cables from one another in order to prevent interference or other unwanted consequences?
- Labeling
  - Segregation
  - Dressing
  - Tracing/Testing
-

# TOPIC D

## Manufacturing and Other Critical Spaces

While the data center is probably the most common critical space that an organization relies on, there are plenty of other production environments that provide critical services to the organization or its consumers. As an MCO technician, you need to know what some of these other production environments are and how they serve the larger organization, as you may need to work directly with personnel or even equipment within that space to ensure continued operations of your own MCO facility. In this topic, you will identify other common mission critical production environments and their associated equipment.

### Common Mission Critical Production Environments

Knowing that MCOs are the organizations or parts of an organization which require absolute continuity of operational success, it may be hard to know where the line is drawn to identify which functions are absolutely critical to business. For organizations that themselves are not fully mission critical, we can split our view to identify the mission critical production environments within the larger organization that truly can't go down without a serious (if not disastrous) impact to the organization or the people that rely on it.

You've looked at data centers in great detail as it is an industry that is consistently growing (and, currently, most in need of qualified operations professionals), but there are still plenty of other sectors that are considered mission critical facilities and should be approached with the same sensitivity to ongoing, optimal operations. The following are some of these mission critical production environments.

<i>Environment</i>	<i>Description</i>
Research and Development	These are the firms or business units working on innovations to continue to allow the greater organization to thrive. Perhaps they do not operate 24/7, but controlled environments and support systems are critical to protect the work in progress.
Communications	Ranging from air traffic control and emergency response centers, to centralized operations and call centers, these facilities are geared towards 100% availability and free flow of information. They may monitor the entire organizations assets and ensure connectivity to global markets and teams.
Manufacturing	The speed and accuracy of manufacturing technologies continues to grow and improve to the point that raw materials are being used within minutes of arrival to a facility and finished products enter the distribution supply chain almost immediately. While the threat to life or security may be minimal with downtime at these facilities, their ability to generate millions of dollars worth of product in a matter of minutes or hours means that the cost impact of extended production interruptions may threaten the financial security of the organization.

<b>Environment</b>	<b>Description</b>
Hazardous Materials	Production environments dealing with hazardous materials (biotech, raw material processing, weapons, etc.) also require the same MCO sensitivity as the most high-tech data centers due to dangers associated with materials being produced or used. The support systems (waste disposal, airflow management, containment, etc.) are there for a reason and the inability for them to perform their functions may have disastrous consequences.

## Mission Critical Production Equipment by Industry

For the sake of prioritizing maintenance, casualty response, operations personnel training, etc., it's worthwhile to further identify the most critical equipment within the infrastructure of a mission critical production environment. This includes any equipment or other component of the infrastructure that, should any fault or failure occur, production could come to a grinding halt.

Common mission critical equipment in manufacturing environments encompasses all sorts of specialty automated machines, conveyor systems, robotic vehicles, and raw material handling or waste disposal equipment. These are the pieces of equipment that perform each step in the manufacturing process or production line.

Programmable Logic Controllers (PLCs) are the devices that have largely been responsible for the automation of much of modern manufacturing and production, allowing machines to work with speed and precision (without fatigue!) far beyond the capabilities of human workers. PLCs are essentially localized computers that are specially programmed to perform specific actions/functions. PLCs may operate in a standalone manner controlling one machine or system, or they may be networked together to communicate information between other systems and provide real-time production information to MCO operators and technicians.

While PLCs have helped automate a good majority of production tasks, plenty of equipment still requires motive force that cannot come from electricity alone. Hydraulic (fluid) and Pneumatic (gas) systems may operate at extremely high pressures to perform specific manufacturing actions. They supply the energy for a machine to do its job (moving material, pressing/cutting parts out of raw forms, etc.) and are equally important as the components controlling them (typically, PLCs).

## ACTIVITY 9-4

### Identifying Mission Critical Production Environments and Equipment

#### Scenario

In this activity, you will identify mission critical production environments and their equipment.

---

- 1. The continued operations of other important production sectors, such as manufacturing or communications, are not as important to maintain because they do not provide functions that are absolutely critical to an organization or the general public.**
    - True
    - False
  - 2. When it comes to a production environment, any piece of equipment or other component of the infrastructure that could halt the production operations of the facility if a fault were to occur should be considered mission critical.**
    - True
    - False
-

## Summary

In this lesson, you identified and applied industry best practices, strategies, and techniques for the proper design and configuration of critical production spaces. As an MCO operator, you need to have a strong working knowledge of the secondary spaces that help keep your MCO facility running smoothly and allow it to continuously operate and provide its critical services to those who rely upon them; this includes those critical production spaces ranging from the data center and the important information services, to the manufacturing spaces that physically construct the products it provides to the organization or its consumers. By following industry best practices and industry-standard strategies and techniques, you can help ensure that these critical production spaces are functioning under optimal conditions, which in turn allows your MCO facility, in general, to continue to operate properly as well.

# 10 | Networking

## Lesson Objectives

In this lesson, you will identify and apply networking fundamentals as they apply to a mission critical facility. You will:

- Identify the basic components of a network.
- Identify basic networking concepts.
- Identify types of networks.

## Lesson Introduction

In any organization, including Mission Critical Operations (MCOs), one of the common tasks that will take place on a daily basis is the transferring of information between people and places—whether it is in the form of sending emails, sharing files, or accessing important devices and their respective data. The connection of devices and the ability to transfer data between them, of course, is known as networking. In MCOs—where the sharing of important data between personnel within the organization is imperative for the continued, safe operations of the facility—a fully-functional network is an important component of those daily operations.

As an MCO technician, you need to have working knowledge of the basic concepts of networking—including the components that make up a network, how those components work (and work together), and the types of networks these parts comprise—in order to ensure that your organization's network is configured properly. In this lesson, you will identify and apply networking fundamentals as they apply to a mission critical facility.

# TOPIC A

## Basic Network Components

In order to provide the kind of information sharing that is imperative for any organization to function in today's data-driven world, there are a number of necessary components that all have to work together to transmit information to the correct place at the right time. As an MCO operator, you need to have a fundamental understanding of the various devices that make up your organization's network and the functions they serve within the network. In this topic, you will identify the basic components of a network.

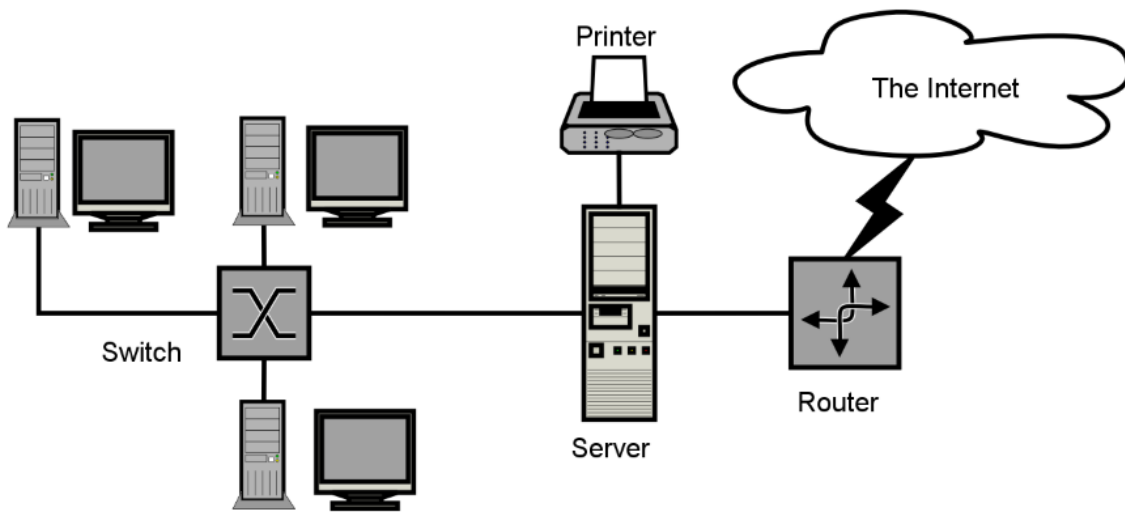
The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Computer network
- Client
- Server
- NIC (network interface controller)
- Router
- Switch
- Gateway
- Patch panel
- Manhole
- Demarcation point (demarc)
- Communication room
- Service closet
- Duct banks
- Distribution frame

## Computer Networks


At the most rudimentary level, a *computer network* is any configuration of two or more computers or other electronic devices that are connected together for the implicit function of exchanging data between them. The simple act of performing a general Google™ search on any mobile device involves hundreds of interconnected and dependent networks. Networks can vary widely in purpose, complexity, and implementation; however, every network includes common components that provide the resources and communications channels necessary for the network to operate.





**Figure 10-1: A diagram of a network.** (Source: SilverStar/Creative Commons (CC BY-SA 3.0)/ <https://en.wikipedia.org/wiki/File:Sample-network-diagram.png>)

There are really only two types of core networks: Local Area Networks (LANs) and Wide Area Networks (WANs). A LAN is a network comprised of multiple data devices located in the same physical geographical location. This can be two computers in a home, an office, a classroom, or all the computers located in a single office building. A WAN is a network that spans across multiple geographical locations, typically comprised of multiple LAN networks that enable the exchange of data across the geographically diverse locations. For example, the exchange of information between an accountant’s computer physically located in New York and a customer’s device located in Los Angeles is facilitated by a WAN.

	<p><b>Note:</b> You will learn about the more detailed differences between these later in this lesson, but these two types will be mentioned throughout this lesson and basic knowledge of these two types of networks will be helpful.</p>
---	---

## Components

While the network technology has greatly improved since inception, there are several common components that make up a computer network, each of which performs a specific task.

<b>Network Component</b>	<b>Description</b>
Network devices	Hardware components that allow for the implementation and use of the network. Common devices found within a network include computers, servers, network interface controllers (NICs), switches, firewalls, and routers.
Physical media	Media components that connect devices to a network and transmit data between the devices. The three most widely utilized types of physical media that you are likely to encounter includes Ethernet cables, coaxial cables, and fiber optic cables.
Network adapter	Hardware components/devices that enable your computing equipment to interface with a local area network and translates data between them. There are two primary categories of adapters—physical (or wired) connection network adapters and wireless connection network adapters.

---

<b>Network Component</b>	<b>Description</b>
Network operating system (OS)	Software that controls network traffic and access to common network resources. They are typically classified as either a Network Device OS (which are typically manufacturer-specific and employ proprietary services specific to the device's performance capabilities, such as Cisco IOS®) or a Computer Network OS (which are typically more universally applied across devices in large-scale implementations, such as Windows Server®).

---

## Clients

A *client* is a device that utilizes a network's resources or functions for the purpose of completing a task. Clients within a network were at one point limited to desktop computers and possibly printers. Today, client devices can be desktop computers, laptops, tablet devices, handheld mobile devices, printers, and even televisions. These devices have to work concurrently on a single network without interference while maintaining the security of said network. This would seem like a tall order but it is handily managed by a combination of servers and routers also on the network. This type of seamless functionality is the result of many years of research and development, as well as adherence to core standards and formats set by the IEEE (Institute of Electrical and Electronic Engineering).

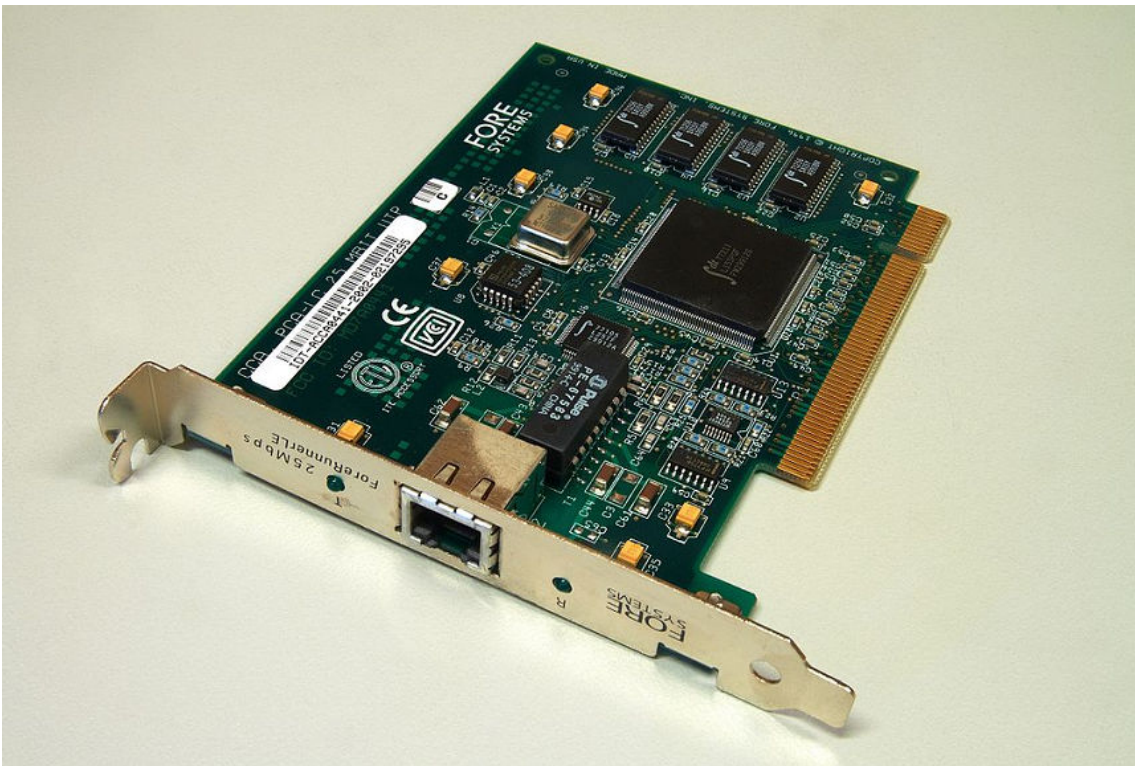
## Servers

A *server* is a non-client computer on the network that performs the activities necessary for the continued functionality of a group of networked client computers or devices. In terms of network functionality, these servers usually provide centralized access to and storage for shared resources (such as applications, files, or services such as email) and perform network and file security functions.

For example, the accounting department within your organization may require access to employee compensation information while the service desk department does not. This access is governed by permissions assigned within the network server. Servers can also help to maintain security of a given network by ensuring all client devices are utilizing the correct level of anti-virus software, verifying that all client access adheres to a specific security schema (such as password strength), and performing centralized backups of pertinent data to reduce any loss caused by client device failure.

## NICs

A *network interface controller (NIC)*, also called a network interface card or network adapter, is a device that connects computers or other devices to the network. The NIC carries a device's individual identification information, which is utilized by other devices to identify and share data between them.



**Figure 10–2:** A NIC. (Source: Barcex/Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:ForeRunnerLE\\_25\\_ATM\\_Network\\_Interface\\_\(1\).jpg](https://commons.wikimedia.org/wiki/File:ForeRunnerLE_25_ATM_Network_Interface_(1).jpg))

## Routers

A *router* is a device that connects multiple networks by “routing” data packets between them to allow many different types of devices to communicate and exchange data. A router’s main function is to develop the best data paths between two devices. This information is known as a routing table and is stored on and utilized by the router for each data request. Without a router, data cannot be shared between multiple localized networks (like an office’s network) to form the larger, wide-reaching networks (such as a corporation’s geographically-separated network). In short, a router is the brain of the network and forms the basis of all complex network communications.



**Figure 10–3:** A wireless router. (Source: Tors/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:AVM\\_FRITZ!Box\\_WLAN\\_3270.jpg](https://commons.wikimedia.org/wiki/File:AVM_FRITZ!Box_WLAN_3270.jpg))

## Switches

A *switch* is a device used to connect multiple physically networked resources or devices for the purpose of sharing data. The switch is the first component in the physical network, and is tasked with transmitting data correctly between multiple connected devices. Multiple devices located within the same geographical area that are connected physically and wirelessly to a single switch form the basis of a LAN. A switch could be used to connect client devices to a server, clients to a networked resource (such as a printer), or to connect clients to a gateway device for access to an external network.



*Figure 10–4: Two rack-mounted network switches with connected cables. (Source: ShakataGaNai/  
Creative Commons (CC BY-SA 3.0/[https://commons.wikimedia.org/wiki/  
File:Network\\_switches.jpg](https://commons.wikimedia.org/wiki/File:Network_switches.jpg))*

## Gateways

A *gateway* is a device utilized for connecting two or more networks utilizing different communication protocols. Not to be confused with a router, which performs communications between networks utilizing similar protocols, a gateway is tasked with performing data transfer in a much more complex environment. An example of a gateway are the devices, called nodes, that are utilized by Internet Service Providers (ISPs) to grant access to the Internet.

Gateways are also tasked with performing Network Address Translation (NAT), which is the directing of data traffic based on the IP address information attached to data packet. NAT is the mechanism by which a request initiated within a private network is routed to an external network, answered, and routed back to the initiating device. An example would be making a refresh request on a social media application. The refresh request is processed almost instantaneously through the work of many gateways and delivered back to the requesting device as an updated view.



**Figure 10–5:** A cable modem acts as a gateway for a residential network. (Source: Larocomp/  
Creative Commons (Public Domain)/<https://commons.wikimedia.org/wiki/File:EPC3925.jpg>)

## Patch Panels

A *patch panel* is a device containing numerous ports used to connect multiple devices in various combinations, ultimately making cable management and physical device connectivity changes much easier. In the networking world, patch panels are utilized in large physical networks such as an office building or a data center, and provide order and ease of modification to larger network installations that inevitably become a sea of cables in the equipment rack.

Patch panels most often connect to switch ports in a 1:1 configuration, which means that one patch panel port is wired to one switch port. Why not just connect directly to the switch? Well, should you need to physically modify the network, such as adding a user who utilizes a different subnet on the same floor, it is much easier to make the modification via the patch panel than the network rack. A patch panel on each floor of a building allows a greater deal of control versus wiring all floors and terminating at the actual switch. This also has the added benefit of streamlining network issue triage since testing from the patch panel to the end port is easier than from the switch.



**Figure 10-6:** A series of rack-mounted switches (on the bottom) connected to patch panels (on the top) provide clean, organized cable management. (Source: Dsimic/Creative Commons (CC BY-SA 4.0)/[https://commons.wikimedia.org/wiki/File:19-inch\\_rackmount\\_Ethernet\\_switches\\_and\\_patch\\_panels.jpg](https://commons.wikimedia.org/wiki/File:19-inch_rackmount_Ethernet_switches_and_patch_panels.jpg))

## Connection Points

There are numerous connection points within a network where communication data is passed, starting with the cabling as it enters the building and then throughout, as it makes its way to the various locations inside the building.

<b>Item</b>	<b>Description</b>
Manholes	A <i>manhole</i> is the access point or "service entranceway" where communication equipment and cables from the service provider are located and can be accessed outside of the building. While they are not regularly utilized by MCO personnel—they would be accessed by the company that owns and provides the utility—they become critical in the event of a network fault that is found to be external to a building.
Service entrance/ Demarcation point	The service entrance or <i>demarcation point</i> ( <i>demarc</i> ) is the location within or on a building where the service provider's wiring ends and the internal building wiring begins. Service providers are responsible for the fidelity of the wiring up to this point. This is where the "last mile" of carrier cabling terminates. A demarcation point can also be the point where the communication facilities for two service providers interface, or the hand-off point of communication responsibility between two organizations.
Communication room	The <i>communication room</i> within a building is a centrally located room with enhanced power and cooling capabilities utilized for the setup and storage of network communication equipment. This room is most often a secure access area with access being granted only to IT network professionals.

Item	Description
Service closet	A <i>service closet</i> is an offshoot of the dedicated communication room. These closets are usually found on each floor of a building and house non-critical equipment such as patch panels, signal repeaters, or wireless access points. These provide a point of investigation and/or modification for a particular portion of the network and prevents unnecessary interaction with the core equipment located in the communication room.
Duct banks	Communication cabling, whether internal or external to the building, has to travel in the most protected environment possible. To do so, <i>duct banks</i> —a collection of conduits or pipes through which the networking cables are passed and distributed—are most often utilized. The piping in duct banks are most often constructed of PVC piping, however, in installations that see the wiring external to the building, the pipes are sometimes encased in concrete to give an additional amount of protection/isolation. In a single-building installation, duct banks are distributed throughout the building and inside the communication room; in a multi-building/campus installation, they would be used to protect cabling going from building to building.
Distribution frame	A <i>distribution frame</i> is a centralized point in the network where a larger circuit is broken down into smaller user-specific connections. A Main Distribution Frame (MDF) is usually a cable rack where the public lines coming into a building interface with the local network wiring. In larger installations, an Intermediate Distribution Frame (IDF) is utilized to interface between the MDF and the internal network. For example, the external utility provider's circuit would connect to the MDF (as a demarcation point) and subsequently connect to an IDF on each floor, which may contain additional communication equipment such as switches or patch panels for connections to the end user equipment.

## Network Location

Location in network setups is one of the most important, but often overlooked parameters. Everything from the core equipment to the network cables require optimal locations to get the best possible performance.

In the case of core equipment—routers, switches, gateways, and other wireless access point devices—heat is the enemy. Entire rooms in offices are built around the purpose of keeping networking equipment cooled. Network cabinets generate a high amount of heat and as such are most likely to be located in the basement of a building where ambient temperatures are not just lower, but are less likely to fluctuate. Core equipment usually also requires a large amount of power to run as this infrastructure is never switched off. This is one of the reasons this equipment is centrally located, since the circuits needed to handle the consistent load are easier to design and build for a single location rather than a distributed location schema.

Network cables have a maximum range of effectiveness over which data can be transferred without introducing errors. To reduce the chance of interference, you want to use the shortest cable runs possible to keep the data signal strong and robust. This range can also be affected by the environment. For example, you would not want to use the same wiring conduit for networking and electrical cables. While network cables have some shielding, the proximity to live electrical wires would greatly reduce their range as the network signal absorbs interference from the electrical pulses. For this reason, network cables are usually routed away from heavy electrical sources. You will rarely find a network jack next to a wall socket for this very reason, and if you do, the cables inevitably travel in opposite directions behind those wall plates.



# ACTIVITY 10-1

## Identifying Basic Network Components

### Scenario

In this activity, you will identify the basic components that make up a network.

- 1. A computer network is a collection of computers or other electronic devices that are connected together for the purpose of exchanging data.**
  - True
  - False
- 2. Which of the following are the common categories of components included in a computer network?**
  - Adapters
  - Devices
  - Applications
  - Media
  - Files
  - Operating systems
- 3. Which network component utilizes a network's resources or functions for the purpose of completing a task?**
  - A client
  - A server
  - An application
  - An operating system
- 4. Which network component performs the activities that provide the resources or functions needed for the computers or devices on the network to complete their tasks?**
  - A client
  - A server
  - An application
  - An operating system
- 5. Which network component is used to transfer data between networks that use different communication protocols?**
  - A network interface controller
  - A router
  - A switch
  - A gateway
  - A patch panel

6. Which network component develops the best path for the exchange of data packets between different types of devices and across multiple networks?
- A network interface controller
  - A router
  - A switch
  - A gateway
  - A patch panel
7. Which network component connects multiple devices that are using or are being used by the network in various combinations, to provide both device connectivity and cable management?
- A network interface controller
  - A router
  - A switch
  - A gateway
  - A patch panel
8. Which network component connects the various devices to the data network, using unique identifiers to identify each device and share data between them?
- A network interface controller
  - A router
  - A switch
  - A gateway
  - A patch panel
9. Which network component connects multiple data devices on the network in order to transmit data between them?
- A network interface controller
  - A router
  - A switch
  - A gateway
  - A patch panel
-

# TOPIC B

## Basic Networking Concepts

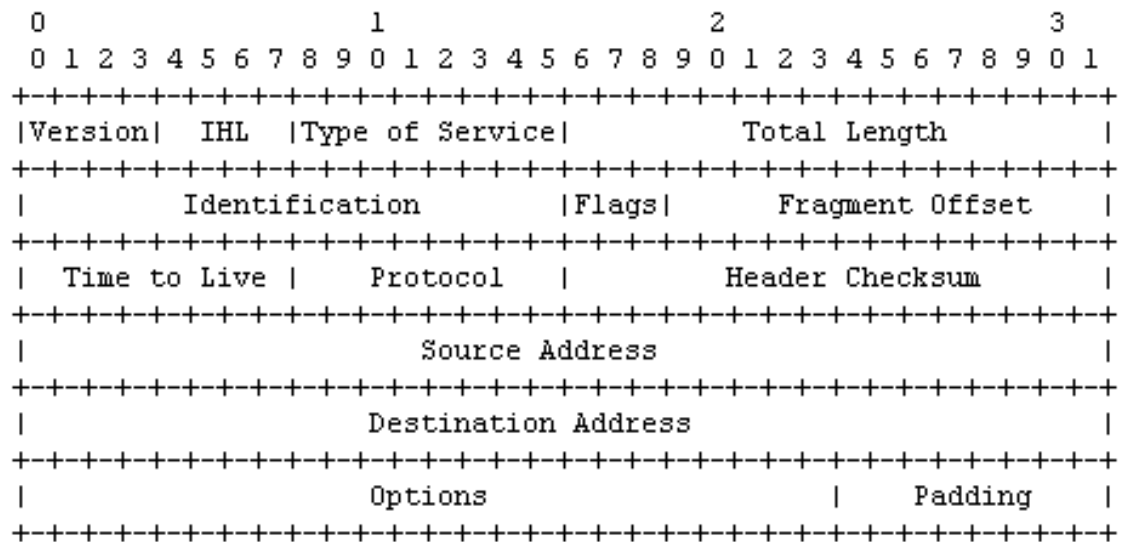
In addition to the necessary components that make up the network, there are a number of conceptual processes and functions that actually work to transmit data between the devices on a network. As an MCO operator, you need to have a fundamental understanding of how a network operates, in order to ensure that the continued, successful transfer of data takes place across the organization. In this topic, you will identify basic networking concepts.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Data packet
- IP (Internet Protocol)
- Network address
- Network name
- OSI (Open Systems Interconnection) model
- TCP/IP (Transmission Control Protocol/Internet Protocol)
- IP address
- Subnet
- Subnet mask
- Private IP address
- Domain name
- Host name
- FQDN (Fully Qualified Domain Name)
- DNS (Domain Name System)
- HOSTS file

## Data Packets

A *data packet*, or datagram, is a segment of data that is utilized for communication between two networked devices. A data packet is made up of quite a bit more than just the data being transferred, in order for it to be received by the intended destination device and to then reconstruct multiple packets into the intended file or request once received. Therefore, data packets contain elements such as the source address, destination address, data size, sequence number, communication protocol, and other information that gives it the ability to navigate the multitude of devices on any given network to reach its destination.



Example Internet Datagram Header

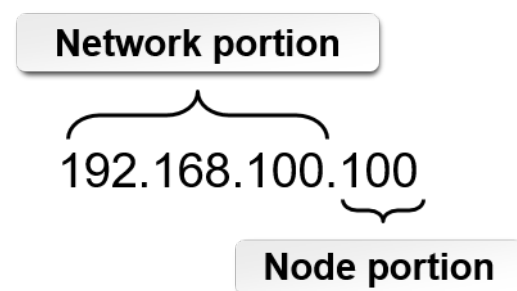
**Figure 10–7:** A diagram of the parts of a data packet. (Source: Jon Postel/Creative Commons (Public Domain)/<https://commons.wikimedia.org/wiki/File:Ipv4fejlec.png>)

## Internet Protocol

*Internet Protocol (IP)* is the communication protocol utilized by all networked devices, by which data packets are structured, addressed, and transmitted. Internet Protocol functions by breaking data into multiple packets, giving them a unique identifier that contains both the sender's and receiver's Internet address, and then transmitting these packets through the network (LAN and WAN) to the receiving computer. The packet is picked up, read, and passed along multiple gateways until it reaches its destination address. All of this based on the address data assigned using the Internet protocol. In layman's terms, Internet Protocol is how your data transmission or request gets to where it needs to be, correctly and intact.

## Network Addresses

A *network address* is the unique identifier given to any device, whether client or host, which allows it to be identified within a network. A network address typically includes two parts: the first part identifies the network, and the second identifies a node on the network. In a modern environment, this is most often your IP address. Your network address, however, can be other unique identifiers such as your MAC address or even a phone number in POTS (Plain Old Telephone Service) systems.



**Figure 10–8:** A network address contains the network and node portions. (Source: Logical Operations for NCMCO)

## Network Names

A *network name* is a string of characters utilized to uniquely identify a specific network and the nodes contained within it. The network name can be used to isolate specific nodes to network pathways and data only pertinent to that group. This creates a layer of security and also serves as a way to make networks more efficient. For example, imagine if all data transmissions utilized the same data path. The network performance would inevitably suffer and the risk of sensitive data being compromised would grow exponentially. Utilizing network names allows data to travel along different data paths and get to its destination with less margin of error.

## The OSI Model

Ever wonder how there can be a large number of network device manufacturers utilizing proprietary network operating systems and the exponential number of software application developers, all utilizing the same networks without issue? This is because of the *Open Systems Interconnection (OSI) model*: the communication standard by which all networks operate regardless of their configuration and technology utilized. The OSI model is made up of seven tasks, divided up into different layers of protocols that work together to create a normalized pathway for data transmission.

<i>OSI Model Layer</i>	<i>Description</i>
Layer 1: Physical	This layer defines the physical, or mechanical, specifications of a data network. This includes the specifications of the medium (copper or fiber cables), pin assignments, the signal timing, and the voltages utilized. This layer guarantees that the hardware being utilized has the ability to transmit and receive data regardless of manufacturer.
Layer 2: Data Link	This layer deals with the transmission of data packets and their protocol management. It is utilized to handle errors found in the physical layer, as well as control flow of data and synchronization. This layer is divided into two sublayers: Media Access Control (MAC), which controls how a device on the network gains access to data and assigns the permissions to transmit it; and Logical Link Control (LLC), which controls the synchronization of packet data and manages error checking.
Layer 3: Network	This layer enables the switches and routers on the network to operate, giving them the ability to create and transmit data sequences from one device to another through IP addressing and providing error and congestion control.
Layer 4: Transport	This layer ensures a complete transfer of data on a network by managing the transfer of variable sized data sequences between the sending and receiving hosts. By ensuring that a data packet is received before transmitting the subsequent packet in the sequence, this layer ensures that a complete data file is received.
Layer 5: Session	This layer controls the communication sessions between hosts (computers). It manages the establishment, maintenance, and termination of a session, which is how the application processes communicate with each other succinctly across a network. Functions such as security and logging are performed at this layer.
Layer 6: Presentation	This layer formats the data that will be presented to the application layer. This layer is sometimes referred to as the translation layer as it translates data from network to application format and vice versa. Functions such as data compression, character code translation, and encryption or decryption are performed at this layer.

<i>OSI Model Layer</i>	<i>Description</i>
Layer 7: Application	This layer supports the end user processes and allows sharing of networked resources commonly utilized. Functions such as directory services, remote printer access, email, and network management reside at this layer of the OSI model.

## The TCP/IP Model

The *Transmission Control Protocol/Internet Protocol (TCP/IP) model* is the suite of communication protocols that are used as the standard for transmitting data over networks. TCP/IP uses the two protocols for different functions: the Transmission Control Protocol (TCP) is responsible for the creation of multiple packets from a single file for transfer across a network, as well as reassembling the file at the destination; the Internet Protocol (IP) handles the addressing of the generated packets. They work together to ensure the proper transfer and receipt of the millions of terabytes of data transferred across the Internet daily.



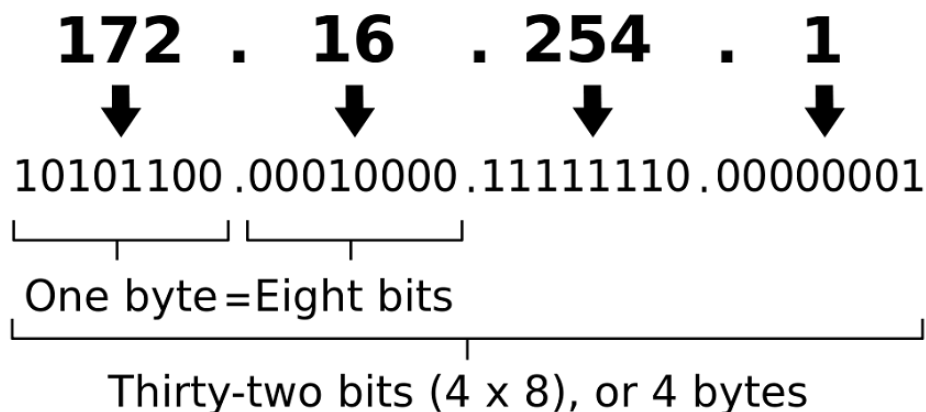
**Note:** TCP/IP is the protocol on which the Internet is based.

## IP Addresses

An *IP address* is a unique numerical label assigned to individual devices that are a part of a TCP/IP network, through which data can be transmitted and received over a network. The addresses of both the transmitting and receiving devices are contained within data packets. This ensures that the data reaches the correct destination and confirms to the transmitting device that the data was received. IP addresses can be public or private, which determines if the device is accessible through the larger public network.

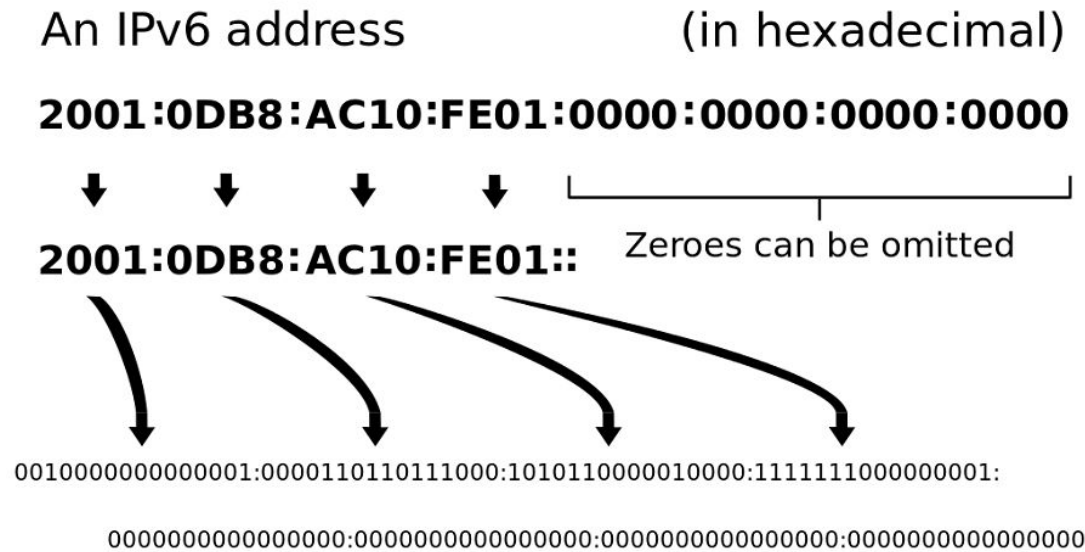
An Internet Protocol Version 4 (IPv4) address consists of a 32-bit binary numerical label, typically separated by dots into four 8-bit octets for readability. Each octet is converted to a single decimal value ranging from 0 to 255, but the first number cannot be 0. In addition, all four numbers cannot be 0 (0.0.0.0) or 255 (255.255.255.255).

An IPv4 address (dotted-decimal notation)



*Figure 10–9: An example of an IPv4 address. (Source: Indeterminate/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:ipv4\\_address.svg](https://commons.wikimedia.org/wiki/File:ipv4_address.svg))*

An Internet Protocol Version 6 (IPv6) address consists of a 128-bit binary numerical label, typically separated by colons into eight groups of four hexadecimal digits (or two 16-bit octets) for readability.



**Figure 10–10: An example of an IPv6 address.** (Source: Indeterminate/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Ipv6\\_address.svg](https://commons.wikimedia.org/wiki/File:Ipv6_address.svg))

The majority of IP addresses currently adhere to the IPv4 standard with future plans for the widespread deployment of the updated IPv6 standard. The primary driving factor for the adoption of the IPv6 standard is the continued proliferation of connected devices, which will quickly deplete the available IPv4 addresses—with IPv4, there are only 4.3 billion addresses available using the 32-bit protocol, while IPv6 can provide 340 undecillion (which is 340 trillion trillion trillion!) addresses using the 128-bit protocol. IPv6, being a much more robust protocol, will provide the needed address range to accommodate all devices for the foreseeable future.

## Subnets

A *subnet* (or subnetwork) is a portion of a network that shares a common address component. Subnets allow for multiple logical networks to be created within a class of IP addresses, which is a much more efficient way of allocating addresses for a larger network containing many devices or nodes. This helps improve network performance as devices within a specific subnet will only have access to the portions of the network allocated, keeping unnecessary traffic to a minimum.

## Subnet Masks

Once a network reaches a level of complexity requiring subnets, a *subnet mask* may also need to be utilized, in which a numerical version of the IP address, divided into a network address and host address, is assigned to a specific subnet. A portion of the host address is then utilized to identify to which subnet it belongs. Subnet calculation is one of the more complicated portions of complex network configuration—so much so, that there are many programs and websites dedicated specifically to the calculation of subnet addresses.

## IP Address Classes

IP addresses are assigned based on the need and size of an organization in question. To accomplish this and maintain a level of order, IP addresses are assigned to one of the following classes.

<i>IP Address Class</i>	<i>Characteristics</i>
Class A	<ul style="list-style-type: none"> <li>• Includes IP addresses 0.0.0.0 through 127.255.255.255.</li> <li>• Can contain a total of 127 unique networks with 16,777,214 possible IP addresses per network.</li> <li>• Usually allocated to very large multi-national organizations.</li> </ul>
Class B	<ul style="list-style-type: none"> <li>• Includes IP addresses 128.0.0.0 through 191.255.255.255.</li> <li>• Can contain a total of 16,384 unique networks with 65,534 possible IP addresses per network.</li> <li>• Usually allocated to Internet Service Providers (ISPs) and large networks such as educational institutions or hospitals.</li> </ul>
Class C	<ul style="list-style-type: none"> <li>• Includes IP addresses 192.0.0.0 through 223.255.255.255.</li> <li>• Can contain a total of 65,534 unique networks with 255 possible IP addresses per network.</li> <li>• Usually allocated to small/midsized companies.</li> </ul>
Class D	<ul style="list-style-type: none"> <li>• Includes IP addresses 224.0.0.0 through 239.255.255.255.</li> <li>• Reserved for multicast functionality, which is the distribution of data from a single host to multiple clients or devices.</li> </ul>
Class E	<ul style="list-style-type: none"> <li>• Includes IP addresses 240.0.0.0 through 255.255.255.255.</li> <li>• Reserved for research and development use by the Internet Engineering Task Force (IETF).</li> </ul>

## Private IP Addresses

To prevent possible IP address conflicts, certain ranges of IP addresses are reserved as *private IP addresses*. The addresses within these ranges are not routed publicly and are reserved for private internal network use only. These ranges fall under three classes:

- Class A: 10.0.0.0 through 10.255.255.255
- Class B: 172.16.0.0 through 172.31.255.255
- Class C: 192.168.0.0 through 192.168.255.255

Private IP addresses are arguably the most often reused range of IP addresses, as it is possible for two different organizations to use the exact same range of addresses since their networks are not connected. Networks using these IP addresses are not visible to the Internet without the use of a gateway device such as a modem.

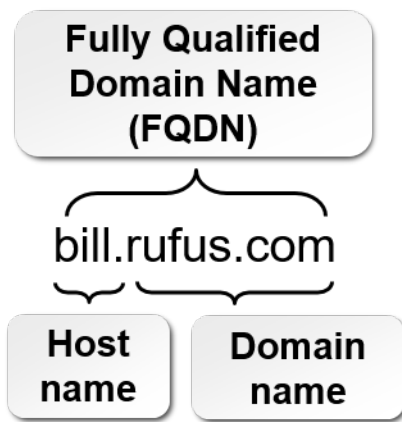
## Domain Names

A *domain name* is the unique label assigned to a network resource that identifies the administrative authority, or domain, to which that resource belongs. In layman's terms, it represents the name assigned to any IP resource—whether that is a computer, a network, or a service—that is accessed via the Internet. For example, the network for the Rufus Company would likely be rufus.com. Domain names are formed and managed by the Domain Name System (DNS).

## Host Names

A *host name* is a unique alphanumeric identifier, up to 255 characters long, that is assigned to a device or node within a network for the purpose of communication. A host name combined with the host's domain name forms the node's *Fully Qualified Domain Name (FQDN)*. For example, two computers with the host names Bill and Ted residing on the Rufus Company's network (rufus.com) would have an FQDN of bill.rufus.com and ted.rufus.com respectively.





**Figure 10–11:** A host name combined with a domain name forms the FQDN. (Source: Logical Operations for NCMCO)

In a networked environment, a computer can be reached via its IP address or its host name; however, the host name must be resolved to an IP address before IP-based communication can be utilized. Host names are also utilized to communicate with devices residing on the same and different networks.

## DNS

The *Domain Name System (DNS)* is a hierarchical system by which domain names are translated into IP addresses. Most commonly utilized for Internet communications, DNS makes it easier for users to remember a specific resource rather than recalling a specific IP address. DNS utilizes a distributed database system to store the translation tables that map the domain names to their translated IP addresses. This means that when a domain name is specified, the request will be routed from server to server until the appropriate IP address entry is found in the translation table and returned, providing access to the resource.

## The HOSTS File

A *HOSTS file* is a plain text file, containing a list of IP addresses and their related host names, that is utilized by devices to resolve a host name to an IP address. It is the first point of validation of a requested host name before a DNS server is addressed. The HOSTS file resides on the client computer or server within the file system of the operating system, and can only be updated by the local administrator.

```

# Copyright (c) 1993-2015 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host
# name. The IP address and the host name should be separated by at least
# one space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97      rhino.acme.com          # source server
#       38.25.63.10     x.acme.com             # x client host
#
# localhost name resolution is handled within DNS itself.
127.0.0.1      localhost
192.168.20.252 bridgeport
192.168.20.148 bill.rufus.com
192.168.20.122 ted.rufus.com

```

*Figure 10–12: The HOSTS file for a device on a network. (Source: Logical Operations for NCMCO)*

## DNS Record Types

DNS records are the mapping records that a DNS server uses to determine which IP address a specific domain name is associated with. In conjunction with DNS records, specific commands dictate the action of the DNS server. These record types provide additional instructions that help the server determine what information should be returned. Some of the more commonly utilized DNS record types include the following.

<i>DNS Record Type</i>	<i>Description</i>	<i>Function</i>
A or AAAA	Address Record	"A" returns a 32-bit IPv4 address associated with a host name. "AAAA" returns a 128-bit IPv6 address associated with a host name.
CNAME	Canonical Name Record	Specifies that the destination can be reached via one or more host names (i.e., an alias). There must be an associated "A" record for this to operate successfully.  For example, Neo.Morpheus.com CNAME Bill.Rufus.com will direct all requests going to Neo.Morpheus.com to Bill.Rufus.com.
MX	Mail Exchange Record	Identifies the mail exchange servers available for a specific domain.

<i>DNS Record Type</i>	<i>Description</i>	<i>Function</i>
SSHFP	SSH Public Key Fingerprint	This is a record of the public host fingerprints used in Secure Shell encryption authentication. These records assist in verifying authenticity of the host.

These are just a few of the available DNS record types. The list is updated as additional functionalities are added to the DNS Record database. The available records and accompanying functionalities are managed by the Internet Engineering Task Force (IETF) through various Request for Comments (RFCs).

## The DNS Hierarchy

The DNS system and the domain names it forms are hierarchical, which allows DNS servers on the Internet to use a minimum number of queries to locate the source of a domain name. Each portion of the DNS address represents a different level of the hierarchy: the top-level domain name, then the first-level domain (or subdomain) name, and so on, until the FQDN for an individual host is complete.

A few examples of top-level domain names that you might be familiar with include:

- .com, which denotes a commercial organization.
- .edu, which denotes an educational institution.
- .gov, which denotes a government institution.
- .mil, which denotes a military group.
- .net, which denotes a network organization (originally used only by service providers, but now utilized by all matter of businesses).
- .org, which denotes an organization (such as a non-profit, school, community, or other group).
- .int, which denotes an international organization.

To better understand the DNS hierarchy, take the two computers, Bill and Ted, that reside on the Rufus Company's network. From a hierarchical standpoint, the computers represented in the host name of the company's website, Rufus.com, would be represented on the Internet as bill.rufus.com and ted.rufus.com respectively. This would be translated as .com, the top level indicating a commercial identity; .rufus, the first level or subdomain indicating the Rufus Company; and .bill or .ted, the second level or subdomain indicating Bill or Ted are a division of the Rufus Company.

## The DNS Name Resolution Process

What happens when you enter a web address into your web browser? The website, or DNS name, must be resolved to an IP address to allow connection and transmission of data from the requested site. This is called the DNS Name Resolution Process. It is, as is the nature of DNS, a hierarchical process. In short, it follows this path:

1. The website address request is made and routed to a top-level DNS server (.com, .gov, .net).
2. The DNS server receives the request and checks its HOSTS file in attempt to resolve the request. If unresolvable, the request is sent to another server for resolution.
3. The server may resolve the request to the domain. If there is a specific host required, the request is forwarded to a DNS server within the domain for translation.
4. The DNS server within the established domain resolves the request to the host name. The IP address is returned to the requesting device and connection is established.

## Common TCP/IP Commands

As with any complex network of machines, there will come a time when performance is being impacted and you need to troubleshoot the issue. To help with this, there are basic commands that

are included in all operating systems that you can use, via basic command line shells, to troubleshoot and configure connectivity and name resolution.

There are a few common commands that you may utilize to troubleshoot your network.

<i>TCP/IP Command</i>	<i>Description and Purpose</i>
PING	This command tests the connection between two hosts using the Internet Control Message Protocol (ICMP) to determine if the remote machine can receive the test packet and reply. Results are reported in milliseconds, providing a measure of how fast the packet was sent and a reply received, which is a great indicator of network path health.
TRACERT	This command (commonly known as trace route) displays the pathway taken by a packet to reach a destination. This command returns the name/IP address of each hop used to reach a destination and can be used to determine the point of failure during a transmission.
NETSTAT	This command provides a view of the network statistics including network connections (both inbound and outbound), routing tables, and specific information about the amount of inbound/outbound traffic.
IPCONFIG	This command provides information about the current network configuration on a host machine, making it one of the most useful commands when performing initial troubleshooting of a localized network issue. Sub-functions of this command can be utilized to modify and reset current network parameters.
ARP	This command allows a host terminal to view a table of locally resolved hardware (or MAC addresses) on a network and can be used when trying to resolve an address resolution issue. The table is updated as you access different remote hosts. The ARP command allows you to review a listing of recently resolved addresses; or, if an address has been reconfigured, the ARP command allows you to clear the table, which helps the host terminal learn the new address and update its ARP database for future requests.

---

# ACTIVITY 10-2

## Identifying Basic Networking Concepts

### Scenario

In this activity, you will identify basic networking concepts.

---

1. **A data packet only contains the data that is being transferred.**
  - True
  - False
  
2. **What is the name of the system of communication rules that all networked devices follow, that allow data packets to be structured, addressed, and transmitted correctly between them?**
  - The OSI model
  - The TCP/IP model
  - Internet Protocol
  - The HOSTS file
  
3. **What is the name of the system of communication rules that is the standard for transmitting data over networks?**
  - The OSI model
  - The TCP/IP model
  - Internet Protocol
  - The HOSTS file
  
4. **What is the name of the system of communication rules under which all networks operate regardless of the technology they use and the way that they are configured, allowing data transmission between them?**
  - The OSI model
  - The TCP/IP model
  - Internet Protocol
  - The HOSTS file
  
5. **What is the unique identifier given to a device that allows it to be identified within a network?**
  - Network name
  - Network address
  - IP address
  - Domain name
  - Host name

6. What is the unique numerical label assigned to a device on the network that is used to direct data to and from the device?
- Network name
  - Network address
  - IP address
  - Domain name
  - Host name
7. What is the common, unique alphanumeric identifier assigned to a specific network and shared by all the devices that reside on that network?
- Network name
  - Network address
  - IP address
  - Domain name
  - Host name
8. What is the unique label assigned to a network resource that identifies the administrative authority to which that resource belongs?
- Network name
  - Network address
  - IP address
  - Domain name
  - Host name
9. What is the unique alphanumeric identifier assigned to a device on the network for the purpose of communication?
- Network name
  - Network address
  - IP address
  - Domain name
  - Host name
10. The Domain Name System uses a hierarchy to translate IP addresses into domain names.
- True
  - False
11. A subnet mask assigns a numerical version of an IP address to a portion of a network that shares a common address component.
- True
  - False
12. Which DNS record returns records used to verify the authenticity of a host?
- A
  - AAAA
  - CNAME
  - MX
  - SSHFP

13. Which DNS record returns the 128-bit IPv6 address associated with a host name?

- A
- AAAA
- CNAME
- MX
- SSHFP

14. Which DNS record specifies an alternate name at which a destination can be reached?

- A
- AAAA
- CNAME
- MX
- SSHFP

15. Which IP address class contains the addresses 128.0.0.0 through 191.255.255.255 and is typically reserved for use by ISPs or other large organizational networks?

- Class A
- Class B
- Class C
- Class D
- Class E

16. Which IP address class contains the addresses 224.0.0.0 through 239.255.255.255 and is typically reserved for multicast functionality only?

- Class A
- Class B
- Class C
- Class D
- Class E

17. Which TCP/IP command would you use to view the current network configuration and troubleshoot any issues with connectivity?

- PING
- TRACERT
- NETSTAT
- IPCONFIG
- ARP

18. Which TCP/IP command would you use to test the connection between devices on the network, to help you determine that the network is functioning properly?

- PING
- TRACERT
- NETSTAT
- IPCONFIG
- ARP

# TOPIC C

## Network Types

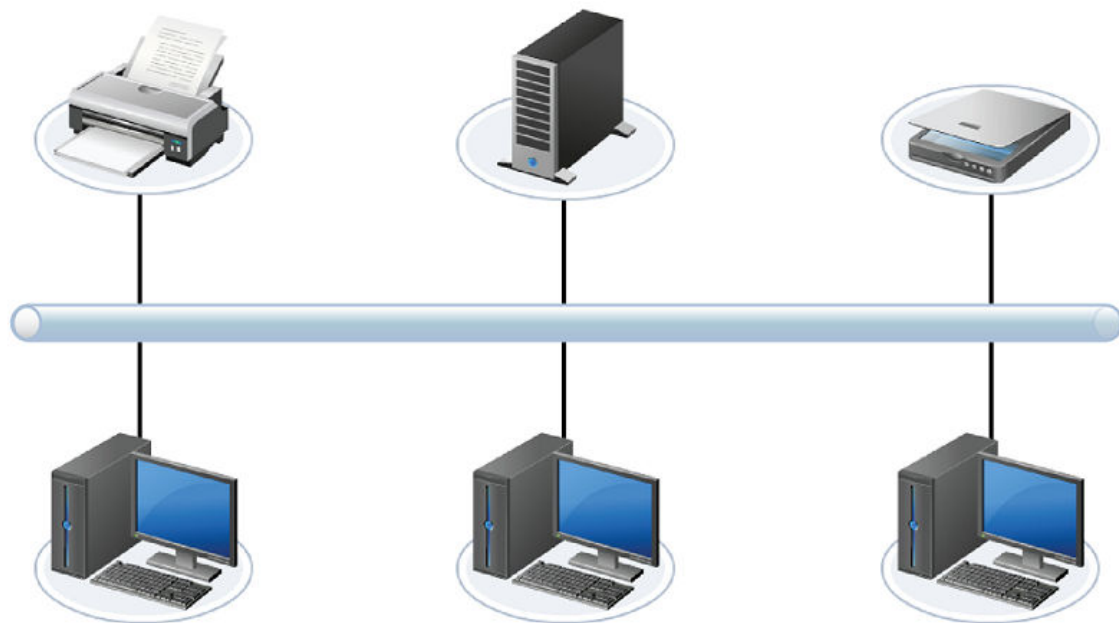
Like with just about everything in life, there are a number of different types of networks, and not all networks are created equal—nor are they all the best fit for your specific organization. As an MCO operator, you need to be familiar with the different kinds of networks, what makes them different, and which kind is best suited to your networking needs. In this topic, you will identify types of networks.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- LAN (Local Area Network)
- WAN (Wide Area Network)
- Internet
- Network coverage area
- BMN (Building Management Network)
- Special purpose network

## LANs

A *Local Area Network (LAN)* is a type of network in which a collection of interconnected devices in the same geographical (or “local”) location create a self-contained network. Most likely, it is the type of network that you are most familiar with and in contact with most often: the wireless network at your home is a LAN, the physical and wireless network at your workplace is also a LAN. One of the most important characteristics of a LAN is that it allows the sharing of common resources, such as a printer, file storage, or—most important in today's connected environments—a gateway to access the Internet.



**Figure 10–13: A LAN. (Source: Logical Operations for NCMCO)**

LANs primarily utilize wired and wireless Ethernet connections. Wireless LANs can be the easiest to implement, but can also be the most environment influenced: something as simple as introducing



a 5.8 GHz cordless phone system to the environment can greatly reduce performance. LANs can also be considered the building blocks of our Internet infrastructure, as they are the foundation on which all of our data consumption habits are built.

## WANs

A *Wide Area Network (WAN)* is a type of network formed by the connection of two or more LANs residing in different geographical locations and connected through a public network. The original concept of the WAN was for the sharing of data across long distances for research and development purposes—which it definitely does, considering that the largest WAN in the world is the *Internet*, which nearly the entire world's population accesses daily. And you access so many other WANs beyond that. Gaming online? You are utilizing a WAN. Accessing your corporate network through VPN to work from home? You are utilizing a WAN. Checking your social media content via a cellular device over a cellular network? Yes, you are utilizing WAN.

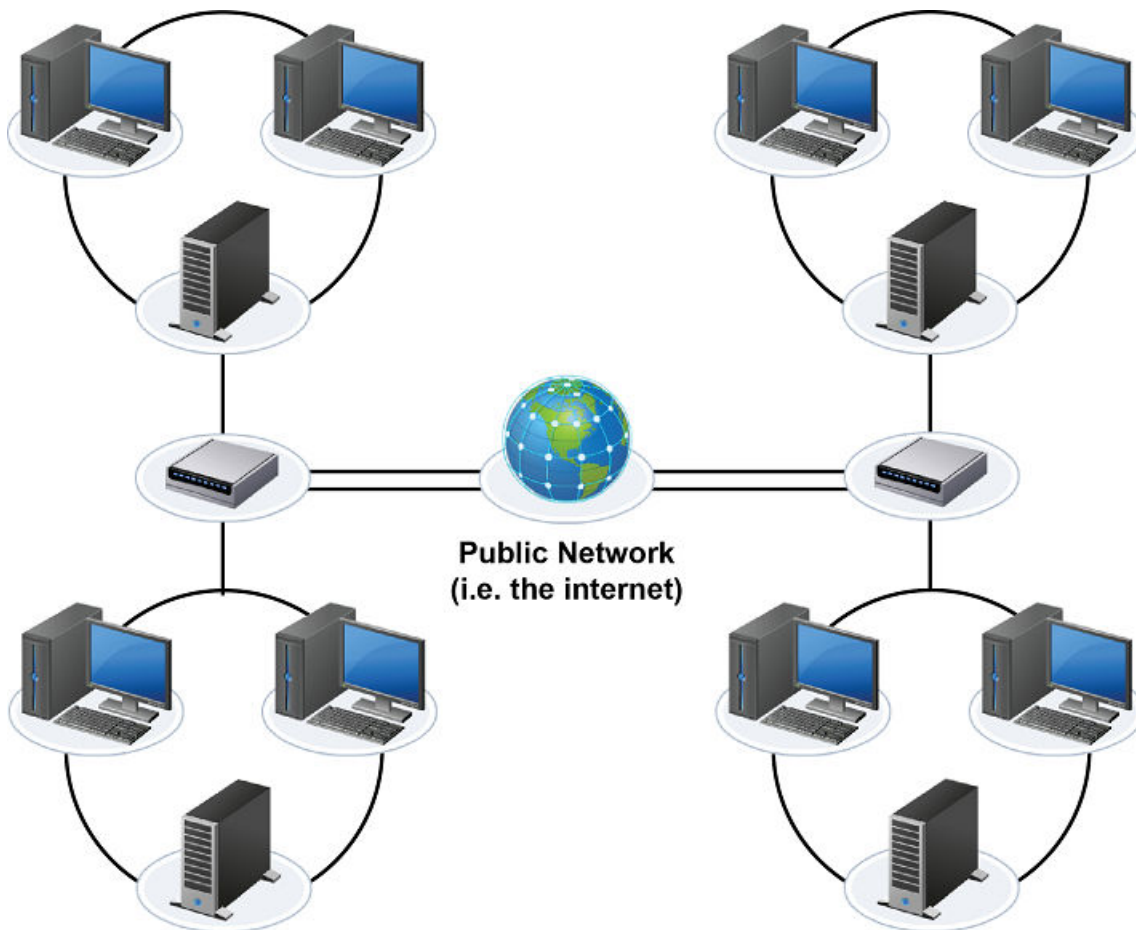


Figure 10-14: A WAN. (Source: Logical Operations for NCMCO)

## MANs, CANs, and PANs

There are a few other types of networks, mainly based on the geographical area that they cover.

Network Category	Description
MAN	A Metropolitan Area Network (MAN) covers an area that is equivalent to a city or a municipality.

<b>Network Category</b>	<b>Description</b>
CAN	A Campus Area Network (CAN) covers an area equivalent to an academic campus or business park. A CAN is typically owned or used exclusively by a specific organization or commercial entity.
PAN	A Personal Area Network (PAN) physically connects two or more computers using cables. A PAN is most often used in small or home offices.  A Wireless Personal Area Network (WPAN) is a variation of PAN that connects wireless devices in close proximity, typically via Infrared or Bluetooth® technologies.

## Network Coverage Areas

The *network coverage area* is the area within which a connection to a LAN or WAN can be obtained. This usually refers to the coverage provided by a wireless or cellular network, but it can also describe the area of access provided for nodes in a private network. Coverage area is governed primarily by the rules of signal strength, and is different depending on the network type (wired or wireless).

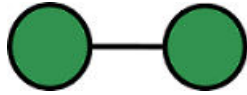
Here's a closer look at how the coverage areas of these two network types differ.

<b>Network Type</b>	<b>Coverage Area Description</b>
Wired	The hard-wired coverage area of a network is dependent on the length of cable media and the propagation of the signal. Traditional Ethernet cable runs are limited to a length of 100 meters, which is probably less than optimal if you have more distance to cover. To overcome this limitation, a signal propagator or repeater must be introduced. This is a device that receives the signal at the end of a cable run, reads the data, regenerates the data packets, and retransmits the data. This can also be done with a hub or a switch, and enables the transmission of data across vast local distances such as a school or business campus. Wired coverage may also be augmented by wireless gateway devices which allow signals to be transmitted without always having extensive—and expensive!—wired access points in place.
Wireless	In contrast to other network practices of placing core equipment on the lowest floor of a building, wireless coverage area benefits greatly from height. Wireless coverage is very dependent on “line of sight” parameters. This is the reason that cellular towers are located on the tops of buildings or on the highest clear geographical feature available. However, this becomes extremely difficult in population-dense areas such as cities and typically requires more wireless antennae to achieve the same amount of coverage that fewer may be able to achieve in a less populated area. Fortunately, advancements in wireless and cellular technology will continue to address the coverage issues, enabling more stable throughput regardless of location.

## Physical Network Topologies

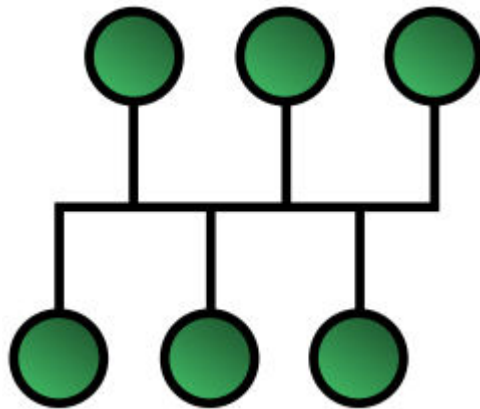
The physical topology of a network is the placement of networking devices to establish network connectivity and achieve the best possible performance and availability given the available components. There are five main types of physical network topologies.

Type	Description
Point-to-Point	The most simple, this type of physical topology establishes a direct connection between two nodes. There is no connection redundancy should the connection be severed.



(Source: Logical Operations for NCMCO)

Bus	This type of physical topology connects multiple nodes through a single, central cable. Should a single node lose connectivity, there is no impact to the connectivity of the other nodes. Unfortunately, if the connection fault occurs on the central cable, the entire network will be disabled.
-----	---

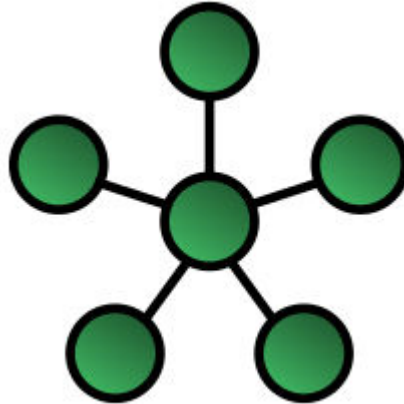


(Source: GW\_Simulations/Creative Commons (Public Domain)/<https://commons.wikimedia.org/wiki/File:BusNetwork.svg>)

Type	Description
------	-------------

Star

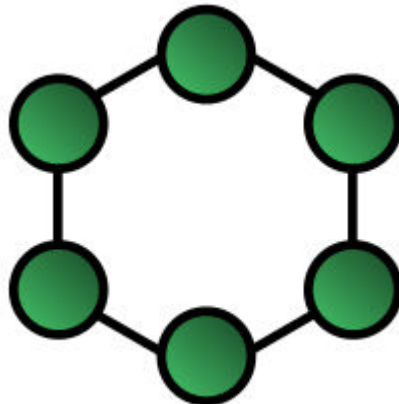
This type of physical topology connects all nodes independently through a centralized hub. An advantage to this topology is that individual node failures have no effect on the network's ability to transmit packets between remaining nodes. Unfortunately, the single failing point for this type of topology is the centralized hub; should the hub fail, all network traffic comes to a grinding halt.



(Source: GW\_Simulations/Creative Commons (Public Domain)/<https://commons.wikimedia.org/wiki/File:StarNetwork.svg>)

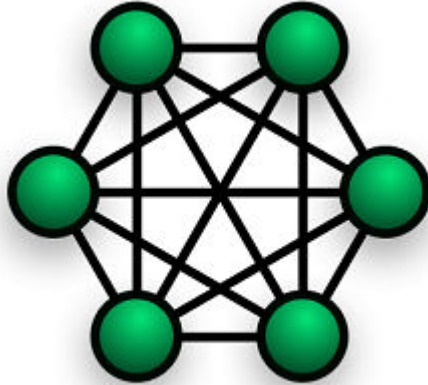
Ring

This type of physical topology connects all nodes in a closed loop. This bolsters signal fidelity as all packets sent are regenerated as they pass from node to node; however, a single break in the connection disables the entire network.



(Source: GW\_Simulations/Creative Commons (Public Domain)/<https://commons.wikimedia.org/wiki/File:RingNetwork.svg>)

<i>Type</i>	<i>Description</i>
Mesh	This type of physical topology requires that each node be connected directly to all other nodes within the network. This guarantees that node failures have zero impact on the fidelity of the network. However, this type of topology has a costly and complex implementation.



(Source: Foobaz/Creative Commons (Public Domain)/<https://commons.wikimedia.org/wiki/File:NetworkTopology-FullyConnected.png>)

## Logical Network Topologies

The logical topology of a network is the manner in which data is efficiently routed through a network. There are two logical network topologies that are most commonly implemented.

<i>Type</i>	<i>Description</i>
Bus	A node broadcasts data to the entire network, and all the other nodes receive the data at the same time. When the other nodes on the network receive the broadcasted data, they determine if it is meant for them.
Ring	Only one node at a time is allowed to transfer data to the network and data is transmitted downstream to each subsequent node. The transmitting node is identified by a token (which is in constant transmission around the network) and only the node holding the token can send data. Once the node has completed its transmission, the token is returned to the network for another node to retrieve and be allowed to transmit.

## Corporate Networks

Corporate networks, commonly known as intranets, are the LANs and WANs owned by a single organization. These networks are highly secure, and only accessible by the employees of the organization utilizing secure access methods. Access to these networks from an external network (such as from home) requires the establishment of a Virtual Private Network (VPN), which extends the private WAN of a corporation to an authorized device. Corporate networks allow for instantaneous dissemination of information, geographically unrestricted collaboration, and other connected activities that allow a corporation to be more agile and pragmatic when attempting to excel in many highly competitive markets.

## Building Management Networks

A *Building Management Network (BMN)* is the collection of inter-networked systems that manage automated processes necessary for the efficient utilization of building resources. A few of the most common BMNs that you are likely to interact with in your MCO facility include those used to control the HVAC, lighting, and building access systems.

<b>BMN</b>	<b>Description</b>
HVAC system	BMN is utilized to determine and maintain optimal temperature based on time of day. Advanced systems can even account for the number of staff onsite through different sensor arrays deployed throughout a building. These systems help to reduce a company's overhead by applying the available data to the resources and processes used to maintain a comfortable working environment.
Lighting system	BMN is commonly utilized to most efficiently light a building through a combination of timers and motion detection devices. This helps to prevent wasted electrical energy, prolong the life of lighting systems, and even contributes to less stress on the HVAC system through reduction of heat generated by unused lighting.
Building Access system	BMN, in conjunction with secure access system, is used to govern access to various areas in a building. This allows efficient management of secure assets and requires less workforce to enforce access restrictions. This type of network is used in many settings such as a school or a corporate building where isolation of non-authorized entities is a requirement.

## Special Purpose Networks

A *special purpose network* refers to a network on which a high-value data stream is isolated either physically (where there may be entirely separate LAN components) or logically (where certain network traffic is given higher priority) from the normal network traffic. The special purpose network can then be utilized for the delivery of data streams that are integral to the organization's performance and success. For example, a special purpose network could be implemented to prioritize and isolate the medical device data in a hospital from the traffic generated by patient's or visitor's personal devices; to isolate the data network utilized to control the automated functions in an automotive factory from other corporate data streams; or, even to isolate core data streams in a financial institution's mainframes.

There are a few specific types of special purpose networks that you are likely to encounter in an MCO facility.

<b>Special Purpose Network</b>	<b>Description and Purpose</b>
SCADA networks	<p>Supervisory Control and Data Acquisition (SCADA) networks are traditionally found in utilities management. They are used to manage constant action systems where performance data is needed to make determinations about current performance and any repair or reconfiguration needs. They are the real-time systems that allow for many of the abilities that are consistently overlooked: the ability to turn on a light or get clean drinking water from the tap. These seemingly rudimentary processes are actually managed by ever-evolving SCADA networks that keep our world running effortlessly.</p> <p>One of the biggest challenges for SCADA systems is that they often have to integrate with a legacy system, which introduces many challenges such as security vulnerabilities and limited data availability. This can be mitigated through the introduction of additional sensors and monitors meant to augment the legacy system.</p>
Fire System networks	<p>Fire System networks (FSNs) are the combination of hardware and software systems employed in a building for the purpose of detecting, preventing, addressing, and communicating a fire on the premises. Components of this system can be the temperature sensors, smoke detectors, sprinkler system, and the notification system connected to the local fire department for the purpose of providing an alert of a fire in progress. Depending on the complexity of the system, information such as the location of the fire, the number of floors or rooms affected, and the current sprinkler system status can give a responding fire department the data needed to form a succinct plan and potentially save lives.</p> <p>Fire System networks continue to evolve as new hardware and data acquisition systems are implemented. Additionally, the data being captured and actioned by FSNs even influences building design, as the ability to reduce the possibility of a fire and mitigate the damage possibly becomes more of a concern for building designers. This is especially true in areas where population density introduces new challenges and requirements for containment.</p>
PLC/DDC networks	<p>Programmable Logic Controller (PLC) and Direct Digital Control (DDC) networks are connected controllers that bring automation capabilities to large scale operations such as manufacturing or utility plants.</p> <p>PLCs were first introduced as actuators for various manufacturing systems and were constructed specifically for their intended environment (such as being hardened to dirt and grit in a manufacturing plant or even hardened against petroleum processing chemicals in a refinery). One major limitation of PLCs was the need to modify programming manually on each PLC based on changes in requirements. DDCs, the digital replacements for legacy PLC systems, overcome these limitations by making it possible to perform these changes at a macro level and disseminate them to individual units based on requirements. They can also be utilized with both digital and analog systems, providing real-time feedback and corresponding response.</p> <p>DDC and PLC systems are often integrated, with the simpler/less frequently modified functions controlled by a PLC and the more complex/frequently modified functions controlled by an inter-networked DDC system.</p>

# ACTIVITY 10–3

## Identifying Network Types

### Scenario

In this activity, you will identify network types.

---

- 1. Which type of physical network topology connects all nodes on the network to a centralized node acting as the hub?**
  - Point-to-Point
  - Bus
  - Star
  - Ring
  - Mesh
- 2. Which type of physical network topology connects all of the nodes within the network to each other to eliminate the impact of a single node failure?**
  - Point-to-Point
  - Bus
  - Star
  - Ring
  - Mesh
- 3. Which type of physical network topology connects multiple nodes through a single, central cable?**
  - Point-to-Point
  - Bus
  - Star
  - Ring
  - Mesh
- 4. Which type of logical network topology uses a token to permit only one node at a time to transfer data to the network, transmitting it downstream to each subsequent node?**
  - Point-to-Point
  - Bus
  - Star
  - Ring
  - Mesh
- 5. Which type of network is a collection of inter-networked systems that help manage automated processes to most efficiently utilize a facility's numerous resources?**
  - Local Area Network
  - Wide Area Network
  - Building Management Network
  - Special Purpose Network



**6. Which type of network is a collection of interconnected devices all residing within the same geographical location?**

- Local Area Network
- Wide Area Network
- Building Management Network
- Special Purpose Network

**7. Which type of network is used to isolate high-value data either physically or logically from the normal network traffic within a facility?**

- Local Area Network
- Wide Area Network
- Building Management Network
- Special Purpose Network

**8. Which type of network is a collection of two or more LANs that are geographically separated but connected through a public network?**

- Local Area Network
  - Wide Area Network
  - Building Management Network
  - Special Purpose Network
-

## Summary

In this lesson, you identified and applied networking fundamentals as they apply to a mission critical facility. As an MCO operator, you need to understand the basic concepts of networking, the common components that comprise a network, and the various types of networks that are available for implementation at your facility. Having a working knowledge of networking will help you select and configure the network that is best suited for your organization and all of its data-transferring needs, ensuring that all personnel can connect to and utilize the information that they need to keep your facility operating under optimal conditions.

# 11

# Communication Systems

## Lesson Objectives

In this lesson, you will identify and apply communication systems as they apply to a mission critical facility. You will:

- Identify wired communication systems and their components.
- Identify wireless communications systems and their components.

## Lesson Introduction

In any organization—regardless of size, scope, or purpose—an integral component is the communication system that allows people to exchange vital information with one another. This is especially true in a Mission Critical Operations (MCO) facility, where communication between various personnel and/or departments is important for safe, consistent day-to-day operations. With the constant evolution of communications technology, both wired and wireless communication systems are now widely available and, likely, both types will be implemented to some extent in your MCO facility.

As an MCO operator, you will need to be familiar with these different types of communication systems and how they function in order to ensure that there is always a mechanism for communication within your facility. In this lesson, you will identify and apply communication systems as they apply to a mission critical facility.

# TOPIC A

## Wired Systems

In this day and age, wired communications systems seem like a thing of the past. But there are still many wired implementations, especially in a business environment. Ever made a phone call to a peer or colleague, simply by calling an extension? Then you've used a wired communication system. As an MCO technician, you will need to have a broad understanding of these wired systems that you might encounter within your facility. In this topic, you will identify wired communication systems and their components.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- POTS (Plain Old Telephone System)
- PBX (Private Branch Exchange)

### POTS

*Plain Old Telephone System (POTS)* refers to the original approach to the communication of voice data over wired networks that prevailed throughout the twentieth century. This is the most basic approach to *telephony*—the construction, technology, and application of systems used for telephones and telephone networks—and is still in wide use throughout the world. POTS involves the transmission of voice data over a twisted pair of copper wires which creates the communication loop that carries the audio signals and a nominal current of 48V DC. Prior to the expansion of Internet services, you may recall that telephones did not require a power cord because they were partially powered by the wired communication connection itself.



**Figure 11-1:** A rotary phone operated using the Plain Old Telephone System transmission protocol. (Source: ProhibitOnions/Creative Commons (Public Domain)/<https://commons.wikimedia.org/wiki/File:WE500dialphone.jpg>)

## PBX

*Private Branch Exchange (PBX)* refers to the installation and operation of a hyper-local POTS network; very simply, the PBX is what allows you to simply dial an extension to reach someone else across campus without having to dial a full 7- or 10-digit phone number. Traditional PBXs have a limited geographic capability due to the need for direct wiring and an “in-house” switch that connects and directs the voice signals to the correct destination on the PBX network.

Modern telephony technology is working to create data-enabled PBXs that are connected via Ethernet cabling instead of traditional twisted-pair; however, the general network structure remains the same. Additionally, PBX switches can be connected to the Internet with VoIP technology, marrying remote PBX switches such that different geographies can interact as if they were in a single geographic location.

## ACTIVITY 11-1

# Identifying Wired Communication Systems and Their Components

### Scenario

In this activity, you will identify wired communication systems and their components.

---

1. **POTS utilizes a twisted pair of copper wires carrying the audio signals and a nominal current in order to transmit voice data.**
    - True
    - False
  2. **PBX is a hyper-local POTS network that allows for direct communications between extensions in geographically separated locations or over large distances.**
    - True
    - False
-

# TOPIC B

## Wireless Systems

As technology continues to advance, wireless communications systems continue to become more prevalent. On a daily basis, you are likely using multiple wireless platforms yourself in just a personal capacity: watching TV on a satellite broadcast, making calls or sending texts over your cellular network, and using your Wi-Fi to access the Internet; on a professional level, you are likely to encounter any or all of the types of wireless systems. Therefore, as an MCO operator, you should have a strong understanding of all of the available wireless communication systems and how they operate. In this topic, you will identify wireless communication systems and their components.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Radio systems
- Microwaves
- Satellite
- Cellular
- Wi-Fi

## Radio Systems

*Radio systems* are the original wireless communication platform. Radio waves operate at the lower end of the electromagnetic energy spectrum, and have wavelengths that can be measured in any increment from millimeters to miles. A particular voice or data signal is encoded via a variety of methods and transmitted at a particular frequency. Radio antennas (as the receiver) can be tuned to listen for a particular frequency and then catch and “decode” the signal being transmitted. Radio communications typically broadcast using broad, unfocused distribution patterns. However, regardless of the scale or complexity of radio communication systems, the process is as simple as tuning your stereo to the right channel (or frequency) to pick up the station you want to listen to.

Even today, traditional radio communication systems are still widely used—from local implementations such as onsite walkie-talkies to city-wide emergency personnel communications—largely because of their relative simplicity and the lack of necessity for large amounts of complex and expensive equipment.



**Figure 11–2:** A radio communications antenna. (Source: SRI International/Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:SRI\\_Dish\\_radio\\_antenna.jpg](https://commons.wikimedia.org/wiki/File:SRI_Dish_radio_antenna.jpg))

## Microwaves

*Microwaves* operate at the higher end of the electromagnetic spectrum, typically wavelengths of 1 millimeter to 1 meter, and at generally high frequencies. The principles of operation for microwave communications are essentially identical to radio systems, except for the actual equipment used to generate and receive microwave signals. A particular distinction between the two is that while radio signals generally have broad distribution patterns, microwaves have a more focused “beam” signal. From this perspective, it is easy to draw the correct conclusion that the same amount of power can send a microwave signal farther than a radio signal, since energy is saved by not transmitting in all directions. This also allows the “reuse” of particular frequencies in a given geographic area, since a particular signal is following a particular path.



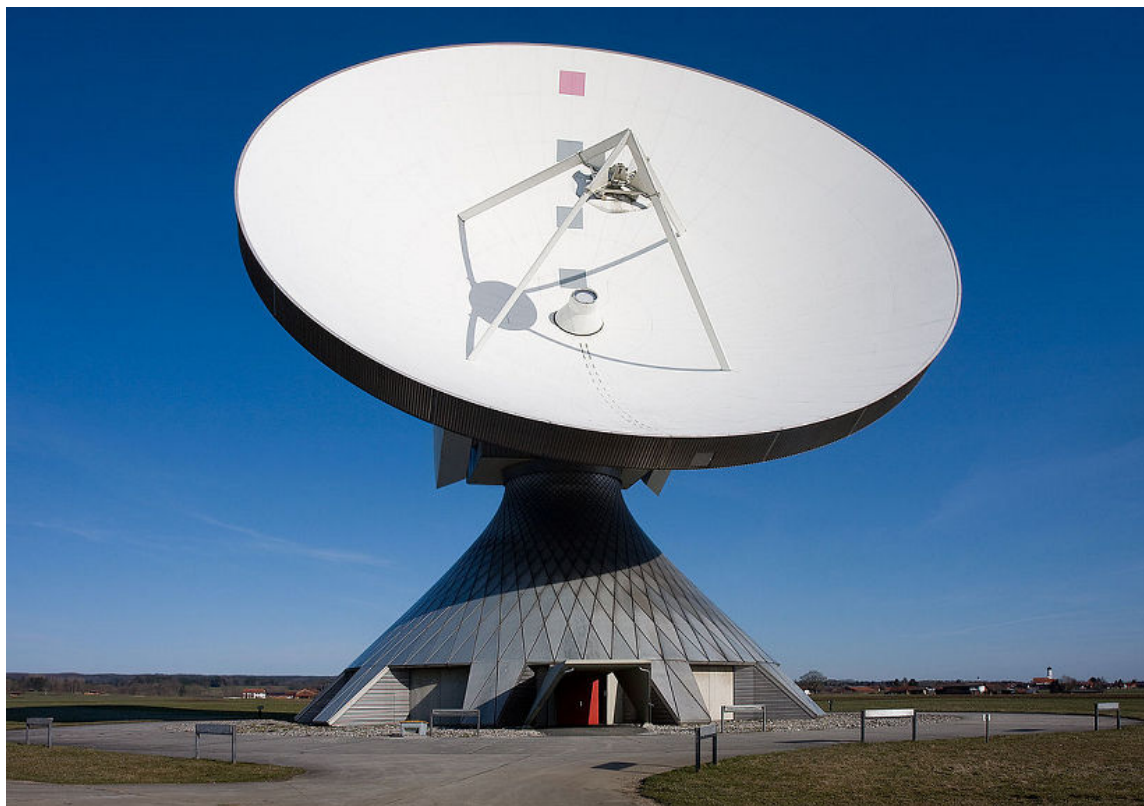


**Figure 11-3: A microwave communications antenna. (Source: Faisal Akram/Creative Commons (CC BY-SA 2.0)/[https://commons.wikimedia.org/wiki/File: Microwave\\_Antenna\\_\(2679399250\).jpg](https://commons.wikimedia.org/wiki/File: Microwave_Antenna_(2679399250).jpg))**

## Satellite

*Satellite* communication systems are unique because of their method of operation, not necessarily because of the signal types. Satellites are the “middle-men” in the system, repeating or reflecting the communication signal back down to Earth. This allows for communications across much larger distances since there is no need to worry about mountains, buildings, or other obstacles getting in the way. Most communications satellites are geosynchronous, which means they orbit the earth in a constant position relative to some point on the ground, such as always located 150 miles directly above New York City.

For example, a geo-stationary satellite directly above Denver, Colorado can be used to receive a signal from Kansas City, Missouri and send it to Seattle, Washington, eliminating the need for the transmission to cross the Rocky Mountains via wired networks. Additionally, if the simple triangular process of this example isn't enough to cross the desired distance, communications satellites can be linked to one another, passing the signal forward before sending it back down to Earth. In this second example, the Denver satellite can pass the signal to one over Anchorage, Alaska; then, over to Tokyo, Japan; and then back down to a ground-based receiver in Beijing, China.



**Figure 11–4:** A satellite communications antenna. (Source: Richard Bartz/Creative Commons (CC BY-SA 2.5)/[https://commons.wikimedia.org/wiki/File:Erdfunkstelle\\_Raisting\\_2.jpg](https://commons.wikimedia.org/wiki/File:Erdfunkstelle_Raisting_2.jpg))

## Cellular

*Cellular* networks are the communication systems we're all familiar with that transmit our voice data from mobile phones, and can be a combination of several different wireless technologies (although satellite use is generally cost prohibitive). Many series of cellular towers pass signals around to create a broad signal distribution network. The types of cellular technologies are varied and rapidly evolving, so the focus for MCO personnel is more on the propagation and reception of the signals.

While cellular network propagation is nearly ubiquitous these days due to the hundreds of thousands of cell towers throughout the U.S., the cellular signal is still a radio wave with limited abilities to pass through obstacles: hence the use of Distributed Antenna Systems (DAS) to propagate signals inside of structures that block most of the cell signals. Large MCO facilities are strong structures whose construction can interfere with radio wave dispersion, or even be designed to prevent it. The DAS solves this problem by working from an external antenna/receiver which is then (usually) wired to small antennas/receivers placed throughout the facility to provide signal coverage.



**Figure 11-5: A cellular communications tower. (Source: Ellin Beltz/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Cell\\_TowerTableBluffCA.JPG](https://commons.wikimedia.org/wiki/File:Cell_TowerTableBluffCA.JPG))**

## Wi-Fi

*Wireless Fidelity (Wi-Fi)* is the radio transmission system widely used today for high-speed Internet access and data transmission. It is what connects mobile devices, laptops, intelligent machines, and so forth to the otherwise wired communication networks, (such as the Internet, a Local Area Network (LAN), a Wide Area Network (WAN), etc.).

Where wired connections are still required, a wireless access point (AP) can act as the gateway to bridge the wired portions of the network to the wireless devices. Wireless AP devices function in the same manner as the large radio, microwave, or cell towers we see outside: the wireless AP connects to the wired network connection, creates its own unique wireless network and broadcasts a wireless signal for the wireless devices in the vicinity to connect to. Since they are software driven devices, they provide the ability to create security protocols of varying complexity; fairly simply speaking, it's the wireless AP device asking for your password when you sign onto a Wi-Fi network.



*Figure 11-6: A wireless access point creates a Wi-Fi network from a wired connection. (Source: Macic7/Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:Linksys\\_WAP54G.JPG](https://commons.wikimedia.org/wiki/File:Linksys_WAP54G.JPG))*

# ACTIVITY 11-2

## Identifying Wireless Communication Systems and Their Components

### Scenario

In this activity, you will identify wireless communication systems and their components.

1. Which type of wireless communication system utilizes antenna towers and, in prohibitive locations, Distributed Antenna Systems to transmit voice and data signals to mobile devices?
  - Radio
  - Microwave
  - Satellite
  - Cellular
  - Wi-Fi
2. Which type of wireless communication system transmits voice or data signals in a focused, beam pattern to their respective antennas, allowing for the reuse of certain frequencies in a given location?
  - Radio
  - Microwave
  - Satellite
  - Cellular
  - Wi-Fi
3. Which type of wireless communication system transmits voice or data signals in a broad, unfocused distribution pattern which are captured and decoded by their respective antennas?
  - Radio
  - Microwave
  - Satellite
  - Cellular
  - Wi-Fi
4. Which type of wireless communication system transmits voice or data signals to mobile devices from typically wired communications channels by creating its own unique broadcasting signal?
  - Radio
  - Microwave
  - Satellite
  - Cellular
  - Wi-Fi

5. Which type of wireless communication system transmits voice or data signals by reflecting and/or repeating the signal from a stationary device orbiting the Earth to its respective antenna on the ground?
- Radio
  - Microwave
  - Satellite
  - Cellular
  - Wi-Fi
-

## Summary

In this lesson, you identified and applied communication systems as they apply to a mission critical facility. As an MCO operator, you need to be aware of the various types of communication systems—both wired and wireless—and how they function in order to ensure that communication among personnel at your facility is always possible. With a fundamental understanding of these different types of communication systems, you will be able to configure and maintain a system that is constantly and consistently available, ensuring that all personnel can exchange the important information and data that they need to in order to keep your facility operating under optimal conditions.





# 12

# Environmental and System Monitoring

## Lesson Objectives

In this lesson, you will identify and apply industry best practices and standards for environmental and system monitoring within a mission critical facility. You will:

- Identify environmental parameters that can affect mission critical equipment and systems operations.
- Identify and apply best practices for metering system and equipment conditions.
- Identify the available monitoring platforms for various MCO systems.
- Identify and interpret system-specific outputs and reports.
- Identify control devices and their functions.

## Lesson Introduction

With all of the various components and systems that make up the larger Mission Critical Operations (MCO) infrastructure—the power systems, the HVAC and plumbing systems, the fire safety systems, the security systems, the networking and communication systems, and then the critical production spaces, too—it is essential that there are programs in place to monitor and track the current conditions of every single one to ensure that it is functioning properly, both individually and collectively. Regardless of the purpose, size, or scope of a facility, there are a number of environmental and system-related parameters that should be consistently monitored to track, analyze, and in some cases, automate the performance of the various critical components and systems throughout your MCO facility.

As an MCO technician, you will need to be familiar with these various system parameters, the programs or platforms that are used to gather the pertinent information from and/or about your systems, and what you can learn about the current operating conditions of your facility from the information that is provided. In this lesson, you will identify and apply industry best practices and standards for environmental and system monitoring within a mission critical facility.

# TOPIC A

## Systems and Equipment Parameters

Like any system, the various components and equipment within your MCO facility have certain conditions under which they will operate successfully and some that will prevent them from functioning properly. When it comes to keeping track of the overall conditions of your MCO facility, there are a number of parameters that need to be constantly monitored, in order to promote optimal working conditions and avoid those that could be a hindrance—if not hazardous—to your operations. As an MCO technician, you will need to know what these parameters are and how you should best monitor them to make sure that your facility is operating at its optimal conditions. In this topic, you will identify environmental parameters that can affect mission critical equipment and systems operations.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Corrosion

## Critical Production Environmental Conditions

As should be apparent by now, it's not just the operations of critical equipment that you need to constantly monitor and analyze as an MCO technician—the ambient production environment of your facility is equally important. It is a constant feedback loop wherein the ambient conditions affect the operating characteristics of the critical equipment, and the equipment affects the ambient conditions of the production spaces. In some cases, you simply want to keep the production environment within the confines of extreme upper and lower limits and in others, ambient conditions need to remain as steady as possible for the safe and efficient operations of the critical gear.

When it comes to the environmental conditions of your critical spaces, you should review some of the following parameters.

<i>Item</i>	<i>Description</i>
Static pressure	Static pressure refers to the “atmospheric” pressure within a space. Which is to say, outside of the direct influence of a particular component (a high pressure vent, for example), what is the standing pressure in the space? This is important to monitor because you often want to keep a slight positive or slight negative pressure in one space relative to another to control contaminants, for instance. MCO operators cannot evaluate this differential pressure without knowing the static pressure in each space.
Humidity	As you should know, humidity refers to the measurement of the moisture content of the air in a given space. The desired humidity will depend largely on the MCO environment and the activities that occur within the critical space. For instance, low humidity in a data center is dangerous because of the increased risk of electrostatic charge buildup, but is imperative in a biotech research facility since any moisture in the air might ruin testing material.

<i>Item</i>	<i>Description</i>
Temperature	Temperature is equally as variable as humidity in regards to the desired condition, but is one of the most common production environment variables measured in MCOs. While the precise operating range is particular to the application, MCO facilities tend to have large amounts of heat generating equipment, so being able to maintain control over the upper end of that range is a critical condition maintained by the HVAC systems.
Air flow	Air flow refers to the combined effects of temperature, humidity, and pressure since they are generally maintained as a group. There are additional ventilation requirements for occupancy, cleanliness, and contaminant concerns, but you also need to measure and understand air flow rates to help affect and control the changes in temperature, pressure, and humidity within the critical space.

## Water Flow and Associated Alarms

In regards to systems and equipment parameters, water flow refers to the intentional movement of water, whether that is for a chilled water system, process fluid system, humidification, general utility service, or so forth. Most MCO systems with notable volumes of water usage have flowmeters tied into the main supply at the very least, if not spread throughout the systems. Generally, these meters are used to track water consumption, often for environmental and efficiency analysis. When capable, facility teams will set these meters to alarm at either insufficient/no flow or excessive flow.

Insufficient/no flow indicates a blockage in the system somewhere or a leak upstream of the meter. Similarly, a meter that begins to register usage that is significantly higher than normal (this could be total volume or time-based measurement points) is another indication of a possible leak.



**Figure 12-1:** A flowmeter. (Source: Cmarcante/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:VORTEX\\_Montado\\_v1.JPG](https://commons.wikimedia.org/wiki/File:VORTEX_Montado_v1.JPG))

## Leak Detection

Leak detection monitors are separate from system flowmeters, and are most often seen as fluid sensitive cables run throughout floors, cable management wireways, or equipment pads. When water hits this cable, an alarm signal is sent back to the monitoring system, usually telling technicians at what “length” of the cable water is detected.

## Moisture Detection

Moisture detection is different than leak detection because it is more concerned with measuring for excessive humidity. Excess humidity crossing over the dew point could certainly cause condensation that would activate leak detection cables. However, some MCO production spaces require extremely dry conditions wherein excessive humidity in the air could ruin research samples or highly sensitive electronic components.

Moisture detectors take on many forms, but most take advantage of the conductivity of water. For instance, a wick can be used to absorb moisture from the air, across which a small voltage is applied to measure changes in resistance correlating to the measured moisture content.

## Hydrogen Concentration

You might recall from high school physics, or the previous discussions about battery systems, that hydrogen gas is a serious explosion hazard, so it is important to regularly monitor for H<sub>2</sub> concentration in MCO production spaces. Lead-acid batteries are a common source of hydrogen during charge and discharge cycles, but other manufacturing processes may create H<sub>2</sub> as a by-product. High H<sub>2</sub> levels may set off an alarm and/or automatically activate emergency exhaust systems. A common type of H<sub>2</sub> sensors use palladium coated components that absorb hydrogen molecules, which allows you to measure the quantity of palladium hydride that is created and then calculate the accompanying hydrogen levels.

## Battery Monitoring

Battery monitoring systems are fairly common throughout the infrastructure of most MCO sectors since emergency power is so important to reliability of our systems. Battery monitoring systems cover a wide array of complexity and intelligence, and are specific to the types of battery systems being used. Generally, battery monitoring systems have sensors wired to battery banks or individual cells that measure resistance, voltage, and other desired properties. These are used to both monitor steady-state standby conditions of the batteries, as well as track these electrical properties during charge/discharge activities.



**Figure 12–2:** A battery monitor. (Source: S.J. de Waard/Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:Amsterdam\\_RAI\\_METS\\_2011\\_\(138\).JPG](https://commons.wikimedia.org/wiki/File:Amsterdam_RAI_METS_2011_(138).JPG))

## Corrosion

*Corrosion*—the natural, gradual breakdown and destruction of materials caused by a chemical reaction within the environment, usually oxidization—is an ever present concern for MCO facilities inside and out. The main indoor concerns that can affect mission critical equipment are mainly the moisture and corrosives in the air, and the same holds true for outdoor equipment. Heat exchangers like chillers, condensers, and cooling towers are often at a higher level of risk since the associated energy transfers tend to exacerbate corrosion.



**Figure 12–3: Corrosion, in the form of rust, on a metal bolt. (Source: Thester11/Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:Rust\\_Bolt.JPG](https://commons.wikimedia.org/wiki/File:Rust_Bolt.JPG))**

The integrity of stationary, structural components is of noteworthy concern as well. To withstand the exposure to changing weather conditions, equipment enclosures like generator or utility houses should be made of corrosion-resistant materials, and pipes and valves should be properly insulated to the greatest extent possible to prevent unwanted moisture build-up.

## Corrosion Monitoring

There are really two options for corrosion monitoring: active and passive. Passive corrosion monitoring would refer to regular inspections of the integrity of equipment and structural components to identify and remediate any compromised areas. Active corrosion monitoring refers to devices that measure the corrosive conditions in the environment. Corrosion coupons are some of the more common devices, consisting of a strip of material that is particularly susceptible to a specific type of corrosion (there are many test options available) on which the amount and severity of corrosion can be monitored without having to access a comparable piece of installed equipment directly.

## Indoor Air Quality

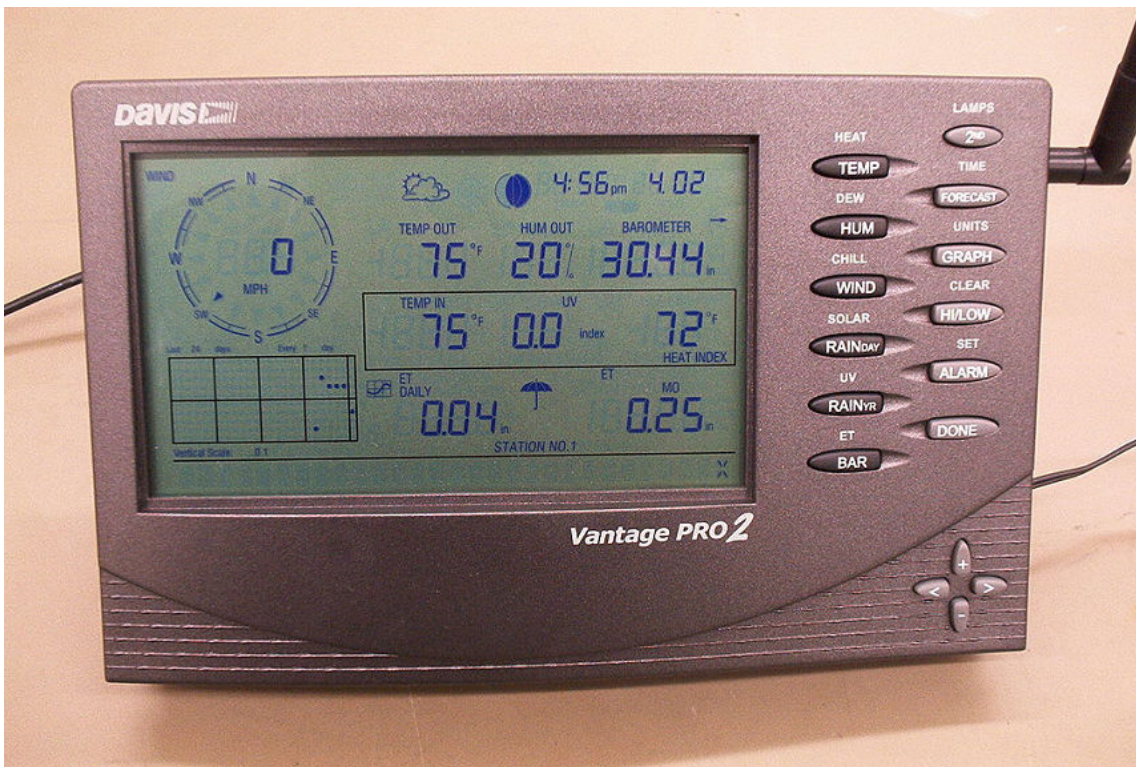
Indoor air quality (IAQ) has long been an HVAC engineering concern in commercial and industrial facilities, but the wide range of equipment operation in MCO facilities has introduced many different factors that affect the safety of personnel breathing the air (many of which have already been discussed, such as gas or other hazardous material leaks). Additionally, MCO production spaces may monitor for corrosives in the air that are minute or innocuous to humans, but can be very damaging to mission critical components. IAQ monitoring stations are often set up as a

combination of specific gas detectors (CO, CO<sub>2</sub>, H<sub>2</sub>S, etc.) and corrosion coupons that monitor for specific corrosives.

## Outdoor Ambient Environment

MCO systems, while heavily protected and isolated, are still susceptible to the effects of the outdoor ambient conditions—sometimes even more so *because* of their isolation. At a minimum, there needs to be some sort of fresh air makeup to the building for habitability, but in general, the facility relies on the outdoor conditions for much more, largely as the final heat transfer process for cooling systems.

Weather stations are devices mounted on the exterior of the building to provide real-time indication of outdoor environmental conditions such as temperature, humidity, barometric pressure, and a wide array of air quality values (such as the levels of corrosives, gas concentrations, and so on).



**Figure 12–4:** The receiver for a weather station, displaying the current outdoor ambient conditions. (Source: Michael L. Umbricht/Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:Weather\\_console.JPG](https://commons.wikimedia.org/wiki/File:Weather_console.JPG))

# ACTIVITY 12-1

## Identifying Systems and Equipment Parameters

### Scenario

In this activity, you will identify the systems and equipment parameters that should be monitored and maintained.

1. **When it comes to maintaining optimal HVAC operations in a critical production space, what important environmental conditions should you constantly monitor?**
  - Air flow
  - Air quality
  - Static pressure
  - Water quality
  - Temperature
  - Humidity
2. **Which type of detection system within a critical space monitors for the presence of excess water vapor within the facility?**
  - Water flow
  - Leak
  - Moisture
3. **Which type of detection system within a critical space uses specific types of metal components that chemically react to a variety of environmental parameters to alert you to the presence of certain undesirable conditions?**
  - Indoor air quality
  - Hydrogen concentration
  - Corrosion
  - Outdoor ambient environment
4. **Which type of detection system within a critical space monitors certain conditions including temperature, humidity, barometric pressure, and air quality in the spaces surrounding the facility?**
  - Outdoor ambient environment
  - Indoor air quality
  - Corrosion
  - Hydrogen concentration
5. **When it comes to monitoring the batteries in use within the critical production space, only the standby conditions of the batteries need to be tracked and recorded.**
  - True
  - False



6. Which type of detection system within a critical space monitors the presence of any fluids coming into contact with certain system equipment or components?
- Water flow
  - Leak
  - Moisture
7. Which type of detection system within a critical space monitors both the presence of gases and the presence of specific chemical reactions (like oxidization) to measure for conditions that are potentially hazardous to human respiration?
- Hydrogen concentration
  - Corrosion
  - Outdoor ambient environment
  - Indoor air quality
8. Which type of detection system within a critical space monitors the movement of fluids throughout the components within the facility?
- Water flow
  - Leak
  - Moisture
9. Which type of detection system within a critical space uses a specific type of metal-coated component that absorbs the gaseous substance being monitored, alerting you to its heightened presence in the space?
- Outdoor ambient environment
  - Indoor air quality
  - Corrosion
  - Hydrogen concentration
-

# TOPIC B

## Metering

In addition to the equipment parameters that should be monitored, there are a number of operational parameters that need to be monitored to ensure that there are always the proper resources available to keep those components running. As an MCO operator, you will likely be responsible for making sure that all of your mission critical components and systems are receiving the resources that they need to function and that they are utilizing those resources efficiently. In this topic, you will identify and apply best practices for metering system and equipment conditions.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Metering

## Metering

*Metering* refers to the measurement of available data points related to the performance of critical infrastructure systems and equipment. There are often thousands of points that you can measure and analyze trends for in an MCO facility, but it's simplest to think of metering in terms of how power, water, gas, and other resources are being used by the facility.



**Note:** The terms monitoring and metering are often used interchangeably, so it's easiest to use the term that is most commonly used throughout the industry for each specific system.

## Utility and Generator Power Metering

Main electrical power—either the source power provided by a utility or generated onsite—gets much of the attention in MCO metering, due to the rising costs and large amounts that are consumed. Main power meters in MCO facilities are just large, more robust versions of the power meters found on the side of your house, but usually have enhanced electronics to capture detailed information. In addition to measuring the total amount of power being drawn, these meters may capture and trend minimum, maximum, or average readings; sags and surges; or any other relevant events.



**Figure 12-5: Multiple power meters and switches on the exterior of a commercial building.**  
(Source: Ildar Sagdejev/Creative Commons (CC BY-SA 4.0)/[https://commons.wikimedia.org/wiki/File:2008-07-26\\_Electrical\\_meters\\_and\\_switches\\_in\\_Durham.jpg](https://commons.wikimedia.org/wiki/File:2008-07-26_Electrical_meters_and_switches_in_Durham.jpg))

## Branch Circuit Metering

Branch Circuit Power Monitoring (this is the more common term used for reference) refers to the metering that is performed one step down from the utility. This means that, at main distribution points throughout the facility—critical versus non-critical switchboards, transformers, different rooms, etc.—the overall power consumption to that area or system is metered. Since this still measures power consumption at relatively large loads, the meters used typically have the same capabilities as the main utility meters.

## Outlet Metering

Outlet metering refers to the measurement and trending of power consumed at the level where a specific piece of equipment, component, or device is connected. This could be where a machine is plugged in or throughout a power strip that the device is connected to, like in a data center where all the servers are plugged in. Decreasing costs of electronic components and the ease of network connectivity have strongly supported the increase in adoption and desirability of outlet level metering within the last decade. Due to the nature of the device, these meters are small and may have limited capabilities. In a manufacturing space, for instance, these meters may only log points periodically or provide a health status signal as opposed to the real-time, complex analytics provided by the intelligent power distribution units (PDUs) in a data center.



**Figure 12–6:** A plug-in power meter measures the amount of power being drawn by the connected appliance. (Source: Gareth.randall/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Plug-in\\_Power\\_%26\\_Energy\\_Monitor\\_in\\_UK\\_Domestic\\_Mains\\_Socket.jpeg](https://commons.wikimedia.org/wiki/File:Plug-in_Power_%26_Energy_Monitor_in_UK_Domestic_Mains_Socket.jpeg))

## Water Level Metering

Water still may not compete with power for total expense in most cases, but since there are many MCO applications that consume this resource, water level metering has become more common. Conserving water has also become a top priority for many eco-conscious organizations—many of which have detailed reporting requirements. There are a few common practices for monitoring water levels in an MCO facility.

Item	Description
Cooling tower basins	Cooling towers of the scale used in MCOs may use water at the volume that an entire neighborhood or small town might consume, so you can imagine why it is an important resource for MCO management to keep tabs on. Metering the water flowing through cooling towers and monitoring basin levels are absolutely necessary to be able to make smart decisions about improving efficiency. It's no longer enough to simply know how much water is being used or how often basins need to be re-filled. By metering these functions, water use can be analyzed and correlated to environmental conditions and facility operations, which helps pinpoint the factors that could be contributing to water waste.

<i>Item</i>	<i>Description</i>
Make-up water storage	The same holds true for general make-up water storage—if you can analyze and correlate changes in make-up water volumes (and thereby, usage) to specific activities, you can better understand when and how the systems it supports are consuming water. Intelligent devices monitoring make-up levels typically have enhanced capabilities that can alert MCO technicians to low water levels or high consumption rates before simply allowing the systems to refill; then, you can defer filling to periods of time where water utility rates are lower or the consumption has less of an impact on the community.
Water treatment and chemical levels	Municipal water supplies aren't always the desired purity or condition that MCO systems require, giving rise to the need for chemical treatments—another aspect that should be metered whenever possible. Connecting water quality meters to chemical storage levels and/or injection rates helps to fine tune the water treatment process and eliminate wasteful treating.

## Fuel Metering

Fuel metering largely brings to mind emergency generator fuel sources, but the same can hold true for other site-specific fuel types. If you run out of gas on the highway, you can call roadside assistance, but this is not an option for MCO facilities. Operators are always monitoring fuel supply volumes to make sure there is adequate availability of emergency power based on what was designed and planned, as well as monitoring fuel consumption rates (via flowmeters on the generators or between supply tanks during system utilization) to calculate and plan for any required fuel deliveries. Additionally, you should also perform real-time or periodic fuel quality monitoring to check the current conditions of the available fuel. For example, diesel fuel is susceptible to degradation, water accumulation from condensation, etc., when it remains stagnant; if it is sitting for long periods of time, waiting to be used as a fuel source for a backup system, it could degrade to the point that it is unusable, or worse, unsafe.

## Gas Metering

Previously, you looked at several types of gasses used in MCO systems, which are another set of resources important to measure and analyze. Many of these gasses are either not generated onsite or not continuously generated, so metering both stored volumes and pressures is just as important as metering the flowrate of these gasses as they are being delivered to the equipment using them. The most common types of gasses metered in MCOs include:

- Compressed air that is being used in maintenance equipment applications or equipment operations.
- Nitrogen that is being used for pressurization or storage purposes.
- Medical gasses that are being used in healthcare applications.
- Natural gas that is being used as a fuel and/or heat source.



**Figure 12–7: Pressure regulators and gauges installed on various compressed gas storage containers. (Source: Ildar Sagdejev/Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:2008-07-02\\_Pressure\\_regulators.jpg](https://commons.wikimedia.org/wiki/File:2008-07-02_Pressure_regulators.jpg))**

## Process Variables

Process variables refer to any aspect of the operation of facility infrastructure that measures how the equipment is performing its intended function, as well as other system-level conditions influencing operations. Mission critical infrastructure that performs a function beyond power and cooling, for instance, may not have specific measurements tied to their primary purpose; instead, you might need to use multiple process variables to get a feel for how well they are working. Technicians frequently meter or monitor system pressures and temperatures, differential pressures across system components, flowrates throughout the system, and so forth to build a holistic view of how the entire system functions.

# ACTIVITY 12-2

## Metering System and Equipment Conditions

### Scenario

In this activity, you will identify how to meter system and equipment conditions within a critical space.

1. **Metering refers to the measurement of how well the critical infrastructure equipment or systems are utilizing certain resources.**
  - True
  - False
2. **Which type of power metering measures the power being utilized at the point that it enters the facility for general consumption?**
  - Utility and generator metering
  - Branch circuit metering
  - Outlet metering
3. **Which type of power metering measures the power being utilized at the point at which specific components or devices are connected?**
  - Utility and generator metering
  - Branch circuit metering
  - Outlet metering
4. **Which type of power metering measures the power being utilized at the point where it is distributed for use around the facility?**
  - Utility and generator metering
  - Branch circuit metering
  - Outlet metering
5. **Water level metering should include monitoring which of the following levels or conditions?**
  - The amount of water flowing through cooling towers and water levels in basins.
  - The chemical levels of utility-provided water and the amount of treatment required to make it suitable for use in the facility.
  - The amount of wastewater being generated by and removed from the facility.
  - The amount of make-up water available in onsite storage tanks.
  - The pollution levels of waterways or bodies of water in proximity to the facility.

6. Which of the following actions should be performed to have an overall understanding of the state of the fuel sources stored onsite?
- Periodically check the fuel being stored to gauge its current conditions.
  - Monitor the amount of fuel delivered over the course of a given amount of time.
  - Keep track of the amount of fuel that has been used to plan for and schedule deliveries appropriately.
  - Periodically calculate the ratio of fuel on hand to fuel consumed for a given amount of time.
  - Monitor the amount of fuel on hand to ensure enough is available in an emergency.
7. Which of the following conditions should you monitor for the various types of gasses stored or used within your facility?
- Degradation
  - Volume
  - Temperature
  - Pressure
  - Flowrate
8. Process variables refers to the various data points that may need to be taken into consideration in order to measure how a specific component or even an entire system as a whole is functioning.
- True
  - False
-



# TOPIC C

## Monitoring Platforms

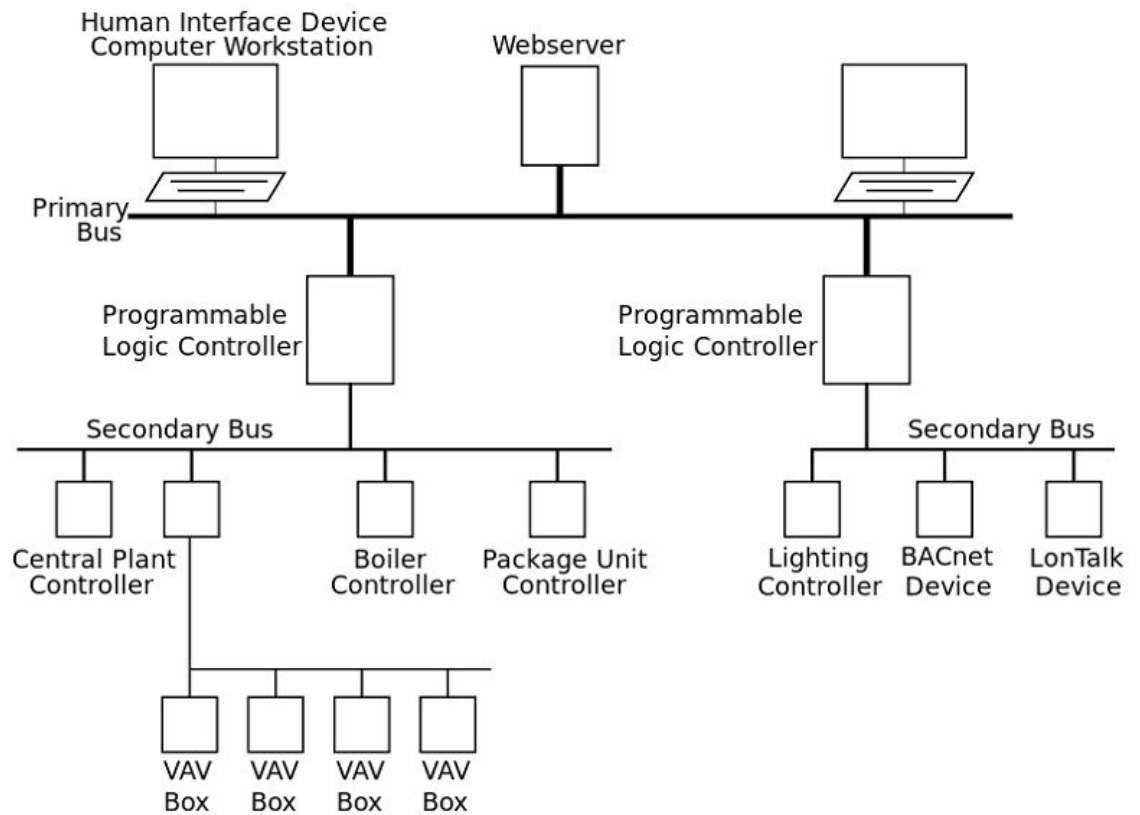
In any MCO facility, there are myriad systems functioning both separately and together that keep the facility up and running. To ensure these numerous components and systems are functioning properly, there are a number of monitoring platforms that can track, record, and in some cases, even control their day-to-day operations. As an MCO operator, you need to be aware of the platforms that are available and how they work to implement and/or maintain the option that best suits your facility's needs. In this topic, you will identify the available monitoring platforms for various MCO systems.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Building Management System (BMS)
- Building Automation System (BAS)
- Electrical Power Monitoring System (EPMS)
- Supervisory Control and Data Acquisition (SCADA)

### BMS/BAS

A *Building Management System (BMS)* or *Building Automation System (BAS)* is a computer-based monitoring system, typically comprised of both hardware and software, that monitors and controls the various critical systems or components, including HVAC, power, fire, and security. BMS/BAS monitoring can be classified into two broad categories, passive and active, mainly dependent on the MCO staffing. Passive monitoring refers to systems with information available about connected equipment, but is generally used in a “read-only” state, such as when an operator logs in. In most cases, these facilities do not have 24/7 technician staffing and alarms are set up for remote notification. Active monitoring refers to systems that are more fully utilized to provide live trending and analysis. These systems may have multiple displays presenting information all the time for operators to conduct real-time analysis and control system components to keep them fine-tuned.



**Figure 12–8: An example diagram of a BAS implementation.** (Source: Mat the w/Creative Commons (CC BY-SA 3.0)/<https://commons.wikimedia.org/wiki/File:RiserDiagram.svg>)

## EPMS

*Electrical Power Monitoring Systems (EPMS)* are commonly kept running in the background to monitor power quality and consumption at various system/component levels. Monitoring for and recording data about utility power supply events has traditionally been the greatest area of concern, but high-speed networking has shifted that focus. Now that so many components throughout an EPMS design can be network connected, MCO teams have access to live power consumption data at the equipment-level. Aside from monitoring operational trends (for instance, is a specific motor starting to draw too much current), EPMS helps determine and assign very precise costs to the operational expense of individual systems or equipment.

## SCADA Systems

*Supervisory Control and Data Acquisition (SCADA)* systems are used to monitor more complex processes, particularly with gear that doesn't necessarily all operate on the same platform. More “fixed” designs like data centers are easily connected to common BMS/EPMS systems, but critical manufacturing, R&D, and other MCO infrastructure tend to have more disparate, but interconnected components that require a more complex monitoring system like SCADA. SCADA systems collect as much operational data as possible from these disparate systems or components, and merge it into a single, aggregated means of display that allows you to have an overall view of how these various systems are operating as a whole.



*Figure 12–9: A SCADA system displays information for the various connected components. (Source: Sunilshamnur/Creative Commons (CC BY 3.0)/<https://commons.wikimedia.org/wiki/File:Chemengg.jpg>)*

## Equipment Level Monitoring

MCO systems are including more “intelligent” equipment that is capable of providing extensive data sets about their current operational conditions and making it widely available via network connections. The more data you have about specific equipment, the better you can track its health as well as calculate more precise operating costs. Even for those pieces of gear without advanced internal monitoring and analytical capabilities, other connected devices still provide a method for monitoring operations, including:

- Programmable Logic Controllers (PLCS) allow you to monitor the control functions in use and modify sequences of operation to improve efficiency.
- Human-Machine Interfaces (HMIs), which are typically graphical interfaces, allow you to operate the equipment and query data remotely.
- Meters, gauges, and relays (even as “old” analog devices) can be connected to provide basic data such as on/off or above/below setpoint.
- Local Control Systems—the individual, often proprietary control interfaces on specific equipment—can be connected to provide data on individual components.



**Note:** To further explore how to use the information provided from your integrated systems to better monitor your operations, you can view the **Use Integrated Systems to See the MCO Big Picture** presentation from the Certified Mission Critical Operator Video Series.

# ACTIVITY 12–3

## Monitoring Various MCO Systems

### Scenario

In this activity, you will identify the various monitoring platforms available to help keep track of your MCO systems.

---

1. Which monitoring platform would be best utilized to monitor the efficiency of specific electrical components operating within your MCO system?
    - BMS/BAS
    - EPMS
    - SCADA
  
  2. Which monitoring platform would be best utilized to monitor the efficiency of the various components and/or systems of your MCO facility to gain an understanding of how they are all operating as a whole?
    - BMS/BAS
    - EPMS
    - SCADA
  
  3. Which monitoring platform would be best utilized to monitor the efficiency of various components and systems of your MCO facility, and either passively or actively control them as needed?
    - BMS/BAS
    - EPMS
    - SCADA
-

# TOPIC D

## Outputs and Reports

System monitoring isn't just about collecting information about the current conditions of the systems or components within the larger MCO infrastructure—you need to be able to use the information that metering and monitoring platforms provide in smart, specific ways that allow your MCOs to operate at optimal conditions. The outputs and reports that certain systems provide to you can be used to track and analyze the past and current performance of critical components, and even predict how they will perform in the future under specific circumstances. As an MCO operator, you need to understand the information provided by the various systems in place within your facility and use this information to make informed decisions that will keep your facility running smoothly. In this topic, you will identify and interpret system-specific outputs and reports.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Normal state
- Abnormal state
- Trending
- Predictive results
- Dashboarding

### Normal States vs. Abnormal States

As complex and detailed as control and monitoring systems have become in MCO industries, the data is only “intelligent” if the mission critical operators at the helm can understand it. Fundamental to this understanding is the ability to differentiate between normal and abnormal states. A *normal state* refers to the regular or expected condition of the indication, whereas an *abnormal state* could really be anything else. Although it seems black and white at first glance, consider emergency equipment that might have an “engine not running” alarm: the normal state (presuming all primary systems are operational) of the engine running would cause the alarm to turn on; the abnormal state—engine off and emergency system running—would be noted by the *absence* of the alarm.



**Figure 12–10:** A console for a mass notification system displays a notification that the system is in a normal state. (Source: Gamewell-FCI (Bcarl)/[https://commons.wikimedia.org/wiki/File:Local\\_Operating\\_Console\\_\(LOC\).jpg](https://commons.wikimedia.org/wiki/File:Local_Operating_Console_(LOC).jpg))

## Alarm Conditions

Alarm conditions speak a little more broadly to the status of equipment and systems. True, this could reflect the binary view of the presence or absence of an actual alarm. However, capable operators know to work from all available indications, so you may observe systems in alarm conditions (where you can clearly see indications at or beyond critical thresholds) even if there are no alarms presented due to indicator failure, monitoring system issues, and so forth. In short, you should keep in mind what *characteristics* define alarm conditions for the equipment and shouldn't rely solely on a flashing red light or alert message to tell you that a component is operating outside of those parameters.

## Warning

Alarm conditions that have reached a level that indicates an initial concern are generally characterized as warning alarms/indications. In these cases, immediate response or automated action may not necessarily be required, but acts as a notification that the affected gear is outside of normal desired operating characteristics.

The warnings most likely to come to mind are those of systems approaching critical thresholds—where the equipment is outside of normal range of function, but not to the level where damage, injury, or downtime is imminent. In most cases, this means that there is time to evaluate other conditions and indications to determine the best course of action such as reducing load, shifting equipment lineups, preparing backup systems, and so forth.

While critical thresholds are generally quantitative measurements, warnings may also refer to more qualitative conditions that come from multiple indications. For instance, common warnings in mission critical equipment include approaching minimum or maximum load (for given equipment lineup) or equipment time out (conditions not being met for continued operation). In either of these scenarios, while a particular threshold may not be in jeopardy, the indications are pointing towards an undesired state of operation.

## Trouble

Trouble alarms/indications reflect an abnormal or undesired condition of the critical infrastructure. Trouble alarms can be very basic (such as the check engine light on your vehicle) indicating that maintenance is due or that a general diagnostic alarm has been initiated for the equipment. Because the equipment in MCO facilities is so diverse, these indications cover a very wide array of conditions. Additionally, the specific trouble condition may be unique or even proprietary to the equipment, so there may be times that you are only notified that a general trouble signal has been passed along to the controls and monitoring systems, not what the specific issue is.

The following are some common trouble alarms.

<b>Common Trouble Alarm</b>	<b>Description</b>
Equipment failure	Equipment failure refers to the trouble indication activated when a piece of equipment has experienced a fault that is jeopardizing or preventing safe and proper operation. In most cases, this means the equipment is secured from further operation without technician intervention.
Process shutdown	Process shutdown troubles are systemic and indicate faulted conditions preventing several pieces of equipment from working together to perform their intended function. For example, a critical manufacturing process where contamination has occurred somewhere in the line would likely shut down completely.

<b>Common Trouble Alarm</b>	<b>Description</b>
Network outage	A network outage trouble is increasingly common now that so many different pieces of equipment have network communication connections. This may mean the gear has lost communication with other parts of the system and/or you may have lost the ability to monitor and receive information from it. Some equipment might be designed to shut down upon a communications loss if independent operation could present a danger to operations or personnel.

## Trending

*Trending* refers to the collection of time-based data points that provide discrete measurements of operating characteristics of equipment throughout the mission critical infrastructure. By repeatedly recording the value of the same point over time, you can begin to get an overall picture of how the associated system is operating.

In the MCO industry, the term “trend” is used since so many of these points are not static and because what you are really looking for is how and when these points change. The rate and magnitude of change is vastly more accurate when you have as many data points as possible for a given period of time. If you only took a reading of a specific piece of equipment once a day for a given period of time, the values might be the same despite notable operational swings during that period.

When trending is set to record data at very short intervals (depending upon the application, this could be minutes, seconds, milliseconds, etc.), you begin to build a very accurate history correlating to points in time. When an event occurs, you can pull up trend logs for all sorts of related equipment; from this data, you can try to find what caused the fault and evaluate how other parts of the system responded at that time.

While modern MCO facilities tend to have advanced and highly detailed data collection, some of the most commonly trended operational characteristics are:

- Utility consumption
- Production levels
- Raw material consumption
- Water use or various other fluids consumption

## Predictive Results

*Predictive results* refers to a higher evolution of trending the data received from controls and monitoring platforms, in which current trends are closely analyzed in order to anticipate how the systems will behave or respond in the future. For example, an increase in resistance readings on electrical components may indicate an impending failure, allowing MCO teams to make controlled repairs *before* something breaks and interrupts operations. Predictive results also help you plan ahead for infrastructure needs; for instance, increasing operating loads may mean you need to bring additional equipment online before reaching the maximum operating limits of the existing equipment.

## Mitigating Risks and Failures

Trending and predictive analysis can be the quantitative tools for mitigating risks and failures in MCO installations. Merging this data with your own personal technical experience for the prudent planning of maintenance and repair activities is one of the best ways to mitigate risks and failures. A report can inform you that a critical component is starting to wear down, but not to what critical

level; your knowledge and experience, however, informs you that those parts have a long lead-time, so you should start planning the repair now.

Backup part inventory (or “critical spares”) is the collective stock of repair and/or replacement parts on-hand at the facility. You may choose to keep certain items in stock because they are frequently used, they have an acute cost related to their down time, they are hard to come by, or any combination thereof. Analyzing maintenance reports can provide a pretty clear picture of what breaks down or wears out and when, while predictive analysis of operational trends can indicate the likelihood of irregular failures.

Upgrading systems means very much the same thing for equipment or infrastructure as it does for technology systems. Sometimes the equipment wears out before the facility reaches the end of planned use; sometimes facilities or systems are used for longer than planned and components simply become outdated or obsolete. Regardless of the reason, by taking advantage of the information provided by your monitoring systems regarding the operating health or capacity of your critical infrastructure, you are better prepared to make informed decisions about when and how your facility will take on the daunting task of upgrading critical components. (Not to mention, financial managers are much happier with operations teams when you can plan in advance for such large expenditures!)

## Dashboarding

*Dashboarding* refers to the practice of compiling large amounts of operational data (often real-time) into concise text or graphical outputs that provide quick glances at the overall status of mission critical infrastructure and production. Dashboarding has become a buzzword across all mission critical sectors due to the lowering cost of obtaining and storing data, as well as the increased ease of access to multiple sources of information.

The screenshot displays the OPNsense web interface. The top navigation bar includes the OPNsense logo, the domain name 'OPNsense.localdomain', and links for 'Help' and 'Logout'. A left sidebar contains navigation icons for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is titled 'Lobby: Dashboard' and features an 'Add widget' button. Two primary widgets are visible:

- System Information:** A table providing details about the system's name, versions, updates, CPU type, uptime, current date/time, DNS server(s), and last configuration change.
- Interface List:** A table showing the status of network interfaces: WAN (DHCP), LAN (1000baseT <full-duplex>), WLAN (DHCP), and DMZ.

System Information	
Name	OPNsense.localdomain
Versions	OPNsense 15.1.9.1-amd64 FreeBSD 10.1-RELEASE-p9 OpenSSL 1.0.1m 19 Mar 2015
Updates	Unknown Click to check now
CPU Type	Intel(R) Atom(TM) CPU D510 @ 1.66GHz 4 CPUs: 1 package(s) x 2 core(s) x 2 HTT threads
Uptime	00 Hour 36 Minutes 03 Seconds
Current date/time	Thu Apr 16 13:56:45 UTC 2015
DNS server(s)	127.0.0.1
Last config change	Thu Apr 16 13:53:35 UTC 2015

Interface List		
WAN (DHCP)	autoselect	
LAN	1000baseT <full-duplex>	192.168.178.222
WLAN (DHCP)	autoselect	
DMZ	none	

**Figure 12–11:** A dashboard for a firewall distribution system shows various system states and performance snapshots. (Source: Miraclexix/Creative Commons (CC BY-SA 3.0)/<https://commons.wikimedia.org/wiki/>)



*File:Dashboard\_of\_the\_firewall\_distribution\_OPNsense\_15.1.png,\_displayed\_on\_a\_web\_page,\_viewed\_with\_a\_browser.png)*

## Effects of Local Failures on Other Mission Critical Systems

Local failures of environmental and system monitoring systems can have widespread effects on MCOs—to the point where a single sensor going bad can bring operations to a halt. This is just another of the myriad reasons why redundancy and reliability in design are so important.

Here are just a few examples of the effects that a local system failure could have on the larger mission critical system as a whole.

<i>Type of Failure</i>	<i>Effect on the Mission Critical System</i>
Control system failure	Control systems can suffer cascading faults throughout the larger system infrastructure; for instance, if a temperature sensor in a data center fails, cooling supply fans might halt (because they don't think there is a demand anymore), and IT equipment could overheat.
Monitoring system failure	Many monitoring systems are "daisy-chained" together, so that one panel is wired to another in succession until they get back to the main control device; a single bad power supply could cause a break in the communications and entire sections of monitoring panels could be dropped.
Supply chain disruption	In manufacturing installations, sensors monitoring for process quality control or ambient temperature near critical equipment could fail, causing the entire production line to shutdown as it reverts to safe mode.

## Case Study: Rackspace Data Center Outage

The unfortunate reality of any large-scale system, like the mission critical system, is that it is comprised of numerous other systems—any and all of which are not infallible. And if one of these local systems fails, it can have disastrous consequences on the mission critical system as a whole and, in some cases, on the people and processes that rely on those MCOs. One such unfortunate event occurred at the Dallas-based data center for Rackspace®, a global web hosting and cloud management firm that acts as the backbone for a large amount of Internet sites, including a few highly-accessed sites and fellow hosting companies such as Laughing Squid.

In mid-November of 2007, a truck hit the transformer that provided utility power to Rackspace's data center in Dallas-Fort Worth, which was home to the numerous servers that provided hosting capabilities for many of Rackspace's customers. Initially, power to the entire data center was disrupted, but emergency generators immediately kicked on to provide backup power for the facility and eventually power was transferred successfully to a secondary utility power system—all without any loss of service to its customers. However, two of the data center's chillers within the server space failed to start when secondary utility power was established, and temperatures in the data center already began to climb.

To make matters worse, the utility provider determined that it needed to shut off power to the facility entirely in order for emergency responders to have safe, unfettered access to the truck driver that had taken out the transformer in the first place. When the secondary utility power was disrupted, the chillers within the data center cycled again, and temperatures climbed even higher within the server space. Rather than let the servers fail on their own due to the rising temperatures, Rackspace manually took a number of its servers offline as a precautionary measure to prevent them from overheating which could potentially result in lost data, until the chillers could operate normally and/or power could be restored to the space.

Unfortunately, by taking the servers down as a precautionary measure, a number of its customers websites that were hosted on these servers were taken offline, as well. For a company such as

Laughing Squid, whose web hosting services were housed on Rackspace's servers, their hosting capabilities were taken down as well—resulting in a cascading effect of unintended downtime for many websites and disrupting access and operations for a multitude of end users.

All in all, the total outage time at the Dallas data center was only around 3 hours, but the outage affected not only Rackspace and its customers, but also its customers' clients. This data outage is a prime example of the effect that a local system failure can have on MCOs as a whole and, in this case, the effect that it can have on the people that rely on the stable, consistent operations of MCOs themselves—in this case, the customers that rely on Rackspace's data center and the services it provides.



## **The Role of Output and Reports in Preventative Maintenance**

When performing preventative maintenance on MCO equipment, it is important for the technician completing the work to review all available operational data, as well as capture test data from the equipment during the maintenance activity when possible. The output of these two, combined with any observations made during the work, should lead to a comprehensive maintenance report that is then provided to the MCO leadership team. This practice is one part of maintaining accurate and detailed material history for mission critical systems, as well as providing technical managers the information necessary to plan for repairs, replacements, and upgrades.

# ACTIVITY 12–5

## Interpreting and Applying Output and Report Data

### Scenario

In this activity, you will interpret and apply the output and report data received from MCO monitoring platforms.

---

1. **An abnormal state represents the condition that will always trigger an alarm notification.**
  - True
  - False
  
2. **A normal state is the usual and expected condition of a component, even if that condition is the absence of a specific characteristic.**
  - True
  - False
  
3. **Which type of alarm reflects that a component or system within the critical infrastructure has reached an abnormal or undesired condition?**
  - Caution
  - Trouble
  - Malfunction
  - Warning
  
4. **Which type of alarm reflects that a component or system within the critical infrastructure has reached a level indicating an initial concern?**
  - Malfunction
  - Caution
  - Trouble
  - Warning
  
5. **Which utilization of the outputs or reports from the monitoring systems in your MCOs allows you to determine a system baseline and confirm that any changes haven't negatively affected performance?**
  - Predictive results
  - Measurement and verification
  - Trending
  - Dashboarding

6. Which utilization of the outputs or reports from the monitoring systems in your MCOs allows you to compile all the data into a simple, visual view of how each component or the system as a whole is operating?
- Predictive results
  - Measurement and verification
  - Trending
  - Dashboarding
7. Which utilization of the outputs or reports from the monitoring systems in your MCOs allows you to create a history of performance data over distinct periods of time in order to track and analyze specific component or system usage?
- Predictive results
  - Measurement and verification
  - Trending
  - Dashboarding
8. Which utilization of the outputs or reports from the monitoring systems in your MCOs allows you to collect and analyze performance data to determine how a component or system will behave under specific conditions?
- Predictive results
  - Measurement and verification
  - Trending
  - Dashboarding
-

# TOPIC E

## Controls

Keeping track of the conditions within your MCO facility is only half of the story—you need to do something with the information you gain from the metering and monitoring platforms you have in place. Controls allow you to automate many of the functions within your facility, whether they are actions that need to be taken based on the system's current conditions or the actions that need to be taken in order to reach optimal operating conditions. As an MCO operator, you need to know what these control devices do in order to make sure they are implemented properly, so you can keep your components and systems operating at their best possible states. In this topic, you will identify control devices and their functions.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Set points

### Set Points

*Set points* are specific values used in control and monitoring to establish parameters within which infrastructure systems should operate. These values are programmed into the equipment or control programs, and should be accessible to MCO technicians to modify as you learn more about the behavior of your systems or need to make changes to accommodate facility needs.

Set points are commonly used within the controls system to:

- Determine high and low thresholds within which the equipment should operate to function optimally.
- Establish parameters for alarm notification if a specific condition or change in condition causes equipment to react.
- Identify trends by monitoring for a specific point or rate of change that consistently occurs or should occur given specific conditions.
- Generate triggers by establishing values that will be used to turn equipment on or off (or perform another specific activity or task) based on system needs.

### Set Point Adjustment

MCO operators should, with the proper training, have the ability to make set point adjustments. This could be caused by changes made to the equipment, or simply learning more about how the facility responds to other conditions. Adjustments should always be made in a controlled manner, the changes should be documented (including the original value, the new value, the date and time the change was made, and who made the change), and the expected response should be determined so you and other operators know whether or not to keep the adjustment in place.



**Figure 12–12:** A Proportional–Integral–Derivative (PID) Controller can be used to determine the difference between a process variable and a desired set point, in order to adjust it appropriately. (Source: Bitjungle/Creative Commons (CC BY-SA 4.0)/[https://commons.wikimedia.org/wiki/File:Industrial\\_PID\\_controllers\\_-\\_front\\_display.jpg](https://commons.wikimedia.org/wiki/File:Industrial_PID_controllers_-_front_display.jpg))

## Equipment Status

Even the most basic monitoring systems should provide information about the current status of the connected equipment. As large as MCO facilities tend to be, with hundreds or even thousands of working components, monitoring systems provide the platform for us to know the status of the infrastructure without physically laying eyes on the equipment. This allows a single operator to remotely keep tabs on the facility, eliminating the need for large teams to be stationed throughout the facility or conducting frequent tours.

Equipment statuses that are commonly used and that you are likely to encounter in your MCO systems and components include:

- On/Off
- Running/Standby
- Secured (or locked out)
- Alarm/Fault
- Mode of operation (such as speed, volume, setting, high/low, heat/cool, etc.)

## On/Off Schedules

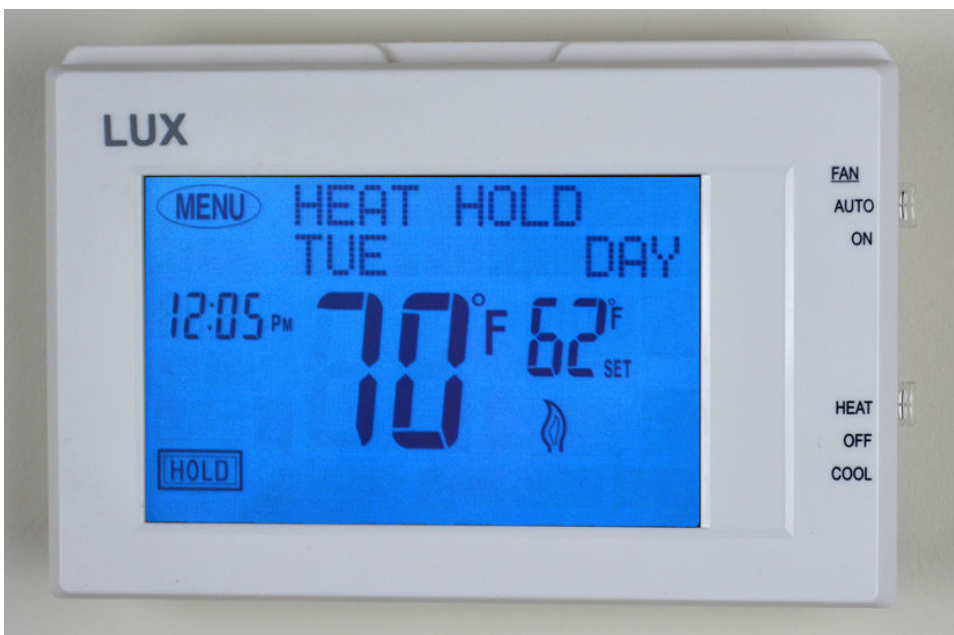
Another basic form of monitoring that helps provide efficiencies in terms of facility operations is controlling the infrastructure via automated on/off schedules. Traditionally, this is a time-bound control scheme that could be as basic as turning lights off when spaces are not scheduled to be occupied, or starting/stopping support equipment outside of production times. With the adoption



of more intelligent monitoring, automated on/off schedules can even be expanded based on environmental conditions. For example, space heaters can be programmed to come on only when the outdoor temperature drops below a specific set point.

## Alarm Thresholds and Reset

Alarm thresholds and resets refers to more dynamic monitoring points that are not necessarily binary in nature (such as an on/off schedule). Think of the threshold as the value that triggers an alarm or action, and the reset as a different value that must be achieved for the alarm to clear. This practice allows for more effective system operation, prevents alarms from going on and off rapidly, and avoids any subsequent equipment cycling. Take a common cooling function, for example: you want to keep a space below 75°F, so as that point crosses the 75°F threshold, a warning alarm is indicated on the building controls and an Air Handling Unit comes online. To prevent the system from bouncing around uncontrolled—which would be a waste of energy and resources—you could establish a 3° reset (or fixed reset of 72°F) to which the AHU will cool the space and at which point the alarm is cleared.



**Figure 12–13:** A thermostat can be set with a threshold at which to turn on and a reset at which to turn off. (Source: Dennis Murphy/Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:Lux\\_Products\\_TX9600TS\\_Thermostat.jpg](https://commons.wikimedia.org/wiki/File:Lux_Products_TX9600TS_Thermostat.jpg))

## Process Control Devices

Often, there are process control devices tied to environmental monitoring points in MCO facilities to correlate specific actions or reactions of the systems to particular conditions that trigger alarms. Process control is a broad concept used to classify any modification of the main system function; which is to say, these kinds of devices are used to tweak the system's operations, rather than to bring entire components of the infrastructure online or offline.

The following are some common process control devices.

Process Control Device	Description
Variable frequency/speed drives	Devices that incrementally change the speed of motors as conditions drift away from the desired parameters.

<b>Process Control Device</b>	<b>Description</b>
Thermostats	Temperature-sensing devices that provide input information to alarm functions and/or other process control devices.
Actuators	Mechanical devices that physically change a piece of equipment in response to a signal from another component (such as opening or closing dampers).
Variable air control	A set of devices that modulate air pressure in order to operate or position other equipment (for instance, to control actuators).
Control valves	A specific type of valve designed to throttle system flow based on desired performance criteria (as opposed to isolation valves designed to fully secure system components).

---

# ACTIVITY 12–6

## Identifying Control Devices and Their Functions

### Scenario

In this activity, you will identify control devices and their functions.

- 1. Which process control device modifies the air pressure within the system in order to physically alter other system components in a specific manner?**
  - Variable frequency/speed drive
  - Thermostat
  - Actuator
  - Variable air control
  - Control valve
- 2. Set points are used to establish the parameters within which your MCO components or systems should function and operate optimally.**
  - True
  - False
- 3. Which process control device responds to signals from another system component by physically altering a different component in a specific, requested manner?**
  - Variable frequency/speed drive
  - Thermostat
  - Actuator
  - Variable air control
  - Control valve
- 4. An on/off schedule utilizes two different set point values, such as a high temperature and low temperature, to establish when a device or component should turn on and off.**
  - True
  - False
- 5. Which process control device senses variations in temperature and sends that information to another system component that can then take action on the ambient conditions?**
  - Variable frequency/speed drive
  - Thermostat
  - Actuator
  - Variable air control
  - Control valve

6. Which process control device monitors and modifies the movement of motors in other system components if conditions slip away from optimal operating parameters?
- Variable frequency/speed drive
  - Thermostat
  - Actuator
  - Variable air control
  - Control valve
7. A threshold is a value that triggers an alarm or action, and a reset is a different value that must be achieved for the alarm to clear or the action to cease.
- True
  - False
8. Which process control device monitors and modifies the flow within the system if specific performance parameters are no longer being met?
- Variable frequency/speed drive
  - Thermostat
  - Actuator
  - Variable air control
  - Control valve
-

## Summary

In this lesson, you identified and applied industry best practices and standards for environmental and system monitoring within a mission critical facility. As an MCO operator, you need to be aware of the parameters under which your critical components and/or systems should operate—especially as they should optimally operate. With a strong understanding of these system conditions, you can then utilize the various metering and monitoring options available to gather and analyze vital information about how your systems are currently performing, and use this information to ensure that your MCO infrastructure is functioning under the best conditions possible.



# 13

# Operations and Procedures

## Lesson Objectives

In this lesson, you will identify and apply industry standards regarding operations and procedures within a mission critical facility. You will:

- Identify the typical elements of the organizational structure in a mission critical facility.
- Identify the typical operating procedures for a mission critical facility.
- Identify and apply best practices for managing change within a mission critical facility.
- Identify the regulatory bodies and standards within the MCO industry.

## Lesson Introduction

With so many different components and systems that make up Mission Critical Operations (MCOs) within a facility—and so many various organizations that are involved in MCOs in general—it is incredibly important that there is some consistency to the way that all these disparate elements operate. There are a number of different types of guiding principles and protocols that can be followed, both in the industry in general and within a specific institution, to promote an element of uniformity regarding the processes, procedures, and practices that are performed throughout the organization. These include certain organizational structures, operating procedures, and change management protocol that may be specific to a particular company, or the overarching standards, guidelines, and other best-practices that industry-specific regulatory bodies provide to create consistency amongst the various organizations.

As an MCO operator, you need to be very familiar with all of the various protocols that might have an impact on how your specific MCO facility operates, especially to ensure that your facility is functioning under optimal conditions and meeting industry expectations. In this lesson, you will identify and apply industry standards regarding operations and procedures within a mission critical facility.

# TOPIC A

## Organizational Structure

In any organization, there is always personnel of varying levels of expertise, responsibility, and skills; this naturally requires that some sort of structure or framework is in place to organize and manage everyone appropriately. In an MCO organization, this organizational structure is incredibly important to ensure that there is a clear understanding of who is responsible for certain actions, important tasks are completed in the proper order, and information is shared with the appropriate people. As an MCO operator, you need to have a strong understanding of the various elements that comprise the organizational structure, as you will be closely involved with the day-to-day operations that depend on this organizational hierarchy. In this topic, you will identify the typical elements of the organizational structure in a mission critical facility.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Chain of command
- Escalation path
- Organizational chart

### Chain of Command

In the organizational structure of any business or operation, the *chain of command* refers to the reporting relationship hierarchy. The chain of command is the avenue in which information and reporting is relayed and escalated from the upper levels of personnel to the lower, and from the lower to the upper.

Additionally, this chain of command structure establishes accountability at each level and determines proper authority and decision-making power within the structure. In a functional chain of command, direction is given from a higher level to an individual directly below them in a lower level position. At this point the lower position owns full responsibility for the directive, but may delegate the directive to a person lower in the chain. It is important to note that the directive may be delegated, but the overall responsibility is not transferable.

The organizational chain of command is necessary to determine clear lines of authority and responsibility while streamlining processes and improving communication within the organization. This "top down and bottom up" structure is a superb method to enable individuals to mature within various levels of the organization in preparation for future growth and potential advancements in leadership opportunities.

### Escalation Paths

The hierarchy laid out in the chain of command provides guidance about who to contact in the *escalation path*—the explicitly defined order in which information is passed, support is enlisted, approval is gained, etc., along the hierarchical levels of the organization. In most cases, the proper flow of escalation will resonate from a lower level in the hierarchy to a higher level in the proper sequence at each level of authority and position as determined by the organizational command structure. An authority level should not be skipped vertically in the process of an escalation unless deemed absolutely necessary by the person in possession of the escalation. There may be occasions when a level in the reporting chain is skipped in the escalation process, such as if the individual next in the reporting chain cannot be contacted or the nature or extreme gravity of the situation dictates a more rapid escalation process.



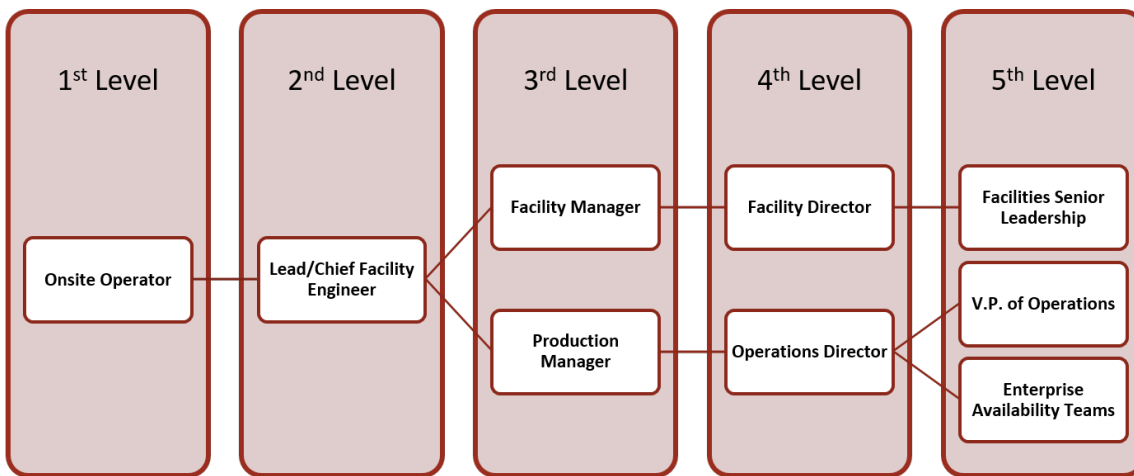


Figure 13-1: An example escalation path for a data center facility. (Source: Logical Operations for NCMCO)

## Organizational Charts

An *organizational chart* is a diagram that graphically depicts the chain of command and how one level of an organization relates to another, both vertically and horizontally. The organizational chart illustrates the levels of responsibility, the chain of command, and the proper escalation paths. Additionally, the diagram may convey relationships between CEOs, VPs, directors, managers, and other personnel in the organization; the relationship of one department to another; and/or the relationship of one function of the organization to another.

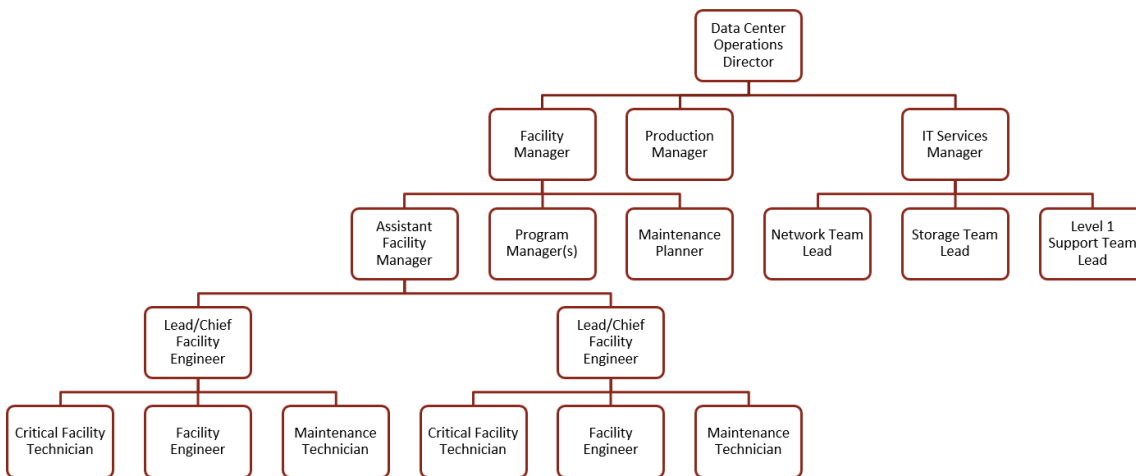


Figure 13-2: An example organizational chart for a Data Center. (Source: Logical Operations for NCMCO)

## Client and Contractor Relationships

Often, the success of organization depends on the relationship between the client and the contractor. A relationship must be established that is structured upon the principle that a partnership is developed with the common goal of ensuring that the client is able to reach goals and expectations as seen through the statement of work provided to the contractor. This partnership cannot be established without the presence of positive values demonstrated by the contractor, such as integrity, trust, fairness, and both quality and quantity of work.

Securing a contractor that can deliver superior results on time and per the statement of work is one of the highest priorities of a client. It is vitally important that this relationship is built upon the

principles of professionalism and sound business practices. A contractor who has this type of relationship with the client is able to effectively leverage the ability to provide their expertise and guidance, as well as to drive efficiencies within the businesses to potentially increase profitability of each.

## Vendor Management

As with client-contractor relations, it is vitally important that key professional relationships are established between key members of the organization and its vendors. Vendor management enables organizations to gain increased value by controlling costs, mitigating risk, supporting the statement of work, and driving service excellence.

On the organization's end, you should freely share as much information about the organizations as possible with your vendors to ensure they understand your business model and the priorities associated with your statement of work, as well as continue to provide the necessary information, in a timely manner, to help them properly support your needs. This communication will help gain the commitment from the vendor to support the business, as well as build that relationship and level of commitment from you.

When possible, MCO teams should attempt to build long-term partnerships (rather than short-term relationships) with the vendor. Constantly changing vendors to save a little money usually will cost more money in the long run and will surely impact quality and consistency of services. Additionally, long term relationships will help you understand their side of the business and this information may create opportunities to leverage the expertise of the vendor to further support your business needs.

# ACTIVITY 13-1

## Identifying the Elements of Organizational Structure

### Scenario

In this activity, you will identify the elements of organizational structure.

---

1. **When it comes to establishing relationships with your vendors, it makes more financial sense to focus on short-term relationships in order to shop around for the best vendor at the best price.**
    - True
    - False
  
  2. **Which element of organizational structure depicts the organization in a graphical format, detailing the hierarchy of relationships throughout the organization as a whole?**
    - Chain of command
    - Organizational chart
    - Escalation path
  
  3. **Which element of organizational structure details the hierarchical relationships within the organization, especially as it relates to sharing vital information with the appropriate personnel?**
    - Chain of command
    - Organizational chart
    - Escalation path
  
  4. **Which element of organizational structure details the order in which various actions should be initiated, advanced, and completed within the hierarchical structure of the organization?**
    - Chain of command
    - Organizational chart
    - Escalation path
-

# TOPIC B

## Operating Procedures

Just as there are organizational structures in place to provide a framework for understanding and managing the personnel hierarchy within an organization, there should also be a number of operating procedures established and utilized to ensure that tasks and operations are performed within a consistent, unified plan. These operating procedures range from those followed for day-to-day operations, to those that should be followed when maintaining or repairing critical components, to those that should be followed in the event of an emergency. As an MCO operator, you need to be aware of each type of operating procedure that you are likely to encounter in your MCO facility, since you will likely be responsible for creating, enforcing, and following many of them. In this topic, you will identify the typical operating procedures for a mission critical facility.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- SOP (standard operating procedure)
- EOP (emergency operating procedure)

### SOP

A *standard operating procedure (SOP)* is an established procedure that has been created to solidify a precise way of conducting a task or operation in order to achieve a predictable, desirable result. It is a proven procedure that provides step-by-step directions to accomplish the task or operation, through its entirety, in accordance with industry regulations, provincial laws, and business standards or regulations. SOPs are associated with tasks that are commonly or routinely performed and are, therefore, subject to continuous scrutiny, review, and if needed, updating.

The intent of a standard operating procedure is to establish a method to ensure that a task is performed consistently and in a uniformed manner. This will drive increased efficiency of operations, higher reliability, low error rate, and task consistency while improving risk management and operational predictability. For this reason, they are most often designed to handle the operation or alignment of equipment and systems, where consistency and predictability is key to optimal performance.



**Figure 13–3:** An engineer follows standard operating procedure for recording data for a critical infrastructure component at a materials plant. (Source: Huntstock/Thinkstock)

## EOP

An *emergency operating procedure (EOP)* is designed similarly to a standard operating procedure, but it is a plan comprised of specific actions to be conducted in a particular order and manner in response to an emergency event or situation. EOPs are designed with steps that should be followed sequentially in an effort to stabilize the emergency situation. Once the emergency is stabilized, additional action or repair can be accomplished in a more controlled environment utilizing a maintenance or repair procedure to return systems or equipment to a normal operational configuration.

Since it is not likely that emergency operating procedures would be utilized on a frequent basis, it is vitally important that these procedures are thoroughly reviewed on a regular basis. Additionally, these procedures should be walked through and drilled frequently to ensure they are accurate and users of the procedure can respond without hesitation and with high efficiency.

Often, developing and implementing EOPs is mandatory, and some organizations may even be obligated to do so under statutory or regulatory requirements.



**Figure 13-4:** Firefighters responding to an emergency involving hazardous materials follow emergency operating procedures, such as wearing the required PPE. (Source: Huntstock/Thinkstock)

## Other Procedures

In addition to standard and emergency operating procedures, other procedures may be developed to standardize processes, create greater efficiency, enable higher reliability, and increase predictability. These procedures can range from the general administrative “how to” procedures, to very complex and detailed procedures that must be accomplished in a specific sequence.

The following are some other procedures.

<b>Type of Procedure</b>	<b>Description</b>
Maintenance	Maintenance procedures typically refer to the required inspection and maintenance of critical equipment in order to ensure that these actions are performed as per operation/equipment manuals and manufacturer recommendations. They are often developed from original operating equipment manuals and standard maintenance practices. Preventative maintenance is commonly performed under a maintenance procedure to ensure that equipment is maintained to particular specifications and so each piece of the same equipment is maintained at the same level of quality and thoroughness.

<i>Type of Procedure</i>	<i>Description</i>
Repair	Repair procedures are utilized for corrective maintenance upon the failure or malfunction of a piece of equipment or system. They may be developed in a matrix or chart format, allowing the technician to match the failure description with the potential corrective action, which would consist of a procedure to follow to troubleshoot and repair the failed item. Other repair procedures may be more specific to equipment or systems that may fail frequently, in which case the repair will consist of specific steps to take and will be relatively routine in nature.
Commissioning and Recommissioning	When a piece of equipment or system is commissioned or recommissioned, there are specific procedures that must be followed to ensure that all components and associated systems are designed, installed, tested, operated, and maintained in accordance with the manufacturer, client, or owner specifications. Commissioning and recommissioning procedures are developed at the time of commissioning to capture the information needed to operate and maintain the equipment for the remaining service life of the equipment or system. Many times these commissioning procedures are developed utilizing the manufacturer operations manuals, and modifications are documented to reflect the specific and unique sequences or operation factors of the installed equipment.



**Note:** Maintenance and repair procedures may also refer to or encompass SOPs (such as securing equipment or shifting specific systems) in order to make sure that the repairs are performed in the same standard manner.

# ACTIVITY 13–2

## Identifying Operating Procedures

### Scenario

In this activity, you will identify types of operating procedures.

---

- 1. Which type of operating procedure should be followed when performing a typical day-to-day task that requires a specific and desired outcome based on industry best practices or manufacturer's recommendation?**
  - Standard operating procedure
  - Emergency operating procedure
  - Maintenance procedure
  - Repair procedure
  - Commissioning/recommissioning procedure
- 2. Which type of operating procedure should be followed when introducing new or removing old components within established systems in your MCO facility?**
  - Standard operating procedure
  - Emergency operating procedure
  - Maintenance procedure
  - Repair procedure
  - Commissioning/recommissioning procedure
- 3. Which type of operating procedure should be followed when a component within your MCO system needs to be cleaned and inspected per the manufacturer's suggestions in the operation manual?**
  - Standard operating procedure
  - Emergency operating procedure
  - Maintenance procedure
  - Repair procedure
  - Commissioning/recommissioning procedure
- 4. Which type of operating procedure should be followed when an unforeseen event occurs that disrupts or interrupts the normal day-to-day operations of the components or systems within your MCO facility?**
  - Standard operating procedure
  - Emergency operating procedure
  - Maintenance procedure
  - Repair procedure
  - Commissioning/recommissioning procedure



5. Which type of operating procedure should be followed when a component within your MCO system has malfunctioned and needs to be restored to operational conditions?

- Standard operating procedure
  - Emergency operating procedure
  - Maintenance procedure
  - Repair procedure
  - Commissioning/recommissioning procedure
-

# TOPIC C

## Change Management

In any organization, there are standard operating procedures and processes for a very specific reason: to keep the day-to-day operations of critical activities as unified and consistent as possible. It stands to reason, then, that any changes made to a standard set of procedures should be made with as much consideration and oversight. When it comes to making any changes or performing any change-related tasks, there are a number of best practices that should be followed to make sure that they are being made in ways that will have the least amount of impact on the people, processes, and ongoing operations of the MCO facility. As an MCO operator, you will often be the one performing or overseeing these changes, and it is incredibly important that you understand the various parameters guiding proper change management techniques. In this topic, you will identify and apply best practices for managing change within a mission critical facility.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Blackout date
- Maintenance window
- Cutover window
- Permit to work
- Hot work permit
- Energized work
- Off-hours work
- Scheduled shutdown
- Double custody switching

## Restricted Change Periods/Blackout Dates

Restricted change periods, more commonly referred to as *blackout dates* (or, for longer or extended periods of time, freeze periods), refer to any periods of time when making changes to systems or processes would have too great of an impact on important or time-sensitive operations and, therefore, implementing any changes should be avoided during this time. While MCO operators always need to be cognizant of the needs, plans, and expectations for system changes, any non-emergency alterations, modifications, or risky operations should not take place during these time periods, because the effects of interruptions or downtime would likely be catastrophic if not irreparable. Some examples of organizational activities that might result in a restricted change period include:

- End of year financial processing
- The handling or transferring of sensitive materials
- High-volume operational activity such as data storage, hosting services, or communications

## Maintenance Windows

A *maintenance window* is a pre-established period of time during which change-controlled work is regularly allowed to take place. Based upon the core MCO functions of the facility, there are usually periods of time during which interruptions—although still never desired—may not have a serious impact on business continuity. Regular preventative maintenance activities affecting redundancy and reliability (taking a UPS offline for annual maintenance, load-bank testing generators, etc.) generally will not require quite as much scrutiny and levels of approval to take place during these maintenance windows.

For instance, domestic wireless/communications firms recognize off-peak traffic volumes during the middle of the night when most of the country is asleep and not using their cell phones. Downtime experienced at their data centers or switch locations during these acceptable maintenance windows would certainly still impact end-users, but at much smaller magnitudes than, say, during the middle of a Saturday during college football season.

## Cutover Windows

A *cutover window*, sometimes also referred to as a switching window, is a planned period of time during which there is a transition between using an old system or component and using the new system or component that is replacing it. Typically, there will be a plan in place for how long both systems or components (if possible) will be operating concurrently to make sure the new one is working properly, and a cutoff date after which the old system will no longer be functional. Like with other change-controlled tasks, the plan and the changes made to the relevant systems should be well-documented for any future use.

## Permits to Work and End-User Approval

Work that might be hazardous or that poses a specific threat to normal business operations often requires special permission and/or end-user approval. A *permit to work* is used in situations when the work is potentially dangerous to those performing it, and is a formal, written document that specifies the work to be done, the equipment and personnel involved, the potential hazards that the work poses, and the precautions that should be taken while work is being performed. The permit to work must be authorized by the appropriate higher-level personnel before work can commence.

The facility manager at an MCO location is often the approval authority for the majority of work, but if the change or maintenance activity directly impacts important core processes, critical servers, or other sensitive equipment, established protocol may involve sign-off by senior leadership responsible for these functions. It is not uncommon for these leaders to be unfamiliar with mission critical facility infrastructure, so the better an operator or technician can explain the work, and the more robust the procedures in place, the more at ease we can put the end-user.

## Hot Work Permits

A *hot work permit* is a work permit specific to repair or maintenance activities that involve open flames, create sparks, or otherwise introduce acute fire hazards, such as welding or soldering. The permit will identify the specific work activity, location, date and time, duration, involved equipment and personnel, the responsible party, and required fire protection actions. Similar to the other change management processes already discussed, hot work permits may also need to be counter-signed by senior leadership or end-user representatives.



*Figure 13–5: Welding work within the MCO facility requires a hot work permit. (Source: Library of Congress/Creative Commons (Public Domain)/<https://commons.wikimedia.org/wiki/File:AlfredPalmerwelder1.jpg>)*

## Energized Work

*Energized work* refers specifically to repair and maintenance activities that involve electrical work on circuits that cannot be fully de-energized. Many organizations have policies that expressly forbid energized electrical work, no exceptions. Sometimes energized work cannot be avoided without taking down critical operations, which is particularly true in legacy facilities that have infrastructure pre-dating more robust designs. If this is the case, extreme precautions will be taken to isolate as much power as possible, and will usually require working with electrical contractors specializing in this particular work, since even the most highly trained facility technicians don't encounter energized work often enough to be prudent.



**Figure 13-6:** An engineer prepares to shut off power to energized equipment in order to perform necessary change-related work. (Source: ndoeljindoel/iStock/Thinkstock)

## Off-Hours Work

*Off-hours work* refers to a variant of the maintenance window philosophy, but not quite as structured. It may simply mean performing work outside of core facility working hours when more people are working throughout the facility, or anytime throughout the weekend, or scheduling during/away from holidays, for example. Whereas maintenance windows are firmly pre-established and to some extent pre-approved, the notion of off-hours work remains flexible relevant to a particular situation.

## Scheduled Shutdowns

A *scheduled shutdown* can be thought of as a highly pre-planned, extended maintenance window. Some activities, such as switchgear maintenance, refueling activities, or large installations/decommissioning are of critical concern in regards to change management, but simply cannot be performed during a single maintenance window or even back-to-back maintenance windows. In planning for these shutdowns, which may last days or even weeks, organizations may shift core operations to other facilities or business units or simply suspend operations temporarily. Work during scheduled shutdowns is generally done around-the-clock in order to maximize the amount of work that can be accomplished in the limited time available.

## Double Custody Switching

*Double custody switching*, also known as the two-person rule, refers to the practice of mandating that two trained operators are involved in any work done to major or high-energy equipment or switchgear breakers. In this setup, one person is designated as the reader of the procedure and charged with verifying the gear as it is operated, while the other person is focused solely on the safe

operation of the gear. It is not uncommon that both operators be outfitted in the same level of Personal Protective Equipment (PPE). Many programs with strict process-driven philosophies may require the practice for all maintenance activities.



**Figure 13–7:** Two linemen follow the double custody switching protocol while performing maintenance on a power line. (Source: rpernell/iStock/Thinkstock)

## Maintenance Schedule Changes

Any changes to an existing maintenance schedule should only be done with proper approval and in coordination with the appropriate parties that have broad visibility to all facility operations. Large installations have a lot of work to be done on a regular basis that requires careful planning, with little or no wiggle room to accommodate getting out of sync. You may be working an off-shift and feel you want to work on a side project instead of assigned maintenance this week, but making that decision on your own might interfere with work you are not aware of, to which your assigned task might be a pre-requisite.

## Procedure Change Methods

Every organization may have a different format for writing procedures and planning for change-controlled work, but even without industry-wide standards in place, there is broad agreement on two points: internal standardization across mission critical portfolios is both necessary and beneficial, and a methodical approach to MCO work is the best tool for assuring ongoing, optimal operating conditions.

Procedures and process-control plans may vary greatly across organizations, but there are several common best practices that are generally consistent among them all.

<i>Item</i>	<i>Description</i>
Dry run/testing	Dry-runs or walk-throughs of procedures are always advised—certainly in the case of highly involved, infrequent maintenance and repair activities, but even the first time you're working to get a new, low-risk, common procedure approved. It is always recommended to get out on the floor and physically walk through the steps of the process.
Switch tag	Borrowing a term from networking, switch tag refers to the practice of assignment of unique identifiers to major components in a system, which then carries forward to the rest of the subsystems and components. MCO power distribution systems are a common example. Distinct but similar feeds (perhaps identified by a UPS system) to multiple rooms, production areas, or even buildings will contain components with the same tag in them. This is an important practice for change control and maintenance management because your facility might have dozens of pieces of identical equipment, all supporting different functions, serving different areas, etc. Simply authorizing a procedure to replace a flux capacity on the first floor might seem detailed enough, until the technician pulls flux capacity Z-1 instead of A-1 which has normal production redundancy while Z-1, just one room over on the first floor, was a standalone unit supporting experimental work.
Back-out/contingency plans	Good procedures always include back-out or contingency plans detailing what to do if things start to go wrong, which could be as simple as the few steps needed to place the system(s) in a safe condition and notify management. Complex procedures with multiple phases of switching or re-alignment of gear may benefit from multiple specific back-out plans at key points along the way.
Tools and materials inventory	Whenever possible, going through a list of the tools and materials needed to complete the work ahead of time is a best practice too often ignored. You don't want to be halfway through a major work activity involving power or control systems—especially if you've already taken them offline!—only to find out that you ordered the wrong replacement parts. More commonly, not getting in the habit of checking or pre-staging the required tools and material causes delays in getting the work done.
Spare parts inventory	Spare parts inventory is a need that will vary largely upon the criticality of the systems and, quite frankly, the available financial resources. Even if you are not able to keep a large amount of spare parts related to regular maintenance items on hand, inventorying commonly replaced parts or wear items (belts, filters, gaskets, back-up batteries, etc.) that will be used allows the maintenance planner to evaluate the need ahead of the planned maintenance and order parts on a just-in-time basis.

---

<i>Item</i>	<i>Description</i>
Critical spares inventory	<p>Critical spares inventory can refer to two things: specific critical items needed for a specific maintenance task or the minimum stock of spare parts needed for critical components. Critical spares are those components that are absolutely vital to the continued operation of the critical infrastructure systems but are not readily available. The litmus test here is, if the component fails and there isn't a spare in the shop, is there a large impact on business continuity if that system has to remain offline for days or even weeks until a replacement can be sourced?</p> <p>Regardless of the stand-alone importance of a piece of equipment or systems, minimum critical thresholds for replacement parts and materials may be identified to trigger purchasing actions. These levels may be identified based on their availability or business impact, but also the simple number of similar pieces of equipment. A particular fuse block may not have a drastic impact on business continuity if it failed or a replacement hard to procure; but if there are 100 of them installed on various systems throughout the facility, you might want to have at least a few spares on hand at all times as a minimum threshold.</p>
Pre- and post-change documentation	<p>MCO operators live and die by documentation in their mission critical environments. Particularly when it comes to critical procedures or change-control work, it is crucial to have all of the pre-work documentation in place, including current revisions of procedures, approval documentation, expected results, and so on. Following the work, it is equally important to document the results of completed activities for material history records, as well as any notes gained from the results of the work. Without the proper documentation, it will be difficult to look back and validate that the systems were properly restored at the completion of the change.</p>

---



# ACTIVITY 13–3

## Managing Change

### Scenario

In this activity, you will identify how to manage change in your MCO installation.

1. Which change management best practice requires a formal written document that details the specifics of change-related tasks, particularly related to any work that might introduce fire hazards into the environment that could pose a threat to the person performing the work or normal business operations?
  - Permit to work
  - Hot work permit
  - Energized work
  - Double custody switching
2. Which time-related change management best practice refers to performing your change-related tasks during a time period that is outside of normal business hours in order to limit the impact on business operations?
  - Restricted change period/blackout date
  - Maintenance window
  - Off-hours work
  - Scheduled shutdown
3. Which time-related change management best practice refers to scheduling and planning the transition period between using an old system or component and using a new one?
  - Cutover window
  - Restricted change period/blackout date
  - Maintenance window
  - Scheduled shutdown
4. Which time-related change management best practice refers to performing your change-related tasks during a planned, scheduled time frame that is least likely to impact normal business operations?
  - Restricted change period/blackout date
  - Maintenance window
  - Off-hours work
  - Cutover window
5. Which change management best practice requires a formal written document that details the specifics of any change-related tasks that pose a threat to the person performing the work or normal business operations?
  - Permit to work
  - Hot work permit
  - Energized work
  - Double custody switching

6. Which time-related change management best practice refers to performing change-related tasks that will have an unavoidable impact on operations during a planned, scheduled time frame in which they can be temporarily suspended or moved to an alternate location?
- Restricted change period/blackout date
  - Maintenance window
  - Off-hours work
  - Scheduled shutdown
7. When making any changes to established procedures, you should always document the changes that have been made and the results of those changes on the affected systems.
- True
  - False
8. Which change management best practice requires two trained operators to perform any change-related tasks being done on high-energy equipment?
- Permit to work
  - Hot work permit
  - Energized work
  - Double custody switching
9. Which time-related change management best practice refers to prohibiting change-related tasks during specific time periods that would have too great of an impact on normal business operations?
- Restricted change period/blackout date
  - Maintenance window
  - Cutover window
  - Scheduled shutdown
10. When making any changes to established procedures, you should always have a contingency plan in place in case something goes wrong.
- True
  - False
-

# TOPIC D

## Regulations, Standards, Guidelines, and Compliance

In addition to the company-specific structures, standard operating procedures, and change management processes that help govern the day-to-day operations, there are a number of organizations that determine, supply, and, in some cases, enforce general protocols for the variety of industries involved in mission critical activities. These organizations develop and disseminate a variety of industry-based rules that help establish uniformity among the numerous industries in order to make sure that all MCOs are performed under consistent conditions and with consistent outcomes. As an MCO operator, you need to be aware of all of these organizations and the protocols that they provide. In this topic, you will identify the regulatory bodies and standards within the MCO industry.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Regulations
- Standards
- Guidelines
- Compliance

### Protocol Terminology

There are a number of various terminologies used within the MCO industry to describe the protocols that must be followed—the official (or, sometimes, unofficial) rules that dictate the most widely-accepted ways of doing things. Even as broad efforts (such as the CMCO program) are being taken to work towards commonalities and consistency throughout the industry, the lexicon varies from sector to sector, and even between organizations within the same sectors. In one form or another, all MCO organizations operate under one, some, or all of these various protocols, and you need to be aware of the difference between them.

<i>Item</i>	<i>Description</i>
Regulations	<i>Regulations</i> are established protocols, particular to certain industries or work practices, which are enforceable by law. Sometimes these regulations are written into local, state, or federal statutes and, therefore, can be enforced by the respective justice system. In other cases, publicly chartered agencies define these regulations, the enforcement of which is backed by the courts, but usually involves fines or revocation of business privileges as opposed to potential jail time.
Standards	<i>Standards</i> , one step down from regulations, are protocols defined by public or private industry agencies and associations, and are potentially backed by civil justice powers. An organization or industry may adopt the protocols established by such groups and treat them as seriously as laws and regulations. Standards are often established using environmental, operational, and safety best practices, but may be too detailed or dynamic to be enforced by governments.

<i>Item</i>	<i>Description</i>
Guidelines	<i>Guidelines</i> may come from any of the aforementioned groups, even statutes and laws, but are not mandatory and generally have no similar consequences if not followed. Guidelines provide situational direction for best practices and are often developed internally by your MCO organization.
Compliance	<i>Compliance</i> , very simply put, is whether or not you are following the rules laid out within a protocol. There is not necessarily any implication for how well you are following the rules, or even if you are making the best operational decision—just whether or not your actions or practices violate any applicable regulation, standard, or guideline.

## Building Codes

Building codes are the protocols established at various statutory levels and often supplemented by industry-leading associations that exist largely to govern the safe construction of facilities, which are generally inspected and enforced by local AHJs. There are two building code protocols that may apply to your MCO facility: UBC and IBC.

The Uniform Building Code (UBC), first published in the late 1920s by the International Council of Building Officials, detailed a set of standard requirements for the safe construction of buildings that would be applicable across all cities and states. Up until that time, each city had its own building codes that needed to be followed during construction. The UBC was updated and republished every three years.

In 1997, the UBC was replaced by the International Building Code (IBC), which merged the standards established in the UBC with standards established in three other organizations that published their own building codes in order to create a single, unified set of standards for safe building construction that are now followed throughout the United States and in some global markets.

According to the website for the International Code Council, the organization established to create and enforce the IBC, "the International Codes<sup>®</sup>, or I-Codes<sup>®</sup>, published by ICC, provide minimum safeguards for people at home, at school and in the workplace. The I-Codes are a complete set of comprehensive, coordinated building safety and fire prevention codes. Building codes benefit public safety and support the industry's need for one set of codes without regional limitations." (Source: [www.iccsafe.org](http://www.iccsafe.org))



**Figure 13–8:** *The construction of a new building would have to comply with the unified standards of the International Building Code. (Source: Tomwsulcer/Creative Commons (Public Domain)/ [https://commons.wikimedia.org/wiki/File:Summit\\_NJ\\_Construction\\_Site\\_DeForest\\_Avenue.jpg](https://commons.wikimedia.org/wiki/File:Summit_NJ_Construction_Site_DeForest_Avenue.jpg))*

## LEED

Leadership in Energy and Environmental Design (LEED) is a program operated by the US Green Building Council (USGBC) that provides a rating system for the design, construction, operation, and maintenance of sustainable, environmentally responsible, and resource-efficient buildings and campuses—commonly referred to as "green buildings." It also provides individual training and certification levels for professionals connected to the built environment, which is a reason why it is commonly followed within MCO industries.

According to LEED itself, it is "a green building certification program that recognizes best-in-class building strategies and practices. To receive LEED certification, building projects satisfy prerequisites and earn points to achieve different levels of certification. Prerequisites and credits differ for each rating system, and teams choose the best fit for their project." (Source: <http://www.usgbc.org/leed>)



**Figure 13–9:** *The Student Services building at the University of Texas Dallas is the first academic structure in the state to receive Platinum status under LEED guidelines. (Source: Stan9999/ Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:UT\\_Dallas\\_Student\\_Service\\_Building.JPG](https://commons.wikimedia.org/wiki/File:UT_Dallas_Student_Service_Building.JPG))*

## Uptime Institute

The Uptime Institute is a consortium of various companies in the data center industry that aim to create and disseminate data center information and best practices. It is probably best known for its widely adopted tier classification system, which evaluates and classifies data centers based on their uptime performance.

According to the Uptime Institute itself, it is "an unbiased advisory organization focused on improving the performance, efficiency, and reliability of business critical infrastructure through innovation, collaboration, and independent certifications. Uptime Institute serves all stakeholders responsible for IT service availability through industry leading standards, education, peer-to-peer networking, consulting, and award programs delivered to enterprise organizations and third-party operators, manufacturers, and providers. Uptime Institute is recognized globally for the creation and administration of the Tier Standards & Certifications for Data Center Design, Construction, and Operational Sustainability along with its Management & Operations reviews, FORCSS™ methodology, and energy efficiency initiatives." (Source: <https://uptimeinstitute.com/about-ui>)

## ANSI

The American National Standards Institute (ANSI) is an organization that develops and oversees compliance with national technical standards regarding the production and/or provision of products, services, processes, systems, and other related items. When possible, it coordinates these national standards with available international standards to ensure that products or services developed in America can be used without issue throughout the globe. Additionally, ANSI accredits both standards developed by other organizations, as well as accredits certain organizations for following the available national or international standards related to their product or service.

As detailed on the ANSI website, the organization "oversees the creation, promulgation and use of thousands of norms and guidelines that directly impact businesses in nearly every sector: from

acoustical devices to construction equipment, from dairy and livestock production to energy distribution, and many more. ANSI is also actively engaged in accreditation—assessing the competence of organizations determining conformance to standards. The mission of ANSI is: To enhance both the global competitiveness of U.S. business and the U.S. quality of life by promoting and facilitating voluntary consensus standards and conformity assessment systems, and safeguarding their integrity." (Source: [http://www.ansi.org/about\\_ansi/overview/overview.aspx](http://www.ansi.org/about_ansi/overview/overview.aspx))

## ASHRAE

The American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE) is a globally-supported organization that creates and disseminates information and best practices for HVAC and refrigeration systems in buildings and building systems, including standards and guidelines regarding energy efficiency, air quality, and sustainable practices that are often referenced in building codes and consulted during design and development. ASHRAE's standards and guidelines are widely accepted throughout most MCO sectors, and it regularly publishes standards specific to individual sectors such as medical facilities, communications installations, data centers, and more.

According to the ASHRAE website, it is "a global society advancing human well-being through sustainable technology for the built environment. The Society and its members focus on building systems, energy efficiency, indoor air quality, refrigeration and sustainability within the industry. Through research, standards writing, publishing and continuing education, ASHRAE shapes tomorrow's built environment today. ASHRAE was formed as the American Society of Heating, Refrigerating, and Air-Conditioning Engineers by the merger in 1959 of American Society of Heating and Air-Conditioning Engineers (ASHAE) founded in 1894 and The American Society of Refrigerating Engineers (ASRE) founded in 1904." (Source: <https://www.ashrae.org/about-ashrae>)



**Figure 13–10: An HVAC technician installs HVAC vents using ASHRAE's standards and guidelines.** (Source: United States National Guard/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/](https://commons.wikimedia.org/wiki/File:Colorado_Air_National_Guard_and_Army_Reserve_members_support_the_SMASE_Innovative_Readiness_Training_Program_in_Window_Rock_Airizona_130710-Z-BR512-017.jpg)

[File:Colorado\\_Air\\_National\\_Guard\\_and\\_Army\\_Reserve\\_members\\_support\\_the\\_SMASE\\_Innovative\\_Readiness\\_Training\\_Program\\_in\\_Window\\_Rock\\_Airizona\\_130710-Z-BR512-017.jpg](https://commons.wikimedia.org/wiki/File:Colorado_Air_National_Guard_and_Army_Reserve_members_support_the_SMASE_Innovative_Readiness_Training_Program_in_Window_Rock_Airizona_130710-Z-BR512-017.jpg))

## NETA

The InterNational Electrical Testing Association (formerly the National Electrical Testing Association, and still known as NETA) is an organization that develops and disseminates standards and specifications for the installation and maintenance of electrical power systems. Additionally, it accredits independent, third-party companies and certifies technicians that perform electrical testing according to the standards and specifications it has set forth for the industry.

From NETA's official website, "NETA is an association of leading electrical testing companies comprised of visionaries who are committed to advancing the industry's standards for power system installation and maintenance to ensure the highest level of reliability and safety. The mission of the InterNational Electrical Testing Association is to serve the electrical testing industry by establishing standards, publishing specifications, accrediting independent, third-party testing companies, certifying test technicians, and promoting the professional services of its members. The Association also collects and disseminates information and data of value to the electrical industry and educates the public and end user about the merits of electrical acceptance and maintenance testing." (Source: [www.netaworld.org](http://www.netaworld.org))

## TIA

The Telecommunications Industry Association (TIA) is an organization, accredited by ANSI, that develops and disseminates standards for products and services provided by a wide variety of companies within the Information and Communication Technologies industry. The twelve committees of the Standards and Technology Department within the TIA have developed guidelines for such telecommunications products and services as cell towers, VoIP, mobile communications, data terminals, satellites, healthcare-related telecom, accessibility, and more.

According to the TIA website, it is "the leading trade association representing the global information and communications technology (ICT) industry through standards development, policy initiatives, business opportunities, market intelligence and networking events. With support from hundreds of members, TIA enhances the business environment for companies involved in telecom, broadband, mobile wireless, information technology, networks, cable, satellite, unified communications, emergency communications and the greening of technology." (Source: [www.tiaonline.org](http://www.tiaonline.org))

## OSHA

The Occupational Safety and Health Administration (OSHA) was created under the Occupational Safety and Health Act of 1970 in order to create and enforce standards for safe working conditions and to provide education, training, and assistance to those organizations that need to follow those standards. OSHA defines both the organizations that must comply with its regulations—including both public and private organizations and largely driven by the workplace itself—as well as the regulations that those organizations must follow. Since it is technically part of the Department of Labor and therefore is backed by the US government, violations of OSHA regulations may result in fines or cause operations to be suspended or shutdown, and negligent violations causing environmental impacts, property damage, personnel injury, or death may result in criminal charges.





**Figure 13-11:** OSHA ensures that there are safe working conditions for personnel, such as requiring and verifying that PPE is being utilized when conditions are hazardous. (Source: CEphoto, Uwe Aranas/Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:Cologne\\_Germany\\_Industrial-work-with-Personal-Protective-Equipment-02.jpg](https://commons.wikimedia.org/wiki/File:Cologne_Germany_Industrial-work-with-Personal-Protective-Equipment-02.jpg))

## NFPA

The National Fire Protection Association (NFPA) is a US-based trade association that develops and disseminates standards and unified codes to be used by local governments and their associated fire protection services regarding the proper design and construction of fire-safe buildings and appropriate installation of fire safety systems, as well as guidelines for hazmat response, rescue response, and firefighting activities.

The NFPA describes itself as "a global, nonprofit organization devoted to eliminating death, injury, property and economic loss due to fire, electrical and related hazards. The association delivers information and knowledge through more than 300 consensus codes and standards, research, training, education, outreach and advocacy; and by partnering with others who share an interest in furthering the NFPA mission." (Source: <http://www.nfpa.org/about-nfpa>)

# ACTIVITY 13–4

## Identifying Regulatory Bodies and Standards

### Scenario

In this activity, you will identify the regulatory bodies and standards that might affect your MCOs.

---

1. Which organization develops and oversees standards, guidelines, and best practices for HVAC and refrigeration systems?
  - ANSI
  - ASHRAE
  - NETA
  - OSHA
  
2. Which organization develops and oversees standards, guidelines, and best practices for data center performance?
  - ANSI
  - LEED
  - Uptime Institute
  - TIA
  
3. Which organization develops and oversees standards, guidelines, and best practices for creating and maintaining safe working conditions?
  - ANSI
  - OSHA
  - NETA
  - LEED
  
4. Which organization develops and oversees standards, guidelines, and best practices for the production and/or provision of products, services, processes, systems, and other related items?
  - ANSI
  - NETA
  - TIA
  - Uptime Institute
  
5. Which organization develops and oversees standards, guidelines, and best practices for the proper design, installation, and response techniques for fire protection systems and services?
  - LEED
  - NETA
  - OSHA
  - NFPA

6. Which organization develops and oversees standards, guidelines, and best practices for the proper installation and maintenance of electrical systems?
- ASHRAE
  - NETA
  - TIA
  - ANSI
7. Which organization develops and oversees standards, guidelines, and best practices for the design, construction, operation, and maintenance of "green" buildings?
- ANSI
  - OSHA
  - LEED
  - ASHRAE
8. Which organization develops and oversees standards, guidelines, and best practices for the production and/or provision of telecommunications products and services?
- NETA
  - Uptime Institute
  - ANSI
  - TIA
9. The UBC is a single, unified set of standards for safe building construction that are followed throughout the United States and in some global markets.
- True
  - False
-

## Summary

In this lesson, you identified and applied industry standards regarding operations and procedures within a mission critical facility. As an MCO technician, it is imperative that you have a strong working knowledge of any of the standards, regulations, guidelines, or any other protocol that you need to be in compliance with in order to operate your facility within the strict parameters that these regulatory bodies create and enforce. In some cases, these protocols come with legal consequences attached to any violations or instances of non-compliance; in others, these protocols are nothing but voluntary best practices that are meant to add an element of uniformity to the various organizations across the MCO industry as a whole—but in any case, they will help ensure that your MCO facility is operating under optimal conditions and at the very least meeting (or, even better, exceeding!) the standard expectations of your industry's leading organizations.

# 14

# Facility and System Documentation

## Lesson Objectives

In this lesson, you will identify and apply industry standards regarding facility and system documentation within a mission critical facility. You will:

- Identify the types of documentation and their purposes in regards to MCOs.
- Identify the types of operating and maintenance manuals and their purposes in regards to MCOs.
- Identify types of testing reports and their purposes in regards to MCOs.

## Lesson Introduction

With so many components and systems that comprise the MCO infrastructure, it is incredibly important that there be well-planned, properly maintained documentation to accompany each of them. This facility and system documentation includes the design documents that detail the initial plans for the space or system; the actual, final structure of it once construction was completed; the various plans and diagrams that explain the ways in which the components or systems work together; the manuals explaining the proper operations and necessary maintenance for specific components or systems; and even the various reports that you yourself can generate to verify the proper operations for the various elements of the infrastructure.

With such an extensive list, it is imperative that you, as the MCO operator, have a strong understanding of the kinds of information provided by these different types of documentation and—importantly—how to utilize that information to ensure that your MCO infrastructure is operating under optimal conditions. In this lesson, you will identify and apply industry standards regarding facility and system documentation within a mission critical facility.

# TOPIC A

## Documentation Types

When it comes to keeping track of the various components that make up your critical systems and the various system structures that make up your critical infrastructure as a whole, there's a whole lot of paperwork that you should keep on hand—and update regularly!—to ensure that they are all operating under optimal working conditions. As an MCO operator, who will be in charge of operating and maintaining these systems or overseeing those that do, you need to be intently aware of what the various kinds of documentation can tell you about your components and systems, and the ways in which they all integrate. In this topic, you will identify the types of documentation and their purposes in regards to MCOs.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Basis of Design (BoD)
- Design specifications
- Single line diagram
- As-built drawing
- Record drawing
- Panel schedule
- Submittals
- Flow diagram
- Control diagram
- Plans
- Equipment schedule

### BoD

The *Basis of Design (BoD)* is the first iteration of the design of a facility or project, and explains the operational expectations and limits of the installation at a very high level, typically in a more narrative format. It is the foundation from which the rest of the design and construction plans are created.

Specific equipment will not usually be called out, and the detail of performance specifications is usually limited to full building or system level. For instance, the mechanical BoD may call out the expected maximum cooling capacity, required level of redundancy, expected efficiency or economization requirements, etc., but will not call out the type or number of AHUs to be used.

### Design Specifications

*Design specifications* refer to documentation that details each and every system and piece of equipment within an MCO project that will help establish criteria that will need to be met during development and construction. This includes specific characteristics about the components or systems and important associated information for them, such as the resources required to keep the systems operational. Design specifications are drawn out from the Basis of Design, generally by an engineering partner, and must be specific enough to send out to competing contractors so they can submit bids based on providing essentially the same products and/or services.

For example, the design specs for the mechanical BoD might take a 5,000 ton cooling need with 25% economization, and detail the number of chillers, the capacity of each, the power feed requirements, control packages, etc. Design specifications, particularly for an entire facility, tend to be extremely lengthy, so it is not expected that all MCO technicians have read them in their entirety,

but you must know how to access them if you want to be able to evaluate equipment or systems against their intended or maximum capacity and efficiency.

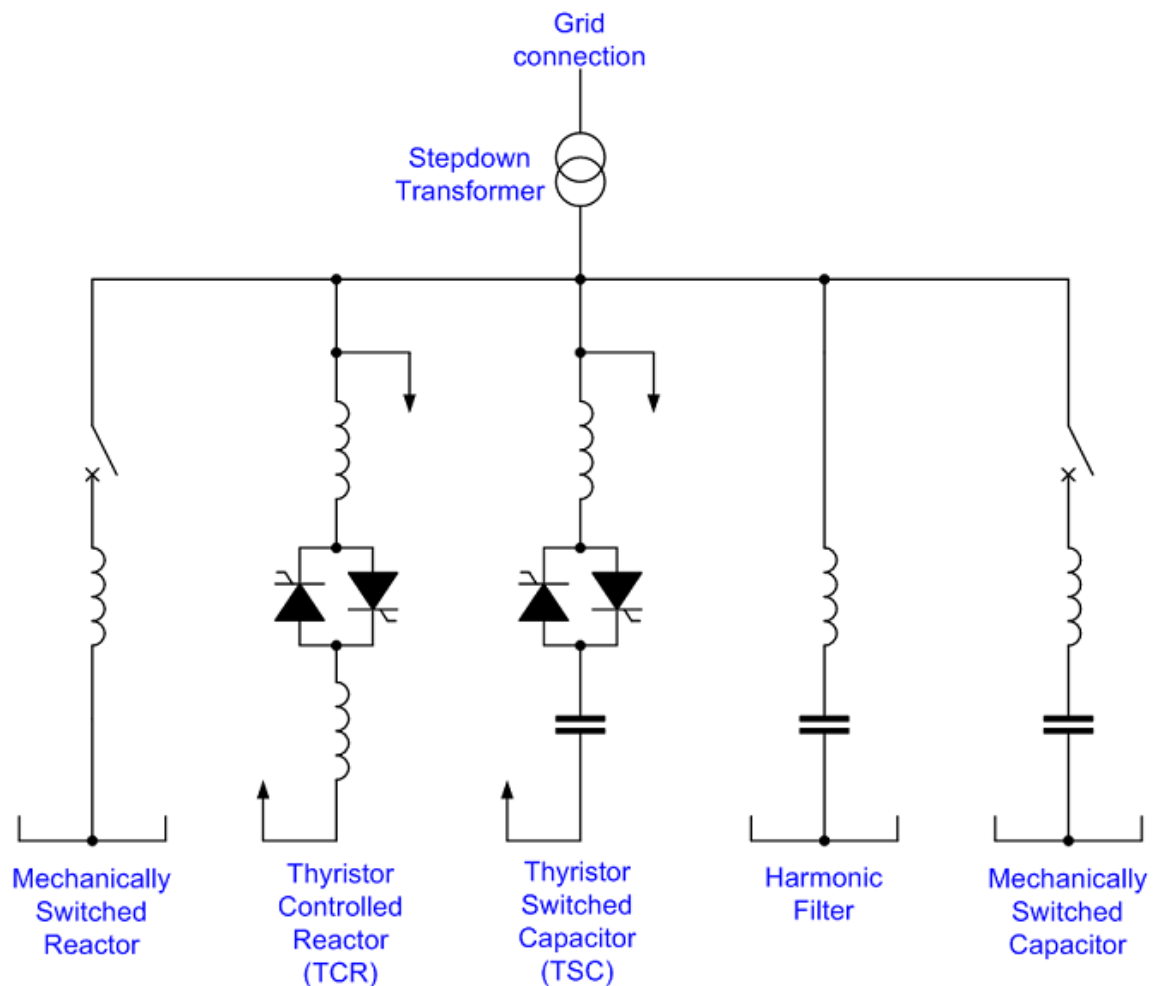
## Single Line Diagrams

A *single line diagram* is a nominally simplified drawing of a system, which illustrates the connections of components and equipment with single lines that might represent wiring, piping, structural components, etc. Depending upon the level of detail desired for the specific drawing, intermediary or connecting components like breakers, valves, flanges, junction boxes, etc., may or may not be represented. The arrangement of components on the diagram does not necessarily represent the true-life orientation in the facility, but critically must represent the actual "flowpaths" of the illustrated systems. A single line diagram is often squared-off to make for a compact arrangement fitting onto the fewest number of pages.

At a minimum, MCO teams should have access to and be familiar with single-line diagrams for the following systems in their facilities:

- Electrical systems
- Mechanical systems
- Plumbing systems
- Fire protection systems
- Control systems

Good facility documentation should include some sets of single lines, but a good measure of a trained MCO technician is that you can draw single-line representations of critical systems from memory.



**Figure 14–1: A single line diagram of the path of electricity through a transmission Static VAR Compensator. (Source: Clampower/Creative Commons (CC BY-SA 3.0)/[https://commons.wikimedia.org/wiki/File:Static\\_VAR\\_Compensator\\_2a.png](https://commons.wikimedia.org/wiki/File:Static_VAR_Compensator_2a.png))**

## As-Built Drawings

As the contractor works with the construction documents to build or renovate the facility, there are often unforeseen conditions or changes that are made during the construction process. These may include conditions that were concealed in an enclosed wall or ceiling, the inability to "fit" infrastructure in as designed, or the substitution of materials as specified. The contractor marks up or "red-lines" the construction documents to note any changes or substitutions; these documents are called *as-built drawings*, since they reflect the structure of the building as it was built instead of just planned. In most cases, as-built drawings are then provided to the consultant (architect/engineer) to revise the drawings. These drawings which are likely done in either Building Information Modeling (BIM) or Geographic Information System (GIS) are then noted as *record drawings*. This step from as-built to record drawings is important in order to have as accurate documentation of the structure as possible; unfortunately, it is not uncommon for a project to be considered complete but the documents have not been updated to reflect the changes made during construction.

## Panel Schedules

A *panel schedule* is a tabular list of the electrical distribution systems and subsystems within a facility. Many operators are probably familiar with component level panel schedules, which is to say, the last sets of panels feeding out directly to equipment. These would be like the circuit breaker panel in



your house—when you open the box, there is usually a grid of boxes on a sheet that mirrors the layout and numbering of the breakers themselves, with each box labeled with the area of the house being powered by that breaker.

Panel schedules are also used at higher levels in the distribution system, both on main distribution panels as well as on electrical drawings. These will show which lower-level distribution panels are fed from each circuit, again mirroring the layout of breakers in the distribution board itself, as well as labeled in the same manner as the circuits themselves.

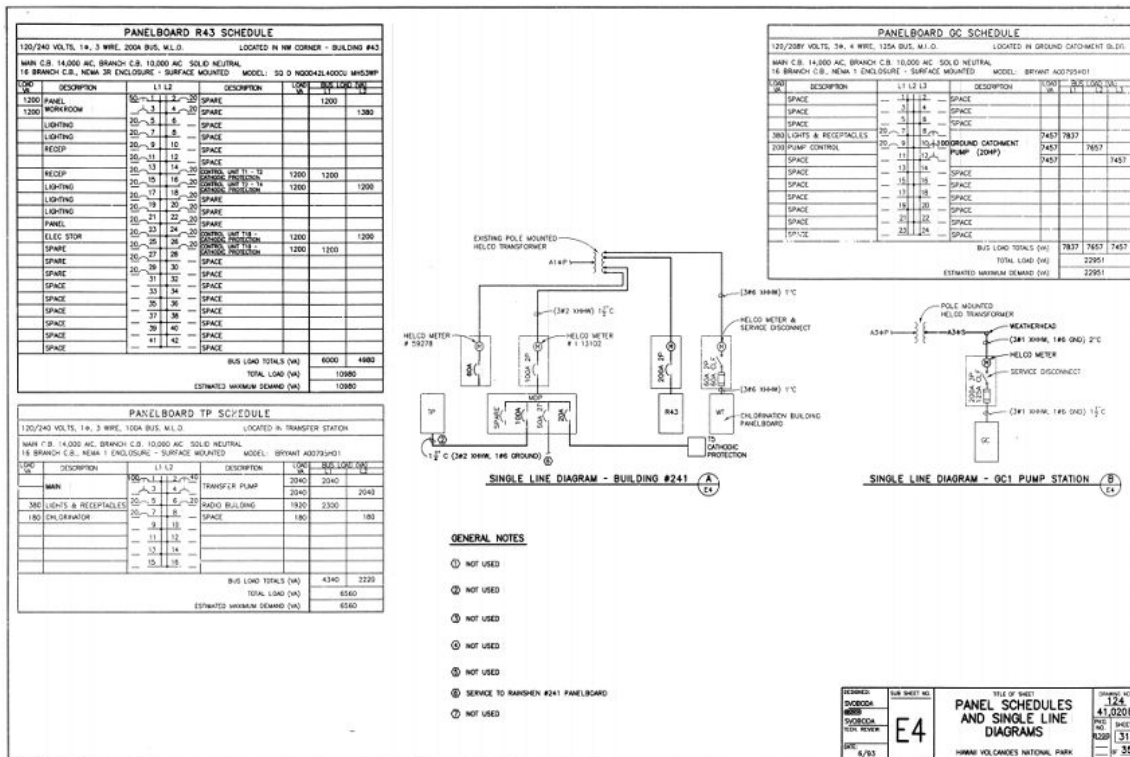


Figure 14-2: A panel schedule and single line diagrams for the water collection system of Hawaii Volcanoes National Park. (Source: Library of Congress/Creative Commons (Public Domain)/ [https://commons.wikimedia.org/wiki/File:Panel\\_Schedules\\_and\\_Single\\_Line\\_Diagrams\\_-\\_Hawaii\\_Volcanoes\\_National\\_Park\\_Water\\_Collection\\_System,\\_Hawaii\\_Volcanoes\\_National\\_Park,\\_Icarno,\\_Hawaii\\_County,\\_HI\\_HAER\\_HI-76\\_\(sheet\\_35\\_of\\_40\).png](https://commons.wikimedia.org/wiki/File:Panel_Schedules_and_Single_Line_Diagrams_-_Hawaii_Volcanoes_National_Park_Water_Collection_System,_Hawaii_Volcanoes_National_Park,_Icarno,_Hawaii_County,_HI_HAER_HI-76_(sheet_35_of_40).png))

## Submittals

Submittals are the general categorization of any design or construction documentation made in response to project requirements that needs some level of review and approval. The construction manager, general contractor, or project manager will be responsible for submittals, so that they are all collected and distributed from the same point and reviewed by the appropriate and necessary higher-level personnel.

While almost anything can be a submittal—even email questions and answers—there are several categories of particular importance to MCO teams.

Documentation	Description
Cut sheets	Cut sheets are also known as equipment specification or system detail sheets. These may be somewhat generic if they are manufacturer's documents, and won't necessarily reflect the final installation details, but are used to ensure the selected components and equipment meet design requirements.

<b>Documentation</b>	<b>Description</b>
Operations manuals	As submittals, operations manuals are the operating sequences and instructions as provided by the manufacturer of the respective equipment. Certain projects may also require that custom operations manuals be drafted, but these tend to fall outside of project submittal processes as it may be difficult to write excellent, comprehensive operations manuals until you see how the gear is installed with all the other interrelated systems.
Maintenance manuals	As submittals, maintenance manuals are somewhat generic manuals originating from the organization that built the equipment or provided final assembly of systems. Original equipment manufacturer (OEM) manuals may include maintenance procedures for multiple models of the same or similar types of equipment. While they may have additional unneeded information or might be missing the desired level of detail, they are documented as submittals so the MCO team has something to work with when the facility is turned over to their care.
Troubleshooting guides	Troubleshooting guides may be included in operations and/or maintenance manuals, but if not, submittal requirements might call for the contractor to provide separate troubleshooting documents for the equipment they are installing.
Signoff and Approval forms	As submittals are treated as formal documentation, the process for receipt, dissemination, review, and approval must be equally as formal. The project manager, therefore, is responsible for ensuring that sign-off/ approval forms are filed with each submittal so there is a complete record of the documentation as part of the project.

## Flow Diagrams

*Flow diagrams* (also known as block and arrow diagrams) show the directional relationships between things and or processes. They can take on many forms and aren't necessarily very detailed or technical, but provide an easy means to share information without much prerequisite level of knowledge or expertise. Emergency plans might show the directions to exit paths, evacuation points, or emergency equipment, as well as using a flow diagram to explain the different paths of notification or escalation required for a particular type of event. Processes work well with flow diagrams also—such as how procedures are written, reviewed, and approved.

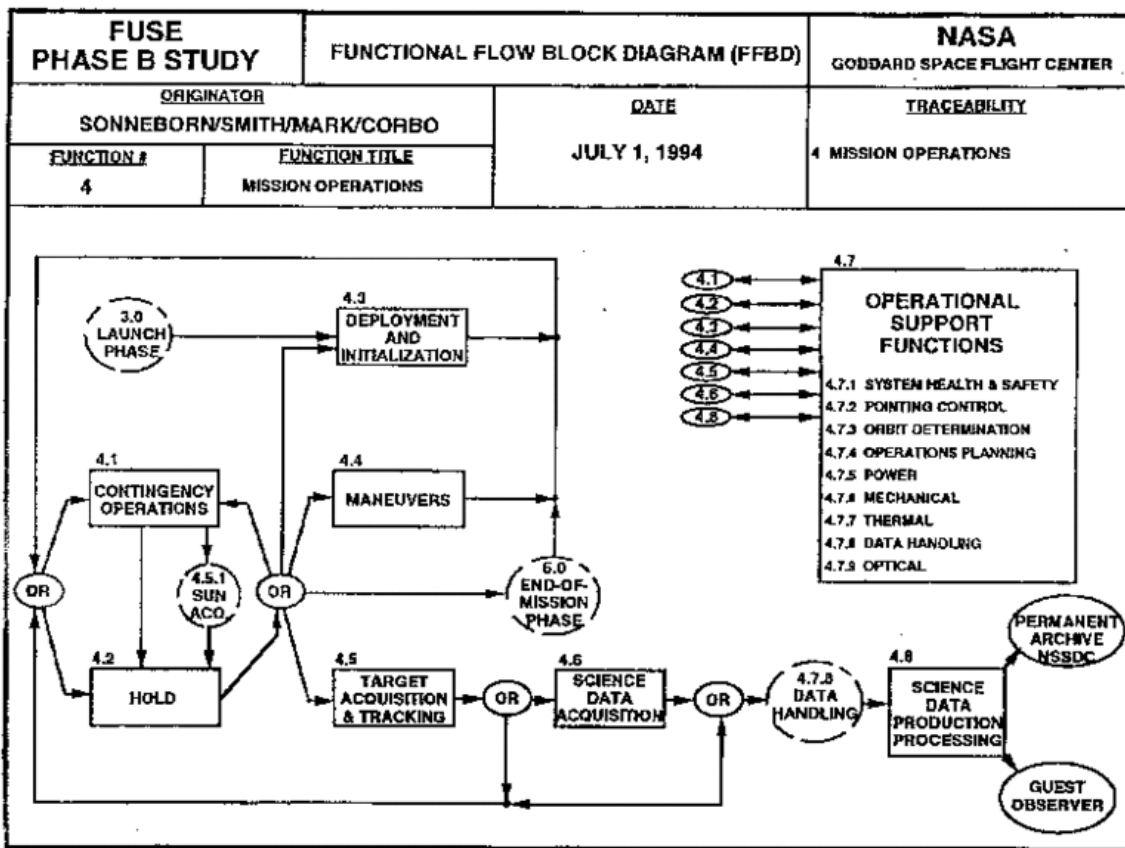


Figure 14-3: A simple flow diagram for mission control operations at NASA's Goddard Space Flight Center. (Source: NASA/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Functional\\_Flow\\_Block\\_Diagram\\_for\\_Mission\\_Control.gif](https://commons.wikimedia.org/wiki/File:Functional_Flow_Block_Diagram_for_Mission_Control.gif))

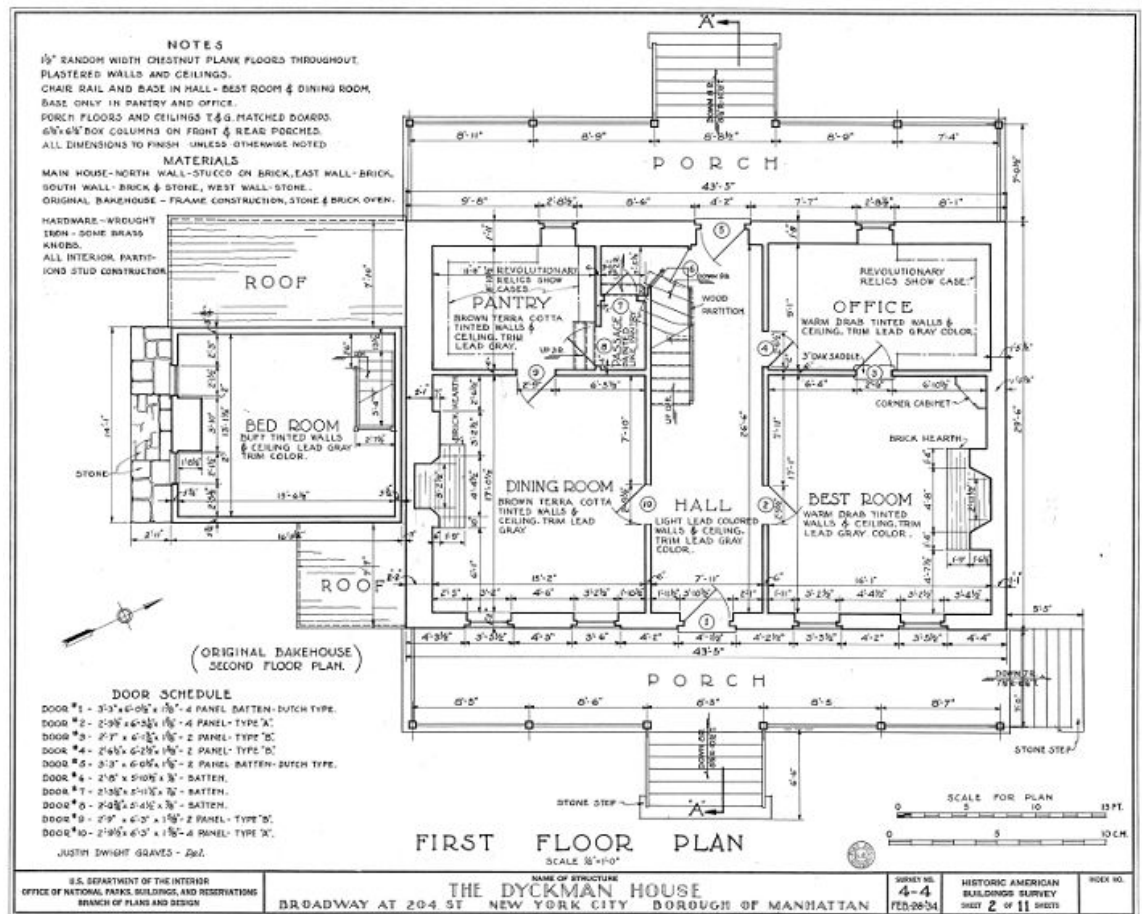
## Control Diagrams

Control diagrams are simple illustrations—usually block diagrams—that show the hierarchy of control panels and the devices that they monitor and/or control. They usually do not include the ladder logic of If-Then statements showing how the control works, unless high-level operations can be simplified into concise flow diagrams.

## Plans

Plans are a general category of documents that detail the means and manner of the design and build processes and often include some of the other types of documentation already discussed, such as single line diagrams. Two common types of plans often utilized in MCO projects include floor plans and equipment layout plans.

Floor plans provide very basic but essential information about the general layout of the facility or space. This is not necessarily the drawing used for construction, but for the owner to use to identify room occupants and equipment location. These plans will include room numbers, door swings, and show fixed equipment. These drawings are often used for documenting emergency evacuation plans.



**Figure 14-4: The floor plan of the Dyckman House, a historic building in Manhattan, New York. (Source: Library of Congress/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:Dyckman\\_House,\\_Broadway\\_and\\_204th\\_Street,\\_New\\_York,\\_New\\_York\\_County,\\_NY\\_HABS\\_NY\\_31-NEYO,11-\(sheet\\_2\\_of\\_11\).tif](https://commons.wikimedia.org/wiki/File:Dyckman_House,_Broadway_and_204th_Street,_New_York,_New_York_County,_NY_HABS_NY_31-NEYO,11-(sheet_2_of_11).tif))**

Equipment layout plans delineate how each piece of semi- or non-permanent equipment will be installed in each area of the facility. The level of effort and detail put into layout plans ahead of installation projects varies, but preparation is crucial on fixed timelines, supporting the old adage "measure twice, cut once." All too often hundreds of thousands—if not millions—of dollars worth of equipment may be delivered for a project only to find out there's not enough room for it to be installed, proper egress routes cannot be established, or worse yet, they're too big to fit in the building! Therefore, equipment layout plans are essential for making sure installation goes smoothly.

## Equipment Schedules

An *equipment schedule* is a systematic itemization of critical equipment within a system or space, similar to electrical panel schedules. Comprehensive documentation will have this information recorded in a few different manners: by system, which would include a list of all the components in a given system (such as a chilled water system); and by location, which would include a list of all the components in a given space (such as a generator enclosure).

Equipment schedules may have specific labels that can be used as a legend throughout various other types of documentation sets.

## Digital System Architecture Plans

Digital systems architecture plans—which detail the structure and connections of the IT, specialized networks, management/automation systems, and other digital systems for the facility—are just as important as the plans for the physical infrastructure, even though they don't necessarily translate as well into diagrams as other infrastructure systems. From a component standpoint, you need to understand how all the devices, controls, routers, and other components that make up these digital systems are tied together. At a minimum, MCO teams will benefit from having digital system architecture plans for BMS, BAS, and SCADA systems.

These plans also help in troubleshooting system issues. MCO technicians can quickly sort through and find the rough level of the fault, while identifying everything affected and ruling out everything still working. However, it is also worth noting that most facilities will not receive service from the same programmer that built the program, so technicians may need access to a high-level overview to establish a baseline understanding before diving into the code and controls to troubleshoot issues.

## Document Aggregation Platforms

By their nature, mission critical facilities will likely have multiple, complex building systems. This results in multiple layers of design, construction documentation, and other contractor-provided information. Therefore, the organization of the various system documentation is critical. The two most commonly used platforms to organize this information are Building Information Modeling (BIM) and Geographic Information System (GIS). With BIM and GIS, the MCO operators can access and become familiar with the systems for preventative maintenance or in the event of an emergency.

BIM is more prevalent for individual buildings. BIM takes what was 2D information in a Computer-Aided Design (CAD) system and pairs it with other building information and data to create an intelligent digital system for designing, constructing, and then operating and managing a building and its associated infrastructure. BIM consists of a series of files that contain data and analysis information along with the design information required for constructing the facility. These files are then networked into a 3D representation that can be used by multiple parties.

GIS is used more often when there are multiple buildings with associated site infrastructure, as it is developed with a spatial data infrastructure reference. Similar to BIM, GIS is used to capture, manipulate, analyze, and then manage all types of building and infrastructure information with references to spatial or geographical data. Although the documents used to construct a building may be produced using GIS, this system is used for many other operations, including site infrastructure planning, environmental and safety management, and transport logistics.

## Record and Drawing Access

Records and drawings are nearly worthless if the MCO team does not have access to them. Original hard copies of drawings, BoD, design specs, and other important documents should always be made in duplicate, ideally with one verified copy kept at a safe, offsite location in the case of some catastrophe. Final sets should be clearly marked, so that if operators need to refer back to them or copies are needed, there is no possibility that they are working off of a draft revision that doesn't reflect final installed details. Additionally, as easy and affordable as it is to store things digitally today, properly labeled electronic copies should be provided—and, if not, requested—as part of all project turnover for any reference needs.



**Note:** To further explore how to document an MCO facility project from the initial concept to the live environment, you can view the **Document an MCO Design—From Start to Finish** presentation from the Certified Mission Critical Operator Video Series.

## Case Study: Transfer of Documentation Knowledge

Any of the myriad systems within an MCO facility will have accompanying documentation, in which there is important information regarding the safe, consistent operations of the equipment and components that keep the MCOs up and running. Making sure that there is a transfer of this documentation knowledge is critical, so that all current and future MCO operators and other integral personnel know how these systems operate—whether that is optimally or problematically—and how to handle them during extreme situations, such as an emergency. To show the importance of the transfer of documentation knowledge, take a look at what could happen if this important action was *not* taken.

A large, independent university has just completed the construction of a Data Research Building. The university's Facilities Design and Construction staff designed the building with the engagement and input of the research faculty and staff in countless meetings with a nationally recognized architectural and engineering firm with specific expertise in data research facilities. The construction of the facility was then completed by a national firm also with expertise in this area. At the completion of construction and as required by contract, the contractor handed over all documentation including submittals, as-built drawings, and O&M manuals to the architectural and engineering firm. This firm confirmed accuracy, created as-built drawings with reference to the submittals and O&M manuals, and then provided all of the required documents to the university's Facilities Design and Construction staff. However, the Facilities and Design Construction personnel never passed on the documentation to the research facility's staff, who would actually be occupying the newly designed and constructed space.

Upon completion of construction, the university took ownership of the building and the research faculty and staff moved into the building. As the faculty and staff moved in, the facilities staff that would be operating the building now had their first exposure to the project. The contractor had now left and moved on to another out-of-state project and the architecture and engineering firm was still in the process of approving final documentation. The data processing center within this facility was state of the art with separate mechanical and electrical systems—essentially nothing like the facilities staff had ever seen. Without any documentation, the staff took on the challenge of figuring this out on their own.

Two months after occupancy there was an electrical failure. The facilities staff understood that, in the event of an electrical outage, power needs would be met by the emergency generator. Without the final documentation, however, what was not clear was what circuits were being fed by the generator. The server room had self-contained room conditioning units to supplement the buildings central HVAC system. The environmental conditions of this room were being tracked remotely at the Central Utilities office. The temperature of this room began to rise and it became obvious that the self-contained room conditioning units were not on the emergency generator.

The facilities staff contacted the design and construction staff and, after an hour, the appropriate contact was made with the engineering firm. The engineer reviewed both the construction drawings and the as-built drawings and determined that there was a discrepancy in the wiring diagrams that had not been previously brought to his attention. Essentially, what was intended to be an emergency power was not. The server room reached a temperature where the servers shut down. Fortunately, since the research faculty and staff had been operating in another facility, data was still being stored at this other location; because of this unplanned redundancy, while the servers were lost, the data was not.



# ACTIVITY 14-2

## Identifying Documents and Their Purposes

### Scenario

In this activity, you will identify documentation types and their purposes in the MCO environment.

1. **Design specifications establish the specific criteria that will need to be met during development and construction, including the specific components, systems, and resources that are required.**
  - True
  - False
  
2. **Which type of documentation provides details regarding any project design and/or construction information that needs to be reviewed and approved by the appropriate and responsible member of the team?**
  - Plan
  - Equipment schedule
  - Submittal
  - Control diagram
  
3. **Which type of documentation provides an itemized list of all of the critical components within a specific system or space?**
  - As-built drawing
  - Equipment schedule
  - Plan
  - Digital system architecture plan
  
4. **Which type of documentation provides details regarding any changes made to the original design as a result of the actual conditions of the space during construction?**
  - Single line diagram
  - Plan
  - Submittal
  - As-built drawing
  
5. **Which type of documentation provides details regarding the means and manner of the design and build processes, such as the general layout of a space or facility?**
  - Flow diagram
  - Control diagram
  - Plan
  - As-built drawing



- 
6. Which type of documentation provides details regarding the directional relationships between components or processes within a system or space?
- Flow diagram
  - Control diagram
  - Digital system architecture plan
  - Panel schedule
7. Which type of documentation provides details regarding the structure and connections of the various networks, management/automation systems, or other specialized systems within a space?
- Panel schedule
  - Digital system architecture plan
  - Flow diagram
  - Single line diagram
8. Which type of documentation uses a simple illustration to provide details regarding the connections of components and equipment within a system or space?
- Flow diagram
  - Plan
  - Control diagram
  - Single line diagram
9. Which type of documentation provides an itemized list of the electrical distribution systems and subsystems within a space or facility?
- Single line diagram
  - As-built drawing
  - Panel schedule
  - Flow diagram
10. Which type of documentation uses a simple illustration to provide details regarding the hierarchy of control panels and the devices that they monitor or control?
- Flow diagram
  - Plan
  - Control diagram
  - Single line diagram
11. Building Information Modeling (BIM) is best suited to capture and manage documents for projects concerning multiple facilities or locations and their associated critical infrastructure.
- True
  - False
12. Which type of documentation explains the operational expectations and potential limitations for the space being constructed, and serves as the foundation for other, more specific design and construction plans?
- Basis of Design
  - Design specifications
  - Record drawing
  - Equipment layout plan
-

# TOPIC B

## Operating and Maintenance Manuals

An important subset of facility and system documentation are the operating and maintenance manuals that accompany a system design and the various components that make up the systems in your MCO facility. These types of documentation provide important information regarding the conditions needed—including how to safely operate them and properly maintain or repair them—for the ongoing, optimal operations of each of these elements. As an MCO technician, you will be responsible for performing these kinds of tasks or, at the very least, overseeing them; therefore, it is imperative that you are familiar with the information contained in these manuals—or, at a minimum, aware of where these manuals can be found for reference—in order to keep your facility running smoothly and safely. In this topic, you will identify the types of operating and maintenance manuals and their purposes in regards to MCOs.

The following terms and concepts will be introduced in this topic. Pay special attention to these terms, as you will need to know them for your certification.

- Shop drawings
- Sequence of operation (SOO)

### Shop Drawings

*Shop drawings* refer to the initial, draft illustrations that detail the facility, system, and equipment design and setup for a project. Shop drawings may start with basic system diagrams, which are then modified with specific details such as the actual equipment to be installed, any required isolations, or even necessary architectural overlays. Shop drawings also refer to manufacturers basic equipment diagrams, which may then be modified based upon special features or components needed for the specific MCO project. As these notes and changes are made to the shop drawings, they are reviewed through the submittal process before being released to the installation contractors. The contractors will then use the shop drawings to determine exactly how and where equipment needs to be installed.

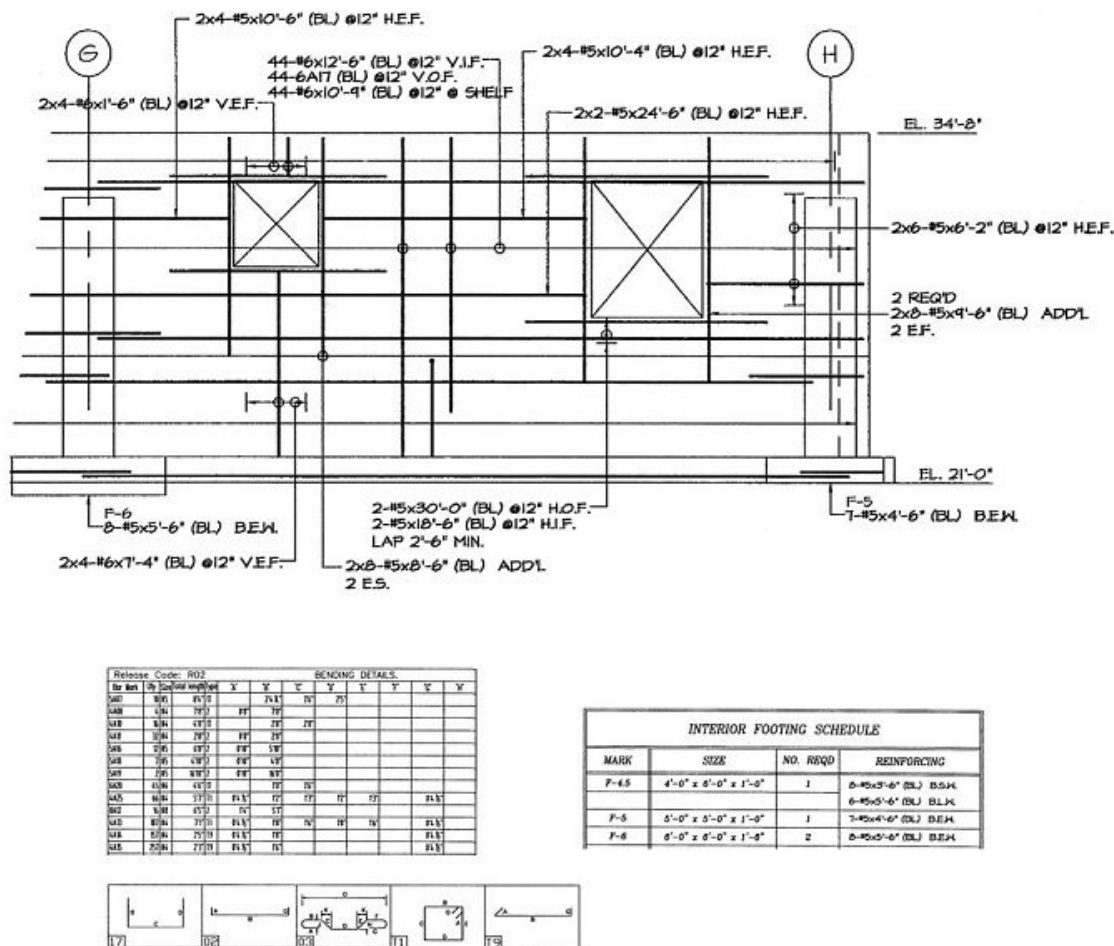


Figure 14-5: A shop drawing shows how steel reinforcements will be used in a foundation wall. (Source: Stephen Shay/Creative Commons (CC BY-SA 3.0)/https://commons.wikimedia.org/wiki/File:Example\_of\_Steel\_Reinforcement\_Shop\_Drawing.jpg)

### SOO

A *sequence of operation (SOO)* refers to a narrative description (although some block/flow diagrams may be used) of how equipment and systems are designed to operate under a variety of conditions or circumstances. Basic SOO will include startup and shutdown procedures, as well as major modes of operation for individual gear. More complex SOO—which need to be well-documented and understood by MCO technicians—will detail how various system operations are integrated together. For example, there should be a documented SOO for how the various systems are designed to trigger backup power systems, transition electrical load to serve critical infrastructure, and place support systems into emergency modes of operation in the event of a utility power outage.

### Warranty Information

Well-detailed warranty information is an often overlooked set of documentation for new build or retrofit projects. For instance, while it might be common knowledge amongst the MCO personnel that the gear that was just installed has a 2 year warranty, the details tend to get muddled. If and when something breaks, does anyone know if it is a full parts and labor warranty? Or the exact start date of the warranty? Should you work with the installation contractor or directly with the manufacturer? The list of questions goes on and on. When a new project is complete, all of the documents should be compiled, checked for completeness and stored (with multiple copies) so the MCO team can access them whenever needed—including all relevant warranty information.

## Seasonal Operation

Some MCO installations have diverse infrastructure that is more directly affected by outdoor environmental conditions. Of course, spaces that are occupied by personnel will have heating and cooling modes for winter and summer respectively, but there might be some system-specific seasonal operations that go beyond these kinds of supplemental heating or cooling needs. For instance, outdoor fluid systems may have special requirements to manage freeze protection concerns in the winter or severe heat-generating equipment may need to be limited in operation during summer heat waves. All of these seasonal operational considerations should be evaluated and detailed during the design and build phases, ideally via a close working relationship with the project engineer and the operations teams. Thorough training should be provided to all facility operators and technicians, but that does not circumvent the needed for complete and accessible documentation detailing operational limits and SOOs for seasonal modes.



***Figure 14–6: A snow-covered campus at the University at Buffalo, State University of New York, likely has some equipment that requires season-specific operations during Western New York winters. (Source: Quintessenceanx/Creative Commons (Public Domain)/[https://commons.wikimedia.org/wiki/File:University\\_at\\_Buffalo,\\_Student\\_Union.jpg](https://commons.wikimedia.org/wiki/File:University_at_Buffalo,_Student_Union.jpg))***

## Preventative Maintenance Procedures and Schedules

Preventative maintenance procedures and schedules can start to be developed as early as possible in the design and construction phases of an MCO project. Manufacturers regularly provide maintenance scope and interval recommendations, which can be supplemented by industry best practices and knowledge from the operations team. It is highly recommended that you require contractors to (at a minimum) provide input for recommended maintenance either as part of installation or as a project deliverable; or, even better, require them to provide drafts of maintenance procedures as part of their hand-off.

# ACTIVITY 14-3

## Identifying Operating and Maintenance Manuals and Their Purposes

### Scenario

In this activity, you will identify the various operating and maintenance manuals and their purposes within an MCO installation.

1. Which type of operating or maintenance documentation provides details regarding changes that may need to be made to some components or systems during specific periods of time in which environmental conditions may affect their normal operations?
  - Shop drawings
  - Sequence of operation
  - Warranty information
  - Seasonal operation
  - Preventative maintenance
2. Which type of operating or maintenance documentation provides a description of how components or systems should operate individually or collectively given a specific set of conditions or circumstances?
  - Shop drawings
  - Sequence of operation
  - Warranty information
  - Seasonal operation
  - Preventative maintenance
3. Which type of operating or maintenance documentation provides details regarding how and when to perform periodic service or repair tasks to maintain optimal operations of components or systems?
  - Shop drawings
  - Sequence of operation
  - Warranty information
  - Seasonal operation
  - Preventative maintenance
4. Which type of operating or maintenance documentation provides details regarding the intended design and setup of components, systems, or the facility in general?
  - Shop drawings
  - Sequence of operation
  - Warranty information
  - Seasonal operation
  - Preventative maintenance

5. Which type of operating or maintenance documentation provides details regarding a manufacturer's responsibility to provide maintenance, repair, or replacement for components or systems within the space?
- Shop drawings
  - Sequence of operation
  - Warranty information
  - Seasonal operation
  - Preventative maintenance
-

# TOPIC C

## Testing Reports

In addition to the various types of documentation provided by designers, contractors, and manufacturers, there are a number of testing reports that can be generated directly from the components and systems within your MCO infrastructure. These reports can be highly effective and incredibly informative, providing important information about the general conditions and current operations of the various elements within the MCO facility. As an MCO operator, you need to be aware of the different types of testing reports that are available, and know how to perform these tests and analyze the information they provide. In this topic, you will identify types of testing reports and their purposes in regards to MCOs.

## Commissioning Reports

The focus of commissioning is to develop and deliver a facility that functions and operates as it was designed and engineered. To achieve a full deliverable in the commissioning process, including the training of facility operators, it is vital that reports are developed to document the verification and performance results of all building systems and related equipment.

The evolution of the reporting begins with the Commissioning Agent (CA) attached to the project, who reviews every phase of the process to facilitate commissioning actions and reporting. Since the CA is included in the design phase of the project, this individual assists the architect and engineers in the preparation of the operations manuals associated with the facility and equipment. The CA will then prepare a commissioning plan and deliver a complete description of the commissioning requirements to the architect and engineers and review the design documents with them in order to assist in coordination efforts.



**Figure 14-7:** The Commissioning Agent for a project reviews the design documents with the project's lead engineer. (Source: Digital Vision/Photodisc/Thinkstock)

Functional Performance Testing (FPT) of facility equipment and related systems is the central focus of the commissioning process. Each piece of equipment and its related systems are tested for design functionality by the appropriate contractor or equipment manufacturer upon installation. The CA is then responsible for witnessing and documenting the FPT to ensure that each piece of equipment functions as designed and can be operated as engineered.

Integrated Systems Testing is the pinnacle of the commissioning process and is critical to ensure that full systems are installed appropriately and according to the design, especially in relation to other equipment components within the system. This type of testing checks the functionality of the system as a whole by manipulating specific components or systems while verifying the various component and/or system interconnections against the design documentation. Integrated systems testing cannot be completed until there is a full understanding of how each piece of equipment operates, how each piece of equipment relates to the system, or how one system relates to another.

Throughout the commissioning phases, the CA will coordinate the commissioning assignments until all systems have been fully verified to function as designed. The CA prepares written reports of all commissioning activities and reports these findings to the owner.

## Testing, Adjusting, and Balancing Reports

Specific to the HVAC systems in your MCO facility, all components should be tested, adjusted, and balanced to ensure that they are functioning as designed/engineered and are operating within system specifications. A system that is designed by the world's best engineers and installed by the most qualified company will still never function to optimum levels of efficiency unless the system is tested, adjusted, and balanced. This is generally accomplished by a certified contractor who specializes in this field of study. First, the systems are tested to check that the air balance of the system is functioning properly and within the design specifications relating to air flow, humidity control, temperatures, and static pressures. From this testing, results are prepared and provided to the Commissioning Agent and the facility owner. These reports are critical for establishing a baseline of operations for the original configuration, which can be referenced and tested against when any future adjustments or modifications are made to the HVAC system that might affect the air balance of the facility.

## Electrical Systems Testing Reports

As MCO installations have grown in scale and diversity, more focus has been placed on dedicated, detailed testing and analysis of electrical systems, both for system installations (including new builds, retrofits and upgrades) and as part of periodic system evaluations. When it comes to electrical systems—more so than for any other infrastructure system—there is no one-size-fits-all approach to this work, and as such, there are a few main types of studies that can be performed singularly or collectively (in varying degrees) to test the performance of your electrical system.

<i>Type of System Test</i>	<i>Description</i>
Short circuit studies	Short circuit studies are necessary to ensure that new equipment ratings are within specifications and are able to withstand the available short circuit energy at each point within an electrical system. This is vital as it relates to safety of personnel and operators of the equipment. These studies provide information that helps establish proper interrupting ratings of equipment protective devices, such as circuit breakers and fuses. If this test was not conducted properly or not conducted at all, the results of an electrical fault exceeding the ratings of the protective devices could cause injury or death to personnel and extensive equipment damage.



<i>Type of System Test</i>	<i>Description</i>
Breaker coordination studies	<p>In conjunction with the short circuit study, a breaker coordination study is used to analyze the tripping times for the series of overcurrent devices. This enables the selection of the proper overcurrent device that would function within the faulted circuit, without the fault affecting any of the other protective devices within the electrical system. The end result is that faults are caught (and breakers tripped) as close to the faulted load as possible. The focus of this test is to ensure that the electrical failure of one device in a system, such as an electrical motor, does not cause a catastrophic event by opening protective devices to other pieces of equipment within the system.</p>
Arc flash studies	<p>The purpose of an arc flash study is to determine the arc fault currents and arc flash hazards of each piece of equipment or system. These results will determine what type and caliber of personal protective equipment must be worn by personnel when working in or around the electrical equipment. The calculated arc flash value must be documented and each piece of equipment must be labeled appropriately, identifying the level of risk if an arc flash were to occur.</p>

# ACTIVITY 14-4

## Identifying Testing Reports and Their Purposes

### Scenario

In this activity, you will identify testing reports and their purposes within an MCO installation.

- 
- 1. After installation of HVAC systems within an MCO space, they should be tested by a certified technician to verify their performance against the intended design and the information should be provided to the facility owner and MCO staff to use as the criteria for optimal operations.**
    - True
    - False
  - 2. Which type of electrical system test ensures that protective devices have been installed in the appropriate location and are functioning properly in order to prevent a single fault from taking out the entire electrical system?**
    - Short circuit study
    - Breaker coordination study
    - Arc flash study
  - 3. Which type of electrical system test ensures that the electrical components and protective devices that have been installed meet all necessary ratings to withstand an electrical fault without putting personnel, equipment, or operations at risk?**
    - Short circuit study
    - Breaker coordination study
    - Arc flash study
  - 4. Which type of electrical system test ensures that all components have been analyzed for potential faults, these measurements have been documented, and the necessary PPE required to interact with them has been identified?**
    - Short circuit study
    - Breaker coordination study
    - Arc flash study
  - 5. Commissioning reports should be prepared by the various staff members or key stakeholder involved in the project that has the most experience and expertise with the specific system being referenced or the document being developed.**
    - True
    - False
-

## Summary

In this lesson, you identified and applied industry standards regarding facility and system documentation within a mission critical facility. As an MCO operator, it is your responsibility to operate and/or oversee the operations of the various components comprising your MCO infrastructure in a manner that is safe, consistent, and compliant with the standards laid out by certain regulatory organizations. With familiarity of the numerous types of facility and system documentation, you can help ensure that your MCO facility is always working under the most optimal conditions, in order to meet—and, hopefully, exceed!—the industry standards and expectations for MCO operations.



# Course Follow-Up

Congratulations! You have completed the *Certified Mission Critical Operator (CMCO)* course. You have successfully identified the basic components and systems of a typical MCO infrastructure; examined the proper design and configuration of critical infrastructure systems and spaces; and explored the strategies, techniques, and best practices for operating an MCO facility according to industry standards regarding safety, security, networking, communications, system monitoring, operating procedures, and documentation.

## What's Next?

You are encouraged to continue to explore the concepts covered in the *Certified Mission Critical Operator (CMCO)* course, in order to build upon and expand the knowledge you have gained regarding Mission Critical Operations. This includes—but is certainly not limited to—participating in relevant online communities, requesting additional resources from your instructor, and seeking out additional training opportunities and real-life applications to further hone and refine your expertise and experience.



# A

# Certified Mission Critical Operator (CMCO) Certification Exam MCO-001

The *Certified Mission Critical Operator* content addresses the Certified Mission Critical Operator (CMCO) Certification Exam knowledge, skills, and abilities. The following table indicates where the knowledge, skills, and abilities tested in the Certified Mission Critical Operator (CMCO) Certification Exam are covered in this course.

<b><i>Objective Domain</i></b>	<b><i>Covered In</i></b>
<b>1.0 Mission Critical Infrastructure</b>	
<b>1.1 Compare and contrast various types of HVAC systems.</b>	
1.1.1 Refrigerant-based cooling system	Lesson 4, Topic B
1.1.2 Water-based cooling system	Lesson 4, Topic C
1.1.3 Alternative technologies	Lesson 4, Topic D
1.1.4 100 percent (%) fresh air technology	Lesson 4, Topic E
1.1.5 Fan systems	Lesson 4, Topic E
1.1.6 Air handling unit	Lesson 4, Topic E
1.1.7 Terminal devices	Lesson 4, Topic E
<b>1.2 Summarize various power source technologies.</b>	
1.2.1 Utility	Lesson 2, Topic B
1.2.2 Generator	Lesson 2, Topic C
1.2.3 Uninterruptible Power Supply (UPS)	Lesson 2, Topic D
1.2.4 Battery	Lesson 2, Topic E
1.2.5 Alternative power sources	Lesson 2, Topic F
<b>1.3 Compare and contrast various power distribution concepts and equipment.</b>	

<b>Objective Domain</b>	<b>Covered In</b>
1.3.1 Level of redundancy	Lesson 3, Topic B
1.3.2 Dual cord	Lesson 3, Topic B
1.3.3 Close transition vs. open transition vs. soft loading	Lesson 3, Topic C
1.3.4 Tier level/Topology	Lesson 3, Topic D
1.3.5 Electrical protection	Lesson 3, Topic E
<b>1.4 Identify basic plumbing concepts and the relationship to core mechanical systems.</b>	
1.4.1 Water treatment	Lesson 5, Topic A
1.4.2 Humidification	Lesson 5, Topic B
1.4.3 Water source	Lesson 5, Topic A
1.4.4 Make up water	Lesson 5, Topic A
1.4.5 Water pumps/pressurization	Lesson 5, Topic A
1.4.6 Natural gas piping	Lesson 5, Topic B
1.4.7 Backflow preventer	Lesson 5, Topic A
1.4.8 Filtration	Lesson 5, Topic A
<b>1.5 Explain life safety system elements, their purposes and impact on normal operations.</b>	
1.5.1 Fire detection	Lesson 6, Topic A
1.5.2 Fire suppression	Lesson 6, Topic B
1.5.3 Fire-rated construction	Lesson 6, Topic C
1.5.4 Fire pump system	Lesson 6, Topic B
1.5.5 Emergency lighting	Lesson 6, Topic D
1.5.6 Emergency receptacle identification	Lesson 6, Topic B
1.5.7 Emergency Power Off (EPO)	Lesson 6, Topic E
<b>2.0 Safety, Security, and Emergency Response</b>	
<b>2.1 Given a scenario, implement proper safety techniques in a mission critical environment.</b>	
2.1.1 Personal Protective Equipment (PPE)	Lesson 7, Topic A
2.1.2 Lock out/Tag out	Lesson 7, Topic A
2.1.3 Barrier/boundaries	Lesson 7, Topic A
2.1.4 Machine guarding	Lesson 7, Topic A
2.1.5 Fall protection and arrest	Lesson 7, Topic A
2.1.6 Arc flash labels and hazard analysis	Lesson 7, Topic A



<b>Objective Domain</b>	<b>Covered In</b>
2.1.7 Global Harmonization System	Lesson 7, Topic A
2.1.8 Confined space access and ventilation	Lesson 7, Topic A
<b>2.2 Given a scenario, execute security methods and best practices.</b>	
2.2.1 Physical security	Lesson 8, Topic A
2.2.2 Access control systems	Lesson 8, Topic B
<b>2.3 Identify basic emergency response procedures.</b>	
2.3.1 Incident reporting	Lesson 7, Topic B
2.3.2 Call tree	Lesson 7, Topic B
2.3.3 Building or critical area emergency action plan	Lesson 7, Topic B
2.3.4 Hazardous material spill procedure	Lesson 7, Topic B
2.3.5 Severe event preparation and reporting	Lesson 7, Topic B
<b>3.0 Critical Production Space</b>	
<b>3.1 Explain the importance of common items and best practices that affect various critical environments.</b>	
3.1.1 Component redundancy within the critical space	Lesson 3, Topic B Lesson 9, Topic A
3.1.2 Raised access floor	Lesson 9, Topic A Lesson 9, Topic B
3.1.3 Rack layout/installation	Lesson 9, Topic A
3.1.4 Best practices	Lesson 1, Topic D Lesson 2, Topic A Lesson 3, Topic B Lesson 3, Topic C Lesson 9, Topic A Lesson 9, Topic B Lesson 9, Topic C Lesson 13, Topic C
3.1.5 Alternative technologies	Lesson 2, Topic A Lesson 2, Topic F Lesson 3, Topic A Lesson 4, Topic D
3.1.6 Grounding	Lesson 2, Topic A Lesson 3, Topic E Lesson 9, Topic A

<b>Objective Domain</b>	<b>Covered In</b>
<b>3.2 Explain air flow management techniques and strategies.</b>	
3.2.1 Computer room air conditioners/computer room air handler unit	Lesson 9, Topic B
3.2.2 In-row cooling	Lesson 9, Topic B
3.2.3 Containment	Lesson 6, Topic C Lesson 9, Topic B
3.2.4 Perforated tile placement	Lesson 9, Topic B
3.2.5 Tile removal limitations	Lesson 9, Topic B
3.2.6 Return air methodologies	Lesson 9, Topic B
3.2.7 Hot aisle/cold aisle	Lesson 9, Topic B
3.2.8 Thermal considerations	Lesson 9, Topic B
3.2.9 Temperature/pressure control strategies	Lesson 9, Topic B
<b>3.3 Summarize data cable management techniques and cable types.</b>	
3.3.1 Types	Lesson 9, Topic C
3.3.2 Labeling	Lesson 9, Topic C
3.3.3 Bend radius limitations	Lesson 9, Topic C
3.3.4 Cable segregation	Lesson 9, Topic C
3.3.5 Cable dressing and placement	Lesson 9, Topic C
3.3.6 Cable tracing and testing	Lesson 9, Topic C
<b>4.0 Facility and System Documentation</b>	
<b>4.1 Compare and contrast various types of record documentation ("as-built").</b>	
4.1.1 Single line diagram/One line diagram	Lesson 14, Topic A
4.1.2 Panel schedules	Lesson 14, Topic A
4.1.3 Submittals	Lesson 14, Topic A
4.1.4 Flow diagrams	Lesson 14, Topic A
4.1.5 Floor plans	Lesson 14, Topic A
4.1.6 Equipment layout plans	Lesson 14, Topic A
4.1.7 Equipment schedules	Lesson 14, Topic A
4.1.8 System architecture diagrams	Lesson 14, Topic A
4.1.9 Control diagrams	Lesson 14, Topic A
4.1.10 Design specifications	Lesson 14, Topic A

<b>Objective Domain</b>	<b>Covered In</b>
<b>4.2 Interpret and explain the contents of various operating and maintenance (O&amp;M) manuals and their associated purpose.</b>	
4.2.1 Shop drawings	Lesson 14, Topic B
4.2.2 Sequence of operations	Lesson 14, Topic B
4.2.3 Warranty information	Lesson 14, Topic B
4.2.4 Seasonal operations	Lesson 14, Topic B
4.2.5 Preventative maintenance procedures and schedules	Lesson 3, Topic F Lesson 4, Topic F Lesson 5, Topic C Lesson 6, Topic F Lesson 13, Topic B Lesson 14, Topic B
4.2.6 Maintenance procedures	Lesson 4, Topic F Lesson 5, Topic C Lesson 6, Topic F Lesson 13, Topic B Lesson 13, Topic C Lesson 14, Topic B
4.2.7 Troubleshooting procedures	Lesson 14, Topic A Lesson 14, Topic B
<b>4.3 Identify the contents and purpose of testing reports.</b>	
4.3.1 Commissioning reports	Lesson 14, Topic C
4.3.2 Short circuit, protective device coordination, arc flash study	Lesson 14, Topic C
4.3.3 Testing, adjusting and balancing reports	Lesson 4, Topic F Lesson 14, Topic C
<b>5.0 Networking and Communications</b>	
<b>5.1 Identify basic networking concepts.</b>	
5.1.1 Basic IP address concepts	Lesson 10, Topic B
5.1.2 Domain Name Service (DNS) concepts	Lesson 10, Topic B
5.1.3 Network types	Lesson 10, Topic C
<b>5.2 Identify essential networking structures and their purpose.</b>	
5.2.1 Components	Lesson 10, Topic A
5.2.2 Locations	Lesson 10, Topic A

<b>Objective Domain</b>	<b>Covered In</b>
<b>5.3 Identify various types of communications systems.</b>	
5.3.1 Wired systems	Lesson 10, Topic C Lesson 11, Topic A
5.3.2 Wireless systems	Lesson 10, Topic C Lesson 11, Topic B
<b>6.0 Real-Time Information Management</b>	
<b>6.1 Explain the fundamentals of environment and system monitoring.</b>	
6.1.1 Critical production environmental conditions	Lesson 9, Topic B Lesson 12, Topic A
6.1.2 Systems and equipment parameters	Lesson 12, Topic A
6.1.3 Metering	Lesson 3, Topic A Lesson 12, Topic B
<b>6.2 Identify common engineering units and conventions.</b>	
6.2.1 Power	Lesson 2, Topic A Lesson 9, Topic A Appendix B
6.2.2 Cooling and air flow	Lesson 4, Topic A Appendix B
6.2.3 General measurements	Lesson 4, Topic A Appendix B
<b>6.3 Explain common monitoring platforms and controls.</b>	
6.3.1 Platforms	Lesson 12, Topic C
6.3.2 Controls	Lesson 12, Topic E
6.3.3 Process control devices	Lesson 4, Topic C Lesson 12, Topic E
<b>6.4 Interpret output from system and monitoring reports and explain the overall impact of these reports on a mission critical environment.</b>	
6.4.1 Normal state vs. abnormal state	Lesson 12, Topic D
6.4.2 Alarm condition	Lesson 12, Topic D
6.4.3 Trending	Lesson 12, Topic D
6.4.4 Predictive results	Lesson 12, Topic D
6.4.5 Mitigate risks/failures	Lesson 12, Topic D

<b>Objective Domain</b>	<b>Covered In</b>
6.4.6 Integration of information across multiple systems to provide overall status	Lesson 12, Topic D
6.4.7 Effects of local failures on other mission critical systems	Lesson 2, Topic A Lesson 12, Topic D
6.4.8 Verify corrective actions	Lesson 12, Topic D Lesson 14, Topic C
<b>7.0 Operations and Procedures</b>	
<b>7.1 Given a scenario, execute proper change management procedures.</b>	
7.1.1 Restricted change periods/blackout dates	Lesson 13, Topic C
7.1.2 Maintenance windows	Lesson 13, Topic C
7.1.3 Switching windows/cutover windows	Lesson 13, Topic C
7.1.4 Methods of procedures	Lesson 13, Topic B Lesson 13, Topic C
7.1.5 Permit to work/End user approval	Lesson 13, Topic C
7.1.6 Hot work permit	Lesson 13, Topic C
7.1.7 Energized work	Lesson 13, Topic C
7.1.8 Double custody switching (e.g. two person rule)	Lesson 13, Topic C
7.1.9 Standard Operating Procedure (SOP), Emergency Operating Procedure (EOP), and Preventative Maintenance (PM)	Lesson 13, Topic B
<b>7.2 Explain common organizational structure concepts.</b>	
7.2.1 Chain of command	Lesson 13, Topic A
7.2.2 Escalation path	Lesson 13, Topic A
7.2.3 Organizational chart	Lesson 13, Topic A
7.2.4 Client-contractor relationships	Lesson 13, Topic A
7.2.5 Vendor management	Lesson 13, Topic A
<b>7.3 Explain the importance of security procedures.</b>	
7.3.1 Authorization procedures	Lesson 8, Topic C
7.3.2 Site access rules	Lesson 8, Topic C
7.3.3 Escorting vendors/visitors	Lesson 8, Topic C
7.3.4 Material shipping/receiving and inspection	Lesson 8, Topic C
7.3.5 Security patrolling/fire watch	Lesson 8, Topic C
7.3.6 Confidentiality policies	Lesson 8, Topic C

<b>Objective Domain</b>	<b>Covered In</b>
7.3.7 Sensitivity of equipment, information, and mission	Lesson 8, Topic C
7.3.8 Awareness of cyber security best practices	Lesson 8, Topic C
<b>7.4 Identify general and industry specific regulatory, standard and compliance organizations/associations.</b>	
7.4.1 Uptime Institute	Lesson 3, Topic D Lesson 13, Topic D
7.4.2 Occupational Safety and Health Administration (OSHA)	Lesson 13, Topic D
7.4.3 American Society of Heating, Refrigeration and Air Conditioning Engineers (ASHRAE)	Lesson 13, Topic D
7.4.4 American National Standards Institute (ANSI)	Lesson 13, Topic D
7.4.5 Telecommunications Industry Association (TIA)	Lesson 13, Topic D

---

# B

## Common Engineering Units and Conventions

It is highly recommended that you familiarize yourself with the following list of common engineering units and conventions, as you will need to know them for the day-to-day operations of various MCO components and systems.

<i>Measurement/Quantity</i>	<i>Unit</i>	<i>Unit Symbol</i>
Voltage	Volts	V
Current	Amperes	A
Frequency	Hertz	Hz
Resistance	Ohms	$\Omega$
Capacitance	Farads	F
Apparent Power/Potential Power	Kilovolt-Ampere	kVA
Electrical Charge	Coulombs	C
Electrical Power	Watts	W
	Kilowatts	kW
Work (Transfer of Energy)	Joules	J
Force	Newtons	N
Heat	British Thermal Units	BTU
Temperature	Fahrenheit	$^{\circ}\text{F}$
	Celsius	$^{\circ}\text{C}$
	Kelvin	K
Mass	Kilogram	kg
	Ton	t
Weight Load (Linear Mass Density)	Pounds per Square Foot	PSF
	Pounds per Linear Foot	PLF
Fluid Pressure	Pounds per Square Inch	PSI
Volume	Cubic Feet per Minute	CFM
Flow Rate	Gallons per Minute	GPM
	Liters per Minute	LPM

<i>Measurement/Quantity</i>	<i>Unit</i>	<i>Unit Symbol</i>
Light	Lumens	lm
	Candelas	cd
Sound/Noise	Decibels	dB



# C

# Uptime Institute Tier Classifications

In this appendix, you will find the description of the Uptime Institute's tier classification system, reprinted here in full with permission from the Uptime Institute.

## What is the Uptime Institute Tier Classification system?

Uptime Institute created the standard Tier Classification System to consistently evaluate various data center facilities in terms of potential site infrastructure performance, or uptime. The Tiers (I-IV) are progressive; each Tier incorporates the requirements of all the lower Tiers.

### Tier I: Basic Capacity

A Tier I data center provides dedicated site infrastructure to support information technology beyond an office setting. Tier I infrastructure includes a dedicated space for IT systems; an uninterruptible power supply (UPS) to filter power spikes, sags, and momentary outages; dedicated cooling equipment that won't get shut down at the end of normal office hours; and an engine generator to protect IT functions from extended power outages.

### Tier II: Redundant Capacity Components

Tier II facilities include redundant critical power and cooling components to provide select maintenance opportunities and an increased margin of safety against IT process disruptions that would result from site infrastructure equipment failures. The redundant components include power and cooling equipment such as UPS modules, chillers or pumps, and engine generators.

### Tier III: Concurrently Maintainable

A Tier III data center requires no shutdowns for equipment replacement and maintenance. A redundant delivery path for power and cooling is added to the redundant critical components of Tier II so that each and every component needed to support the IT processing environment can be shut down and maintained without impact on the IT operation.

### Tier IV: Fault Tolerance

Tier IV site infrastructure builds on Tier III, adding the concept of Fault Tolerance to the site infrastructure topology. Fault Tolerance means that when individual equipment failures or distribution path interruptions occur, the effects of the events are stopped short of the IT operations.

Data center infrastructure costs and operational complexities increase with Tier Level, and it is up to the data center owner to determine the Tier Level that fits his or her business's need. A Tier IV solution is not "better" than a Tier II solution. The data center

infrastructure needs to match the business application, otherwise companies can overinvest or take on too much risk.

Uptime Institute recognizes that many data center designs are custom endeavors, with complex design elements and multiple technology choices. As such, the Tier Classification System does not prescribe specific technology or design criteria beyond those stated above. It is up to the data center owner to meet those criteria in a method that fits his or her infrastructure goals.

### **What is Tier Certification?**

The Tier Certification process typically starts with a company deploying new data center capacity. The data center owner defines a need to achieve a specific Tier Level to match a business demand.

Data center owners turn to Uptime Institute for an unbiased, vendor neutral benchmarking system, to ensure that data center designers, contractors and service providers are delivering against their requirements and expectations.

Tier Certification is a performance based evaluation of a data center's specific infrastructure, and not a checklist or cookbook. Uptime Institute is the only organization permitted to Certify data centers against the Tier Classification System. Uptime Institute does not design, build or operate data centers. Our only role is to evaluate site infrastructure, operations and strategy.

The first step in a Tier Certification process is a Tier Certification of Design Documents (TCDD). Uptime Institute Consultants review 100% of the design documents, ensuring each subsystem among electrical, mechanical, monitoring, and automation meet the fundamental concepts and there are no weak links in the chain. Uptime Institute then provides a report to the owner with the Tier deficiencies. Uptime Institute conducts a compliance review of the revised drawings, and then awards a TCDD letter and foil if the design meets the criteria.

The TCDD is not the final stage in a certification process, but rather a checkpoint for companies to demonstrate that the first portion of the capital project met requirements. All Tier Certification of Design Documents awards issued after 1 January 2014 expire two years after the award date.

Data center owners use the Tier Certification process to hold the project teams accountable, and to ensure that the site performs as it was designed. Which brings us to the next phase in a Tier Certification process: Tier Certification of Constructed Facility (TCCF).

During a TCCF, a team of Uptime Institute consultants conducts a site visit, identifying discrepancies between the design drawings and installed equipment. Our consultants observe tests and demonstrations to prove Tier compliance. Fundamentally, this is the value of the Tier Certification, finding these blind spots and weak points in the chain. When the data center owner addresses the deficiencies, Uptime Institute awards the TCCF letter, foil and plaque.

# D

# Certified Mission Critical Operator (CMCO) Certification Exam Acronym List

It is highly recommended that you familiarize yourself with the following list of acronyms in preparation for taking the Certified Mission Critical Operator (CMCO) Certification Exam. The entries in this table represent the acronyms as they will appear on the exam.

<i>Acronym</i>	<i>Definition</i>
AC	Alternating Current
AHJ	Authority Having Jurisdiction
AHU	Air Handling Unit
ANSI	American National Standards Institute
ASHRAE	American Society of Heating, Refrigeration, and Air Conditioning Engineers
ATS	Automatic Transfer Switch
BAS	Building Automation System
BMS	Building Management System
BTU	British Thermal Unit
CAT3	Category 3
CAT5e	Category 5e
Cat6a	Category 6a
CDU	Cabinet Distribution Unit/Cooling Distribution Unit
CFM	Cubic Feet per Minute
COAX	Coaxial
CRAC	Computer Room Air Conditioner
CRAH	Computer Room Air Handler
DAS	Distributed Antenna System
DC	Direct Current

<b>Acronym</b>	<b>Definition</b>
DCIE	Data Center Infrastructure Efficiency
DDC	Direct Digital Control
DNS	Domain Naming Service
DRUPS	Diesel Rotary UPS
DX	Direct Expansion
EOP	Emergency Operating Procedure
EPA	Environmental Protection Agency
EPMS	Electrical Power Monitoring System
EPO	Emergency Power Off
FACP	Fire Alarm Control Panel
FERC	Federal Energy Regulatory Commission
FPTU	Fan Powered Terminal Units
GHS	Global Harmonization System
GPM	Gallons per Minute
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HMI	Human Machine Interface
HSSD	High Sensitivity Smoke Detection
HVAC	Heating, Ventilation, and Air Conditioning
Hz	Hertz
IAQ	Indoor Air Quality
ICC	International Code Council
IDF	Intermediate Distribution Frame
IP	Internet Protocol
ISA	International Society of Automation
ISO	International Standards Organization
ITIL	Information Technology Infrastructure Library
KWH	Kilowatt-Hour
kVA	Kilovolt-Ampere
KVAR	Kilovolt-Ampere Reactive
KW	Kilowatt
LAN	Local Area Network
LEED	Leadership in Energy and Environmental Design
LOTO	Lock Out/Tag Out
LPM	Liters per Minute
MDF	Main Distribution Frame

<b>Acronym</b>	<b>Definition</b>
MOP	Method of Procedure
MSDS	Materials Safety Data Sheet
MTS	Manual Transfer Switch
NDA	Non-Disclosure Agreement
NEC	National Electrical Code
NERC	North American Electric Reliability Corporation
NETA	InterNational Electrical Testing Association
NFPA	National Fire Protection Association
NiCad	Nickel Cadmium
O&M	Operations and Maintenance
OSHA	Occupational Safety and Health Administration
P&ID	Process and Instrumentation Diagram
PBX	Private Branch Exchange
PDU	Power Distribution Unit
PLC	Programmable Logic Controller
PM	Preventative Maintenance
POTS	Plain Old Telephone Service
PPE	Personal Protective Equipment
PSI	Pounds per Square Inch
PUE	Power Usage Effectiveness
RPP	Remote Power Panel
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SCSI	Small Computer System Interface
SDS	Safety Data Sheet
SOP	Standard Operating Procedure
STS	Static Transfer Switch
TIA	Telecommunications Industry Association
TVSS	Transient Voltage Surge Suppressor
TXV	Thermal Expansion Valve
UPS	Uninterruptible Power Supply
USGBC	United States Green Building Council
VAV	Variable Air Volume
VFD	Variable Frequency Drive
VRLA	Valve Regulated Lead Acid
WAP	Wireless Access Point

<b>Acronym</b>	<b>Definition</b>
Wi-Fi	Wireless Fidelity

# E

## Additional Resources

The following resources can provide additional information that may be useful to your training for the Certified Mission Critical Operator Certification Exam and to supplement your knowledge about Mission Critical Operations in general.

- The National Consortium for Mission Critical Operations (<http://ncmco.us/>)
- Information regarding Critical Infrastructure from the Department of Homeland Security:
  - What is Critical Infrastructure? (<http://www.dhs.gov/what-critical-infrastructure>)
  - Critical Infrastructure Resources (<http://www.dhs.gov/critical-infrastructure-resources>)
  - Critical Infrastructure Training (<http://www.dhs.gov/critical-infrastructure-training>)
- National Disaster data:
  - Earthquake data via the USGS (<http://earthquake.usgs.gov/hazards/designmaps/usdesign.php>)
  - Hurricane data via the NOAA (<http://www.nhc.noaa.gov/>)
  - Flood zone data via FEMA (<https://www.fema.gov/flood-zone>)
  - Tornado data via the NOAA (<http://www.ncdc.noaa.gov/climate-information/extreme-events/us-tornado-climatology>)
- MCO-related and/or relevant information from the Federal Emergency Management Agency (FEMA):
  - National Preparedness information (<http://www.fema.gov/national-preparedness>)
  - Preparedness Grants (<http://www.fema.gov/preparedness-non-disaster-grants>)
  - Authorized Equipment List (<http://www.fema.gov/authorized-equipment-list>)
  - Hazard Mitigation Assistance (<http://www.fema.gov/hazard-mitigation-assistance>)
- Information about energy sources and energy usage:
  - The U.S. Department of Energy (<http://www.energy.gov/>)
  - The U.S. Energy Information Administration (<http://www.eia.gov/>)
- Emergency Response resources:
  - FEMA Incident Action Planning Guide (<https://www.fema.gov/media-library/assets/documents/25028>)
  - National Incident Management System/National Preparedness System (<https://www.fema.gov/national-incident-management-system>)
  - Department of Homeland Security Incident Reporting (<http://www.dhs.gov/report-incidents>)
- Official websites of all MCO-related regulatory organizations:
  - Leadership in Energy and Environmental (LEED) (<http://www.usgbc.org/leed>)
  - Uptime Institute (<https://uptimeinstitute.com/>)
  - American National Standards Institute (ANSI) (<http://www.ansi.org/>)
  - American Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE) (<https://www.asbrae.org/>)
  - InterNational Electrical Testing Association (NETA) (<http://www.netaworld.org/>)

- Telecommunications Industry Association (TIA) (<http://www.tiaonline.org/>)
- Occupational Health and Safety Administration (OSHA) (<https://www.osha.gov/>)
- National Fire Protection Association (NFPA) (<http://www.nfpa.org/>)



# Glossary

## **abnormal state**

Anything other than the regular or expected condition of a component.

## **AC**

(alternating current) A flow of electrical charge that periodically reverses the direction in which it flows.

## **access prevention**

A physical security component that is used to physically control and monitor traffic flow within certain points of the secured facility.

## **AHJ**

(Authority Having Jurisdiction) An individual or organization that has statutory or regulatory responsibility for upholding and enforcing certain standards regarding the safe construction and operation of a facility.

## **air conditioning**

The management of the ambient conditions being delivered to a space, including controlling humidity levels and cooling air temperatures, for either people comfort or equipment operations.

## **air filter**

A device that contains some sort of material, through which a liquid or gas is passed in order to remove impurities.

## **air handling unit**

A collection of devices that drive the flow of conditioned air in HVAC systems,

typically including a blower, heating and cooling elements, sound attenuators, filters, dampers, humidifiers, and other equipment involved with air flow.

## **air-cooled chiller**

A type of cooling device that removes heat from water and conducts it to the atmospheric air as the final stage in the heat rejection/cooling process.

## **air-side economization**

An energy efficient cooling process that uses supply and exhaust fan systems to circulate outside air through a facility for critical space cooling.

## **AR unit**

(air rotation unit) A type of air handler that pulls the return air in at floor level using continuously running fans, and then directs that air back into the space, typically near the ceiling, to maintain a constant temperature in the space.

## **arc fault potential**

The calculated maximum amount of energy that may be released by a fault in a particular piece of equipment, taking into consideration any protective features in place.

## **arc flash**

An explosion of heat, light, molten metal, and plasma that results when an electrical connection is made with very little resistance.

**as-built drawing**

A version of the construction documents that has been marked up or "red-lined" during construction to reflect any changes or substitutions made as a result of the actual conditions of the space.

**ATS**

(automatic transfer switch) A device that connects to and monitors a system's primary and alternate source of power, and automatically switches between the two to maintain a consistent, stable flow of electricity at the voltage needed to handle the system's load.

**backflow prevention**

The protective devices installed in a plumbing system that fully segregate the operational systems from the supply, in order to prevent any sort of backwards or upstream contamination of the water supply.

**barrier**

Any device or structure that creates an impediment to entrance, passage, or movement forward within a specific space or location.

**BAS**

(Building Automation System) A monitoring system that monitors and controls the various critical systems or components, including HVAC, power, fire, and security. Also known as a Building Management System (BMS).

**battery**

A device that converts stored chemical energy into electricity via a process in which free electrons move between a positively charged terminal (cathode) and a negatively charged terminal (anode) through a solution (electrolyte) within a single container (cell).

**battery system**

A set, or sets, of individual battery cells wired together in strings.

**bend radius**

The measurement of the minimum amount that a cable can be bent without causing unwanted negative effects.

**biohazard**

Any biological substance that can cause harm to personnel and/or the environment.

**biomass**

Renewable, organic materials that can be treated in some manner and burned for fuel, the heat from which is generally used to drive steam or gas turbines to create electricity.

**biometrics**

A specific kind of access control system that uses the unique biological "signatures" of individual people (such as fingerprints, palm prints, iris scans, voice recognition, etc.) to restrict or grant access to protected spaces and/or information.

**blackout date**

A period of time during which any changes made to systems or processes would have too great of an impact on business operations and therefore should be avoided. Also known as a restricted change period.

**blower**

A mechanical device used to move air or gases.

**BMN**

(Building Management Network) The collection of inter-networked systems that manage automated processes necessary for the efficient utilization of building resources.

**BMS**

(Building Management System) A monitoring system that monitors and controls the various critical systems or components, including HVAC, power, fire, and security. Also known as a Building Automation System (BAS).

**BoD**

(Basis of Design) The first iteration of the design of a facility or project, which explains the operational expectations and limits of the installation at a very high level.

**bridging**

The practice of installing angled covers over cabling or other components running across floors to allow for equipment movement and to eliminate trip hazards.

**cable dressing**

The practice of arranging adjacent cabling in an organized, orderly manner.

**cable tracing and testing**

The variety of techniques (based on cable type) used to validate the signal strength, quality, or pathway of installed cabling.

**capacitance**

The ability to store some amount of charge, measured in farads.

**capacitor**

An energy storage device that can store very small amounts of electric potential.

**cellular**

A wireless communication system that transmits voice data over mobile phones, using cellular towers to create a broad signal distribution network.

**chain of command**

A reporting relationship hierarchy in which information and reporting is relayed and escalated from the upper levels of personnel to the lower levels, and conversely, from the lower levels to the upper levels.

**chiller**

A cooling device that removes heat from water through a vapor-compression or absorption cycle, which is then typically piped into buildings and passed through heat exchange systems in order to cool air or other equipment.

**clean agent system**

Type of fire suppression system that operates by dispersing some type of inert gas

throughout the space affected by the fire and removes the oxidizing agent element of the fire triangle. Also known as a gaseous suppression system.

**client**

A device that utilizes a network's resources or functions for the purpose of completing a task.

**co-generated power**

An alternative power source in which a fuel source is used to create steam for turbine generators and the leftover heat is extracted from the exhausted waste steam and is used to provide power for other central services.

**coaxial cable**

A type of cable that consists of a single inner conductor that is surrounded by a tubular insulated layer, which is then surrounded by a tubular conductive layer, all of which is surrounded by an insulated outer shield.

**communication room**

A centrally located room with enhanced power and cooling capabilities utilized for the setup and storage of network communication equipment.

**compliance**

The act of following the rules established by a regulation, standard, or guideline.

**computer network**

Any configuration of two or more computers or other electronic devices that are connected together for the implicit function of exchanging data between them.

**conditioned space**

Any (at least partially) segregated space that requires control over its atmospheric conditions such as air temperature, humidity level, pressure, etc.

**confidentiality**

The implicit or explicit promise that certain types of information will be protected from unauthorized access and will not be viewed or shared inappropriately.

**confined space**

Any area that has limited or challenging entry and egress paths and/or poor ventilation due to lack of clean air supply or buildup of harmful gasses.

**containment**

An umbrella term referring to any component or device used to prevent or mitigate the spread of fire and/or smoke.

**control diagram**

A simple illustration—usually a block diagram—that shows the hierarchy of control panels and the devices that they monitor and/or control.

**controls**

The systems that monitor, report, and manipulate site equipment and networks.

**cooling element**

A set of coils or vanes through which the cooling medium flows to remove heat from the air.

**cooling tower**

A cooling device that uses evaporation to remove the heat from water within a confined space, and releases the excess heat as evaporate directly into the atmosphere.

**corrosion**

The natural, gradual breakdown and destruction of materials caused by a chemical reaction within the environment, usually oxidation.

**CRAC**

(Computer Room Air Conditioner) A device that directly performs the heat transfer functions to cool the supply air in a data center.

**CRAH**

(Computer Room Air Handler) A device that moves air across a cooling mechanism, usually chilled water cooling coils, in order to cool the supply air in a data center.

**crisis**

An event or occurrence, typically happening abruptly or with little or no warning, that has

the potential to result in an unstable or dangerous environment.

**crisis management**

The planning and monitoring for, and the immediate response to, any potential threats to a system or facility.

**critical infrastructure**

The physical systems that allow an organization to fulfill its purpose in delivering an important product or service.

**CTTS**

(closed transition transfer switch) A type of transfer switch that uses logic technology to determine if the sources meet the same criteria for voltage, frequency, and phase relationship and, if they do, closes the contacts with a slight overlap to prevent any interruption.

**current**

The flow of electric charge in a circuit.

**cutover window**

A period of time during which a transition is taking place between the utilization of an old system or component and the new system or component that is replacing it.

**damper**

A valve or plate that stops or regulates the flow of air inside of air handling equipment in order to regulate room temperature and/or control other climate conditions.

**dashboarding**

The practice of compiling large amounts of operational data into concise text or graphical outputs that provide quick glances at the overall status of mission critical infrastructure and production.

**data packet**

A segment of data that is utilized for communication between two networked devices.

**DC**

(direct current) A constant flow of electricity that travels in one direction.

**DCIE**

(Data Center Infrastructure Efficiency) The ratio of power consumed by the critical load of the data center to the power consumed by the total critical infrastructure.

**delta conversion UPS**

A type of uninterruptible power supply that uses an inverter in the supply line to provide power for the load and a converter in the transformer to regulate the input current and power, and deliver power to the inverter output.

**demarcation point**

(demarc) The location within or on a building where the service provider's wiring ends and the internal building wiring begins.

**design specifications**

Documentation that details each and every system and piece of equipment required for a project, including specific characteristics and important associated information (such as required resources) to establish criteria that will need to be met during development and construction.

**deterrent**

A physical security component that is used to physically or psychologically demonstrate that an attempt to breach security will be difficult or even impossible.

**dew point**

The equilibrium temperature at which water vapor is absorbed by and condensed from the air at the same rate.

**diesel rotary UPS**

A type of uninterruptible power supply that combines a typical battery-powered or flywheel-powered UPS with a diesel engine to supply backup power.

**distribution frame**

A centralized point in the network where a larger circuit is broken down into smaller user specific connections.

**distribution redundancy**

The practice of overlapping, interlacing, or otherwise mixing up distinct power supply

paths to critical equipment throughout the data center in order to vary the diversity of power supply sources to the greatest extent possible.

**DNS**

(Domain Name System) A hierarchical system by which domain names are translated into IP addresses.

**DOAS**

(dedicated outdoor air system) A type of HVAC system that consists of two parallel systems: a dedicated outdoor ventilation system for latent loads and a parallel system for sensible loads.

**documentation**

A collection of documents that are relevant to a specific topic.

**domain name**

The unique label assigned to a network resource that identifies the administrative authority, or domain, to which that resource belongs.

**double conversion UPS**

A type of uninterruptible power supply that converts all AC power to DC power, some of which is utilized for battery charging, while the rest is simply converted back to AC power to provide power to the critical load.

**double custody switching**

The practice of requiring that two trained operators perform any work on major or high-energy equipment: one to read the procedure and verify the proper operation of the gear, and one to perform the required actions and safely operate the gear being worked on. Also known as the two-person rule.

**drainage**

The collection of components that remove the surplus water or effluent from the plumbing system in a facility.

**dry-bulb temperature**

The measurement of changes in sensible heat in the form of temperature, as read by a thermometer exposed to the air, without taking into account the amount of moisture in the air.

**dual-cord supply**

A type of power scheme designed for component-level redundancy, where an electrical component or equipment is plugged in twice.

**duct banks**

A collection of conduits or pipes through which the networking cables are passed and distributed in order to provide protection from the environment.

**ductwork**

The system of pipes or tubes that transport and deliver conditioned air throughout a facility.

**DX**

(direct expansion) A type of cooling system that directly cools the supply air to an occupied space via a refrigerant that absorbs the heat directly from the air.

**efficiency**

The ability to deliver the same desired critical operations while using less energy, incurring lower costs, and/or requiring less involvement or maintenance by specialized technicians.

**effluent**

Liquid waste or sewage (often called blackwater).

**egress route**

The escape path from individual spaces within the facility or from the entire facility in general to a safe location in the event of an emergency, such as a fire.

**electricity**

A form of energy resulting from either the static accumulation of charged particles or the flow of charged particles.

**energized work**

Any repair and maintenance activities that involve electrical work on circuits that cannot be fully de-energized, and therefore pose a risk to those performing the work.

**entropy**

The molecular disorder or randomness of matter.

**EOP**

(emergency operating procedure) A plan comprised of specific actions to be conducted in a particular order and manner in response to an emergency event or situation.

**EPMS**

(Electrical Power Monitoring System) A monitoring system that monitors power quality and consumption at various system or component levels.

**EPO**

(Emergency Power Off) A single source of action (such as a button, switch, command, or other automatic safety feature) that instantly kills all power to a facility or subset of its infrastructure.

**equipment schedule**

A systematic itemization of critical equipment within a system or space.

**escalation path**

The explicitly defined order in which information is passed, support is enlisted, approval is gained, etc., along the hierarchical levels of the organization, as depicted in the chain of command.

**evaporative cooling**

A cooling system that reduces temperature by removing the latent heat from an object by using the evaporation of a liquid coolant, typically water.

**exhaust system**

A mechanical discharge system where the air is removed from a building and discharged outside the building at a specific location or to a specific distance where it cannot again be readily drawn back in by the ventilation system.

**fan system**

A broad category of equipment that is used to circulate air throughout an infrastructure.

**fiber optic cable**

A type of cable that consists of optical fibers that are surrounded by glass or plastic strands, which is then surrounded by extra fiber strands or wraps, all of which is surrounded by a protective outer shield.

**fire alarm**

The system of devices designed to alert facility occupants of hazardous conditions in the event of smoke and/or fire.

**fire detection**

Sensing the presence of one or more of the by-products that result from a fire, including smoke, heat, infrared or ultraviolet light, and gas.

**fire pump system**

Water pumps dedicated solely to a fire suppression system that are designed to help move water to the sprinkler system devices at the location of the fire.

**fire suppression**

The act of removing one or more of the elements from the fire triangle in order to control and extinguish the source of a fire.

**fire triangle**

A simple, visual representation of the three elements required for fire: heat, a fuel source, and an oxidizing agent.

**fire watch**

A member of MCO personnel assigned to a system, space, or specific facility for a prescribed period of time to physically observe for and report signs of fire while hot work or fire systems maintenance is being performed.

**firestop**

The fire protection system created by sealing off the openings or joints around penetrations and penetrants with fire-resistant materials to prevent fire from spreading through the openings.

**firewall**

A building wall that may or may not be load-bearing for structural support and serves the primary purpose of preventing the spread of fire.

**flow**

The volume of a fluid moving past or through a fixed point over a given period of time.

**flow diagram**

A simplified drawing that shows the directional relationships between things and/or processes. Also known as block and arrow diagrams.

**fluid**

A substance that does not have a stable shape, flows with ease (relative to the surrounding environment), and is susceptible to external pressure changes; specific to MCOs, the substance is typically either a liquid or a gas.

**flywheel**

A mechanical-type storage device that stores energy kinetically by rotating a mass around an axis.

**foam system**

Type of fire suppression system that operates by dispensing a foamed fire suppressant liquid that reduces the fire's heat and coats the fuel to prevent it from coming into contact with the oxidizing agent.

**FQDN**

(Fully Qualified Domain Name) The host name combined with the host's domain name.

**free-air cooling**

A cooling system that uses the natural circulation of outside air only to provide cool air to a facility, without the addition of supplemental air-conditioning equipment or fan-driven air circulation equipment.

**frequency**

The rate at which AC voltage cycles from its positive peak, to zero, to its negative peak, and back again.

**fuel cell**

A type of alternative energy source and storage that converts stored chemical energy into electricity using a chemical reaction between positively charged ions and an oxidizing agent.

**gateway**

A device utilized for connecting two or more networks utilizing different communication protocols.

**generator**

A machine used to convert mechanical energy of some kind into electrical energy.

**geothermal cooling**

A cooling system that moves warm air or water into the ground and uses the earth as the heat sink to absorb rejected heat, and then delivers cooled air or water to the surface for use in the critical space.

**geothermal power**

An alternative power source in which the natural thermal energy generated and stored in the earth is used as a heat source to warm air or water, or as a power source to heat engines that in turn generate moderate amounts of electricity.

**GHS**

(Globally Harmonized System of Classification and Labelling of Chemicals) A standardized system for classifying and labelling chemicals, that is used globally and across industries and manufacturers.

**graywater**

The relatively clean wastewater generated from sinks, showers/baths, dishwashers, washing machines, and other household or building uses.

**grid**

The collective system of transmission lines, switching and substations involved in providing utility power.

**grounding**

The process of removing excess electrical charge and distributing it to a larger body capable of receiving that charge.

**guidelines**

Non-mandatory protocols, typically developed internally, that establish best practices for actions, which are not enforceable by any authority and do not carry consequences for non-compliance.

**HACA**

(Hot Aisle/Cold Aisle) An air flow technique that physically separates the supply air (cold aisle) from the exhaust or return air (hot aisle)

for the equipment in the data center, via various containment strategies such as panels or curtains.

**hazard analysis**

The general process of evaluating the environment, facility, and systems for safety risks to the general infrastructure and the personnel occupying the spaces within it.

**hazardous material**

Any substance that can be harmful to people and/or the environment. Often referred to simply as "hazmat."

**heat**

The transfer of energy, separate from work-related transfer, between two or more items or collections of items.

**heat exchanger**

A cooling device that allows heat from a fluid to pass to a second fluid without the two fluids coming into contact.

**heat recovery system**

A collection of equipment that recycles the waste heat that is a by-product from the operation of equipment or machinery and uses it in another process, such as heating water or air.

**heating**

In general, the warming of air or water for either people comfort or for maintaining the necessary conditions for the proper operation of critical equipment or systems.

**heating element**

A coil or other arrangement of wires in which heat is produced by an electric current.

**high voltage**

Equipment or systems that operate between 1 kilovolt and 15 kilovolts.

**host name**

A unique alphanumeric identifier, up to 255 characters long, that is assigned to a device or node within a network for the purpose of communication.



**HOSTS file**

A plain text file, containing a list of IP addresses and their related host names, that is utilized by devices to resolve a host name to an IP address.

**hot work permit**

A work permit specific to repair or maintenance activities that involve open flames, create sparks, or otherwise introduce acute fire hazards. The permit details the specific work activity, location, date and time, duration, involved equipment and personnel, the responsible party, and required fire protection actions.

**humidity**

The liquid moisture content suspended in a gas; most commonly, the concentration of water molecules in the air.

**HVAC**

(heating, ventilation, and air conditioning) The collective term for the set of systems and equipment that provide the heating, ventilation, and air-conditioning services for a facility.

**IAP**

(Incident Action Plan) An action plan, unique to a specific site and its operational purposes, that describes the procedures that should be followed during or after any event that has the potential for disrupting the normal operations of a facility.

**in-row cooling**

An air cooling technique in which a cooling unit that is inserted within a cabinet, between cabinets, or mounted to the top or bottom of a cabinet in order to deliver cool air directly to a specific location within a data center row.

**inch of water column**

An English (non-SI) unit of pressure that represents the pressure exerted by a column of water that is one inch in height under certain pre-defined conditions.

**incident**

Any occurrence, natural or man-made, that may cause harm and might require action to

maintain functional operations and protect life and/or property.

**incident report**

An official account describing the particular details of an emergency event or occurrence, including all pertinent facts about the occurrence, the sequence of events, and recommendations for immediate and long-term corrective actions to prevent the event from happening again.

**interlock**

A device or controls function, consisting of two circuit breakers that are interlocked so that only one can close at a time; prevents a component from causing damage to itself or the system by stopping during a power outage.

**Internet**

The global network of LAN networks utilizing the Internet Protocol suite of communications protocols to transfer packet switched data over public circuits.

**inverter**

An electrical device that converts DC power to AC power, by slicing varying voltages within the DC current into “steps” that cyclically decrease and increase to create the peaks and valleys of an AC sine wave.

**IP**

(Internet Protocol) The communication protocol utilized by all networked devices, by which data packets are structured, addressed, and transmitted.

**IP address**

A unique numerical label assigned to individual devices that are a part of a TCP/IP network, through which data can be transmitted and received over a network.

**IT**

(Information Technology) The broad application of computer devices and other communications equipment that are used to deliver, receive, and store data or other types of information.

**keypad**

A digital or mechanical lock set that operates by entering an alphanumeric code to unlock the mechanism and access a secured space.

**kilowatt**

The more commonly used measurement of electrical power, equal to one thousand watts.

**kilowatt hour**

The unit of measurement for the amount of power exerted or consumed by a system over an extended period of time.

**KVA**

(kilovolt-ampere) The unit of measurement for the amount of apparent power, or the potential power, available in an ideal system with no losses.

**LAN**

(Local Area Network) A self-contained network formed by a collection of interconnected devices in the same geographical (or "local") location.

**latent heat**

The heat energy added or removed from a substance during a change in state of the substance.

**LBS**

(Load Bus Synchronization) An engineering method to keep the output of two independent UPSs in sync, even if they are operating from two different sources of supplied power.

**lead acid battery**

A type of battery in which the positive terminal is made of lead-oxide ( $\text{PbO}_2$ ), the negative terminal is made of lead (Pb), and the electrolyte solution is some concentration of sulfuric-acid ( $\text{H}_2\text{SO}_4$ ); then, the chemical reaction amongst the three creates the voltage.

**line interactive UPS**

A type of uninterruptible power supply that combines the inverter and charger in the power supply line to supply both the AC power and the backup battery power and regulates its output voltage using a transformer or "buck-boost" circuit.

**lithium-ion battery**

A type of battery in which the positive terminal is made of a lithium oxide material, the negative terminal is typically made of a carbon-based material, and the electrolyte is a liquid comprised of lithium salts and an organic solvent; then, positively charged lithium ions are shared back and forth between the terminals in order to create voltage.

**load shedding**

The practice of simultaneously or sequentially de-energizing certain non-critical loads during utility events in order to conserve emergency power sources.

**loading**

The weight limits of a flooring system, based on the amount of weight that can safely rest on the stanchions and tiles.

**LOTO**

(Lock Out/Tag Out) The practice of physically securing a source of energy with a latch, hasp, chain, or other kind of locking mechanism and noting the danger to equipment and personnel if operated with some sort of tag or label.

**low voltage**

Equipment or systems that operate using 100 volts or less.

**maintenance window**

A pre-established period of time during which change-controlled work is regularly allowed to take place.

**makeup water**

Water that is supplied for equipment that consumes water in some form, whether through discharge, evaporation, flushing, etc.

**manhole**

The access point where communication equipment and cables from the service provider are located and can be accessed outside of the building.

**MCOs**

(Mission Critical Operations) The actions, processes, or systems that enable the execution of the integral functions of a business or organization.

**medium voltage**

Equipment or systems that operate between 110 volts and 1 kilovolt.

**metering**

The measurement of available data points related to the performance of critical infrastructure systems and equipment, specifically about how power, water, gas, and other resources are being used by the facility.

**microgrid**

A small-scale, localized utility-source system that can disconnect from the larger, more traditional utility-source grid and operate autonomously, providing its own generation, storage, and transmission of electrical energy.

**microwaves**

A wireless communication signal that operates at the higher end of the electromagnetic spectrum, at generally high frequencies, and in a focused "beam" pattern.

**mission critical mindset**

The desirable disposition of a Mission Critical Operator, which includes a broad understanding of systems integration and a constant awareness of the interconnectedness of each component within the mission critical system.

**MSDS**

(Material Safety Data Sheets) A document that provides important information about a chemical and how to safely handle and/or work with that chemical, which follows the previous standard for classifying and labelling chemical-based materials (prior to the implementation of GHS and its standardized Safety Data Sheets).

**network address**

The unique identifier given to a device that allows it to be identified within a network.

**network coverage area**

The area within which a connection to a LAN or WAN can be obtained.

**network name**

A string of characters utilized to uniquely identify a specific network and the nodes contained within it.

**networking**

The system of computers and other assorted hardware and software components that are connected together to allow for the communication of data and information between devices.

**NIC**

(network interface controller) A device that connects computers or other devices to the network. (Also called a network interface card or network adapter.)

**nickel cadmium battery**

A type of battery in which the positive terminal is made of a cadmium material, the negative terminal is made of a nickel oxide material, and the electrolyte is an alkaline; then, a chemical reaction between the materials of the two terminals only create voltage.

**normal state**

The regular or expected condition of a component.

**nuclear material**

Any substance that possesses radioactive properties or fissionable properties to sustain the chain reaction that creates energy.

**off-hours work**

Any repair or maintenance work performed outside of normal working hours (such as nights, weekends, or holidays) when the work is less likely to impact business operations.

**open transition transfer switch**

A type of transfer switch that completely breaks its connection to one power source before making connection to the other.

**organizational chart**

A diagram that graphically depicts the chain of command and how one level of an organization relates to another, both vertically and horizontally.

**OSI model**

(Open Systems Interconnection model) The communication standard followed by all networks, regardless of their configuration and technology utilized, in which the data communication process is divided into seven tasks, grouped into different layers: physical, data link, network, transport, session, presentation, and application.

**over-current protection**

A means of interrupting the power flow when it exceeds safe levels, typically by tripping a breaker or blowing a fuse.

**panel schedule**

A tabular list of the electrical distribution systems and subsystems within a facility.

**paralleling switchgear**

Large devices comprised of electrical disconnects, fuses, circuit breakers, and other electrical instruments used to transfer the electrical load from the utility source to the generators (and vice versa) and then appropriately distribute the electrical power throughout the system.

**patch panel**

A device containing numerous ports used to connect multiple devices in various combinations.

**PBX**

(Private Branch Exchange) A hyper-local POTS network that allows users within the same location (such as a business office or campus) to simply dial an extension to reach another user on the network, without having to dial a full 7- or 10-digit phone number.

**PDU**

(power distribution unit) A piece of electrical equipment consisting of multiple outputs designed to distribute electrical power to multiple devices.

**penetrant**

Any mechanical, electrical, or structural component that must pass through a fire-rated material or containment component as part of

the larger facility system that it belongs to (such as HVAC or plumbing).

**penetration**

An opening created in a material or component that needs to have a fire-rating by a penetrant that needs to pass through that opening as part of a larger facility system.

**perforated tile**

A type of floor tile with holes through it that is used to supply cool air from below.

**permit to work**

A formal, written document that specifies the work to be done, the equipment and personnel involved, the potential hazards that the work poses, and the precautions that should be taken while work is being performed.

**phase balancing**

The practice of balancing the power draw from different phases of power delivered to individual cabinets.

**plans**

A general category of documents that detail the means and manner of the design and build processes.

**plumbing**

The system used to transport, capture, and remove miscellaneous fluids throughout a facility, including supply water/potable water, graywater, sewage, and other waste drainage.

**policies**

Guidelines that direct actions or activities to ensure that similar outcomes are achieved given a wide array of possible inputs and variables.

**POTS**

(Plain Old Telephone System) The transmission of voice data over wired networks utilizing a twisted pair of copper wires carrying the audio signals and a nominal current of 48V DC.

**power**

The rate at which a given amount of energy is transferred through an electrical circuit.

**power density**

The quantity of power consumed in a given infrastructure footprint.

**power distribution**

The set of electrical transmission systems that receive power from a primary source and then divide it up, pass it through any protective features, and deliver it to the connected equipment load.

**power factor**

The ratio of real power (the amount of energy actually available or used) to apparent power (the potential power purely available in an ideal system with no losses).

**power load balancing**

The practice of distributing power throughout the data center in such a manner that it provides equal load to and wear on the associated infrastructure.

**PPE**

(Personal Protective Equipment) Anything worn or used to minimize the risk of injury from safety hazards. Sometimes also called Personal Protective Gear, or PPG.

**predictive results**

The process of closely analyzing the data received from controls and monitoring platforms in order to anticipate how the systems will behave or respond in the future.

**pressure**

The force applied to the surface of an object, measured by the unit area over which that force is distributed.

**primary battery**

A category of battery that is only useful for one full discharge, at which point it must be discarded or have components replaced.

**prime mover**

A machine used to convert mechanical energy of some kind into electrical energy, but one that does not necessarily use an engine as the source of mechanical energy.

**private IP address**

An IP address, falling within one of the class ranges, that is not routed publicly and is used for private internal network use only.

**procedures**

Specifically prescribed means for accomplishing tasks in a reliable and safe manner.

**process water**

Water that serves a very particular function for an MCO facility, and therefore will have specific characteristics needed for proper system operation, such as particular purity or pH levels.

**protective relay**

An electromagnetically or electronically operated device that automatically senses or receives input about the system's current power conditions, and then opens and closes breakers if undesirable conditions are detected.

**PSI**

(pounds per square inch) A unit of pressure that represents the force applied by one pound of weight evenly distributed over a surface area of one inch squared.

**PUE**

(Power Usage Effectiveness) The ratio of the power consumed by the total critical infrastructure to the power consumed by the critical load of the data center.

**pumped refrigerant**

A type of cooling system that directly cools the circulating air by conducting the heat to a refrigerant loop; within the loop, the bulk of the refrigeration cycle occurs at a central cooling device and compressors pump the cooled liquid refrigerant in a closed loop with small sets of coils at desired cooling locations.

**radio system**

A wireless communication system in which voice or data signals are encoded, transmitted at a particular frequency over radio waves in a broad, unfocused distribution pattern which are then captured and decoded by radio antennas.

**raised access flooring**

A data center floor system design where the floors are elevated 18 to 48 inches above the slab to allow for under-floor cooling and/or space to run power conduits or other piping.

**record drawing**

A version of the construction documents that has been revised by the architect or engineer to capture the changes made to the space during construction, as reflected in the as-built drawings.

**rectifier**

An electrical device that converts AC power to DC power, by chopping up the moving wave of the AC current into pulses of a constant voltage that move in a single direction.

**redundancy**

The inclusion of extra systems, equipment, or components that may or may not be in service all the time, but provide additional capacity or function to support critical operations in the event of critical equipment failure.

**refrigerant**

A substance that handles heat transfer by changing its state from liquid to gas and back again, absorbing the heat at the low temperature/low pressure state and transferring the heat at the high temperature/high pressure state.

**regulations**

Established protocols, particular to certain industries or work practices, which are enforceable by law (whether backed by state, local, or federal statutes or the court system) and carry consequences for non-compliance.

**resistance**

The innate property of most conductors that creates opposition to the passage of an electrical current.

**return air plenum**

The ducting and/or contained space (usually overhead, above the ceiling grid) through which hot air rejected from the IT equipment is collected and exhausted and/or circulated back to the air handling units for cooling.

**risk management**

The process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level at an acceptable cost.

**room envelope**

The overall isolation of the space or spaces containing the main data center equipment.

**rotary UPS**

A type of uninterruptible power supply that uses a motor generator or some variation of rotating components to transfer power to the load via rotating generation.

**router**

A device that connects multiple networks by “routing” data packets between them to allow many different types of devices to communicate and exchange data.

**RTU**

(rooftop unit) A packaged unit that includes all the components necessary for heating, cooling, air handling, or all of the above, and is usually mounted on a curb or slab on the roof of the facility.

**satellite**

A wireless communication device that resides in a stationary position above a fixed point on the Earth, and repeats or reflects the communication signal back down to a satellite antenna on the ground.

**SCADA**

(Supervisory Control and Data Acquisition) A monitoring system that collects operational data from the various disparate but interconnected systems or components in a facility and presents all the information in an aggregated display to provide an overall view of the connected components as a whole.

**scheduled shutdown**

A highly pre-planned, extended period of time during which more complex change-controlled work that requires systems be taken offline and affects normal business operations is performed.

**SDS**

(Safety Data Sheets) A document that provides important information about a chemical and how to safely handle and/or work with that chemical, which follows the highly standardized classification and labelling of chemical-based materials implemented by the GHS.

**secondary battery**

A category of battery that is useful for numerous discharges, due to its rechargeable properties that allow a charge to be reapplied and stored for future use.

**security**

The application of devices and procedures to ensure that a valuable asset—whether that be an object, a person, a facility, or even information—is protected from harm.

**sensible heat**

The change in measured temperature that results from the addition or subtraction of heat energy within a substance.

**server**

A non-client computer on the network that performs the activities necessary for the continued functionality of a group of networked client computers or devices.

**service closet**

A closet, usually found on each floor of a building, that acts as an offshoot of the communication room and mostly houses non-critical network equipment in an easier-to-access location.

**set points**

Specific values used to establish parameters within which infrastructure systems should operate.

**shop drawings**

The initial, draft illustrations that detail the facility, system, and equipment design and setup for a project.

**single line diagram**

A simplified drawing of a system, illustrating the connections of components and equipment

via single lines that represent the flowpaths of the system.

**single-phase power**

A specific type of AC power distribution where a single conductor carries one waveform of current, or multiple conductors carry multiple currents with matching waveforms.

**SLTS**

(soft loading transfer switch) A type of transfer switch that synchronizes and parallels two independent power sources without the interruption of power, and then transfers the load between the two as it minimizes the momentary variations in the voltage and frequency.

**soft loading closed transition switch**

A type of transfer switch that supports an automatic transfer of power between the utility source and a generator, without interruption of service, by closing the connection between the generator and the utility and then transferring the facility load gradually.

**SOO**

(sequence of operation) A narrative description of how equipment and systems are designed to operate under a variety of conditions or circumstances.

**SOP**

(standard operating procedure) Precise step-by-step directions for how to conduct a frequently-performed task or operation in order to achieve a predictable and desirable result, which have been developed in accordance with industry regulations, provincial laws, and business standards or regulations.

**sound attenuator**

A material or device used to dampen noise by absorbing sound.

**special purpose network**

A network on which a high-value data stream is isolated either physically or logically from the normal network traffic.

**spot cooling**

An air cooling technique in which small cooling units are installed anywhere in the data center where additional cooling is needed.

**sprinkler system**

All of the devices that deliver water as the method of fire suppression to the space being affected by the fire, and spread it to adequately cover all equipment and structures.

**standards**

Protocols defined by public or private industry agencies and associations, typically regarding specific best practices, which are potentially enforced by civil justice powers and may have consequences for non-compliance.

**STS**

(static transfer switch) A type of transfer switch that monitors the two sources of power and automatically transfers to the source that is within proper operating parameters upon any interruption or degradation of the primary (or previous) power source.

**submittals**

Any design or construction documentation made in response to project requirements that needs some level of review and approval.

**subnet**

A portion of a network that shares a common address component.

**subnet mask**

A numerical version of the IP address, divided into a network address and host address, that is assigned to a specific subnet; a portion of the host address is then utilized to identify to which subnet it belongs.

**supercapacitor**

An energy storage device that always maintains a large amount of stand-by charge and has the ability to charge or discharge all of their energy very quickly.

**supply air plenum**

The ducting and/or contained space (usually under the raised floor) through which cool air is supplied to the data center via the air handling units.

**switch**

A device used to connect multiple physically networked resources or devices for the purpose of sharing data.

**TCP/IP model**

(Transmission Control Protocol/Internet Protocol model) The suite of communication protocols that are used as the standard for transmitting data over networks.

**telephony**

The construction, technology, and application of systems used for telephones and telephone networks.

**temperature**

The measurement of the amount of heat an object or substance possesses or the quantitative capacity for an object or substance to transfer heat energy to something else.

**terminal unit**

A small air handler used more locally, such as at the specific location where air handling is needed.

**thermal wheel**

A cooling system that uses a rotating wheel to cool air in a two stage process: first, heated exhaust air is blown into one half of the wheel, where conductive material absorbs the heat and cooled air is expelled for reuse; then, the heated wheel turns and circulated air is blown into the other half, which absorbs the heat from the conductive material and turns the wheel again.

**threat**

Anything that can potentially cause damage or harm to a person or object.

**three-phase power**

A specific type of AC power distribution where three conductors (or sets of three conductors) reach the peaks of their current waveforms sequentially.

**throw-over switch**

A device that connects to and, in some cases, monitors a system's primary and alternate source of power and allows an operator to manually switch between the two to maintain a



consistent, stable flow of electricity at the voltage needed to handle the system's load. Also known as a manual transfer switch.

### **transformer**

An electrical device that increases or decreases the voltage in an AC circuit by varying the current flowing through the conductor's internal wires via electromagnetic induction.

### **trapped key interlock**

A specific type of interlock device in which a key is trapped inside a cylinder that is part of the breaker itself; in one key position, the breaker is free to operate and in the alternate position a physical obstruction is inserted through the breaker operator mechanism to lock it in that position. Often called a Kirk Key, in reference to a common brand used in many MCO facilities.

### **trending**

The collection of time-based data points that provide discrete measurements of operating characteristics of the critical infrastructure equipment.

### **triage**

The act of sorting the various results of a specific risk-related event and determining the priority for addressing each and allocating the appropriate resources to do so.

### **TVSS**

(Transient Voltage Surge Suppressor) A device that provides electrical protection to connected equipment by buffering and absorbing voltage spikes and, as needed, diverting excess voltage away from the connected load.

### **twisted pair cable**

A type of cable that consists of four twisted pairs of insulated wires encased in a single sheath.

### **UPS**

(uninterruptible power supply) A device or machine that provides immediate emergency power when the primary power source fails, using electrical energy stored within the device itself.

### **utilities**

Resources that require connection to public services, such as power, water, sewage, and telecommunications.

### **VAV**

(Variable Air Volume) A type of a heating, ventilating, or air conditioning system that varies the conditioned air flow but maintains the air at a constant temperature.

### **vented access flooring**

A data center floor system design where ducting is run under the floors and vented into the space at specific locations within the infrastructure design.

### **ventilation**

The exchange of air, conditioned or otherwise, for either people comfort or equipment operations.

### **volt**

The unit of measure used to express voltage and an aspect of flowing electricity.

### **voltage**

The potential difference in electrical energy (or charge) between two points.

### **WAN**

(Wide Area Network) A network formed by the connection of two or more LANs residing in different geographical locations and connected through a public network.

### **water-cooled chiller**

A type of cooling device that removes heat from water and conducts it to another source of water as the final stage in the heat rejection/cooling process.

### **watt**

The standard unit of measure for electrical power, with a value of one joule per second.

### **wet-bulb temperature**

The measurement of changes in both sensible and latent heat in the form of temperature, as read by a thermometer utilizing moisture on the sensing bulb that determines how much water evaporates off the bulb and into the air.

**Wi-Fi**

(Wireless Fidelity) A wireless communication system used for high-speed Internet access and data transmission, connecting wireless devices to otherwise wired communication networks.

**zone selective interlock**

An intelligent control feature that can be added to a protective system in order to prevent the entire system from responding to a fault.

# Index

## A

- access control systems
  - biometrics [290](#)
  - keypads [292](#)
  - security badges and readers [291](#)
- air circulation systems
  - air handling units [170](#)
  - air rotation units [172](#)
  - DOAS [171](#)
  - ductwork systems [173](#)
  - exhaust systems [169](#)
  - fan systems [168](#)
  - heat recovery systems [170](#)
  - rooftop units [172](#)
  - terminal units [172](#)
- air handling units
  - air filters [170](#)
  - blower [170](#)
  - dampers [170](#)
  - heating and cooling elements [170](#)
  - sound attenuators [170](#)
- AJH [220](#)
- alternative cooling systems
  - air-side economization [164](#)
  - evaporative cooling [165](#)
  - free-air cooling [164](#)
  - geothermal cooling [165](#)
  - thermal wheel [163](#)
- alternative power sources
  - biomass [94](#)
  - capacitors [95](#)
  - co-generated power [96](#)
  - fuel cells [91](#)
  - geothermal power [96](#)
  - solar panels [92](#)

- supercapacitors [95](#)
- wind power [93](#)

ATS [76, 117](#)

Authority Having Jurisdiction, *See* AJH

automatic transfer switch, *See* ATS

## B

BAS [403](#)

batteries

- lead acid [88](#)

- lithium-ion [88](#)

- nickel cadmium [89](#)

- primary and secondary [87](#)

battery systems [87](#)

biohazards [266](#)

BMN [368](#)

BMS [403](#)

Building Automation System, *See* BAS

Building Management Network, *See* BMN

Building Management System, *See* BMS

## C

cabling

- below-floor [326](#)

- bend radius [328](#)

- cable dressing [329](#)

- cable tracing and testing [330](#)

- coaxial cables [324](#)

- fiber optic cables [324](#)

- labeling [326](#)

- overhead cable trays [327](#)

- twisted pair cables [324](#)

change management

- blackout dates [436](#)

- cutover windows [437](#)
- double custody switching [439](#)
- energized work [438](#)
- hot work permits [437](#)
- maintenance windows [436](#)
- off-hours work [439](#)
- permit to work [437](#)
- procedure change methods [440](#)
- scheduled shutdowns [439](#)
- closed transition transfer switch, *See* CTTS
- communication systems
  - wired systems [374](#), [375](#)
  - wireless systems [377–381](#)
- computer networks
  - in general [338](#)
- Computer Room Air Conditioner, *See* CRAC
- CRAC
- Computer Room Air Handler, *See* CRAH
- conditioned spaces [140](#)
- confined space [244](#)
- controls [3](#)
- controls system
  - alarm thresholds and resets [419](#)
  - equipment status [418](#)
  - process control devices [419](#)
  - set points [417](#)
- CRAC [317](#)
- CRAH [317](#)
- crisis [18](#)
- crisis management
  - overview [19](#)
  - phases [21](#)
- critical infrastructure [2](#)
- critical production environments [333](#)
- critical production equipment [334](#)
- CTTS [116](#)

## D

- data center air flow
  - air management equipment [317](#)
  - HACA [318](#)
  - humidity control [321](#)
  - in-row vs. spot cooling [317](#)
  - perforated tiles [319](#)
  - pressure control [320](#)
  - return air methodologies [320](#)
  - return air plenums [318](#)
  - room envelope [318](#)
  - space integrity [318](#)
  - supply air plenums [318](#)
  - temperature control [320](#)

- Data Center Infrastructure Efficiency, *See* DCiE
- DCiE
- data centers
  - cleanliness [313](#)
  - component redundancy [307](#)
  - DCiE [309](#)
  - distribution redundancy [308](#)
  - floor systems [311](#)
  - grounding [307](#)
  - load shedding [308](#)
  - phase balancing [308](#)
  - placement of IT equipment [310](#)
  - power cabling [307](#)
  - power load balancing [308](#)
  - PUE [309](#)
  - rack cooling [312](#)
  - rack power distribution [310](#)
  - site selection [306](#)
- DCiE [309](#)
- dedicated outdoor air system, *See* DOAS
- Department of Homeland Security, *See* DHS
- DHS
  - design considerations
    - backup systems [47](#)
    - site selection [43](#), [306](#)
    - utilities [45](#)
- dew point
  - calculating [147](#)
  - definition of [147](#)
- DHS
  - critical infrastructure sectors [23](#)
  - overview [23](#)
- direct expansion, *See* DX
- DNS
  - hierarchy [357](#)
  - Name Resolution Process [357](#)
  - overview [355](#)
  - record types [356](#)
- DOAS [171](#)
- documentation [16](#)
- Domain Name System, *See* DNS
- domestic power
  - sources of [67](#)
- ductwork [173](#)
- DX [155](#)

## E

- EHS [249](#)
- Electrical Power Monitoring Systems, *See* EPMS
- EPMS
- electrical protection

- arc fault potential [130](#)
  - arc flash protection [129](#)
  - grounding [125](#)
  - lightning protection [128](#)
  - over-current protection [125](#)
  - protective relays [126](#)
  - surge protection [127](#)
  - zone selective interlocks [130](#)
  - electricity
    - alternating current [60](#)
    - amps [58](#)
    - current [58](#)
    - definition of [52](#)
    - direct current [59](#)
    - frequency [60](#)
    - grounding [63](#)
    - inverters [62](#)
    - kilowatts [62](#)
    - kVA [63](#)
    - kWh [63](#)
    - power [59](#)
    - rectifiers [62](#)
    - resistance [59](#)
    - transformers [61](#)
    - voltage [55](#)
    - watts [62](#)
  - emergency operating procedure, *See* EOP
  - Emergency Power Off, *See* EPO
  - emergency response procedures
    - biohazards [266](#)
    - fire drills [255](#)
    - fires [257](#)
    - gas leaks [257](#)
    - hazardous materials [262](#)
    - IAP [255](#)
    - ICS [255](#)
    - incident and incident reports [253](#)
    - notifications and communications [254](#)
    - nuclear material [267](#)
    - public response systems [254](#)
    - severe events [258](#)
    - utility outages [256](#)
  - entropy [140](#)
  - environmental and system monitoring
    - environmental conditions [388](#)
  - Environmental Health and Safety Program, *See* EHS
  - environmental parameters
    - battery monitoring [390](#)
    - corrosion [391](#)
    - environmental conditions [388](#)
    - hydrogen concentration [390](#)
    - indoor air quality [392](#)
    - leak detection [390](#)
    - moisture detection [390](#)
    - outdoor ambient environment [393](#)
    - water flow [389](#)
  - EOP [431](#)
  - EPMS [404](#)
  - EPO
    - definition [229](#)
    - design and use [230](#)
    - pros and cons [230](#)
  - exit and emergency lighting
    - battery backup [226](#)
    - generator-sourced [227](#)
    - in general [226](#)
    - night light circuits [227](#)
- ## F
- facility and system documentation
    - as-built drawings [458](#)
    - Basis of Design [456](#)
    - control diagrams [461](#)
    - design specifications [456](#)
    - digital system architecture plans [463](#)
    - equipment schedule [462](#)
    - flow diagrams [460](#)
    - panel schedules [458](#)
    - plans [461](#)
    - record drawings [458](#)
    - records and system drawings [463](#)
    - single line diagram [457](#)
    - submittals [459](#)
  - fire detection systems
    - beam detectors [206](#)
    - definition [205](#)
    - fire alarm control panels [208](#)
    - fire alarms [207](#)
    - flame and flash detection [206](#)
    - high-sensitivity smoke detection [206](#)
    - smoke and heat detection [205](#)
  - fire-safe facility
    - AHJ [220](#)
    - containment [222](#)
    - egress route [221](#)
    - firestop [223](#)
    - penetrations [223](#)
    - walls and firewalls [221](#)
  - fire suppression systems
    - clean agent systems [216](#)
    - fire extinguishers [216](#)

- fire pump systems [214](#)
- foam systems [217](#)
- overview [212](#)
- sprinkler systems [212](#)
- fire triangle [204](#)
- flooring systems
  - bridging [312](#)
  - loading [312](#)
  - raised access flooring [311](#)
  - vented access flooring [311](#)
- flow [149](#)
- fluid [148](#)
- FQDN [354](#)
- Fully Qualified Domain Name, *See* FQDN

## G

- generators
  - ATS [76](#)
  - exercising [134](#)
  - fuel types [75](#)
  - overview [73](#)
  - paralleling switchgear [78](#)
  - throw-over switches [77](#)
  - types of [74](#)
- GHS [250](#)
- Globally Harmonized System of Classification and Labelling of Chemicals, *See* GHS

## H

- HACA [318](#)
- hazardous material [262](#)
  - See also* hazmat
- hazards
  - analysis [238](#)
  - chemical and other hazardous substances [243](#)
  - common [239](#)
  - confined spaces and ventilation [244](#)
  - custodial services [248](#)
  - Materials Safety and Awareness systems [249](#)
- hazmat [262](#)
- heat
  - definition of [140](#)
  - delivery systems [142](#)
  - latent [146](#)
  - sensible [146](#)
  - sources of [141](#)
- heating, ventilation, and air conditioning, *See* HVAC

- Hot Aisle/Cold Aisle, *See* HACA
- humidity
  - calculating [147](#)
  - definition of [146](#)
- HVAC
  - air conditioning [143](#)
  - belt maintenance [177](#)
  - coil maintenance [176](#)
  - definition of [140](#)
  - filter maintenance [176](#)
  - heating [141](#)
  - refrigerant [144](#)
  - TAB [177](#)
  - ventilation [142](#)

## I

- IAP [255](#)
- ICS [255](#)
- inch of water column [149](#)
- Incident Action Plan, *See* IAP
- Incident Command System, *See* ICS
- Information Technology, *See* IT
- Internet [363](#)
- Internet Protocol, *See* IP
- IP [350](#)
- IT [7](#)

## L

- LAN [362](#)
- LBS [84](#)
- Load Bus Synchronization, *See* LBS
- Local Area Network, *See* LAN
- Lock Out/Tag Out, *See* LOTO
- LOTO [246](#)

## M

- Material Safety Data Sheets, *See* MSDS
- MCO industry protocols
  - building codes [446](#)
  - compliance [445](#)
  - guidelines [445](#)
  - regulations [445](#)
  - standards [445](#)
- MCO industry standards
  - ANSI [448](#)
  - ASHRAE [449](#)
  - LEED [447](#)
  - NETA [450](#)
  - NFPA [451](#)

OSHA 450  
 TIA 450  
 Uptime Institute 448

MCOs  
 cost/benefit analysis 43  
 definition of 2  
 design parameters 43  
 efficiencies 108  
 key elements 7  
 systems 3

metering  
 branch circuit metering 397  
 defined 396  
 fuel 399  
 gas 399  
 outlet 397  
 process variable 400  
 utility and generator power 396  
 water level 398

mission critical infrastructure  
 sectors 23

mission critical mindset 37

Mission Critical Operations, *See* MCOs

mission critical systems 3

monitoring platforms  
 BMS/BAS monitoring 403  
 EPMS 404  
 equipment-level systems 405  
 SCADA 404

MSDS 250

## N

National Incident Management System, *See* NIMS

network components  
 clients 340  
 connection points 345  
 gateways 343  
 NICs 340  
 overview 339  
 patch panels 344  
 router 341  
 servers 340  
 switch 342

network connection points  
 communication room 345  
 demarcation point 345  
 distribution frame 345  
 duct banks 345  
 manholes 345  
 service closet 345

networking 7

networking concepts  
 computer networks 338  
 data packets 349  
 DNS 355, 356  
 domain names 354  
 FQDN 354  
 host names 354  
 HOSTS file 355  
 Internet Protocol 350  
 IP address classes 353  
 IP addresses 352  
 location 346  
 network address 350  
 network names 351  
 OSI model 351  
 private IP addresses 354  
 subnet masks 353  
 subnets 353  
 TCP/IP 352, 357

network interface controller, *See* NICs

network topologies  
 logical 367  
 physical 364

network types  
 BMN 368  
 intranets 367  
 LANs 362  
 network coverage areas 364  
 other 363  
 special purpose network 368  
 WANs 363

NICs 340

NIMS 254

## O

Open Systems Interconnection model, *See* OSI model

open transition transfer switch 116

operating and maintenance manuals  
 preventative maintenance 470  
 seasonal operation 470  
 sequence of operation 469  
 shop drawings 468  
 warranty information 469

operating procedures  
 common procedures 432  
 EOP 431  
 SOP 430

organizational structure  
 chain of command 426

- client-contractor relations [427](#)
  - escalation paths [426](#)
  - organization charts [427](#)
  - vendor management [428](#)
  - OSI model [351](#)
- P**
- PBX [375](#)
  - PDU [103](#)
  - Personal Protective Equipment, *See* PPE
  - Personal Protective Gear, *See* PPG
  - personnel protection
    - Arc Flash labels [245](#)
    - chemical cabinets [247](#)
    - custodial services [248](#)
    - LOTO [246](#)
    - safety barriers and machine guards [247](#)
    - showers and eye wash stations [243](#)
    - warning labels [245](#)
  - physical security
    - access prevention [274](#)
    - barriers [275](#)
    - communication equipment [285](#)
    - deterrents [274](#)
    - electrical fencing [277](#)
    - fencing [276](#)
    - gates, walls, and fencing [275](#)
    - in general [274](#)
    - intrusion detection [284](#)
    - locking mechanisms [282](#)
    - points of entry [280](#)
    - vehicle barriers [279](#)
    - vehicle security [278](#)
    - video surveillance [283](#)
  - Plain Old Telephone System, *See* POTS
  - plumbing
    - backflow prevention [187](#)
    - drainage [184](#)
    - effluent [182](#)
    - graywater [182](#)
    - rounds and readings [198](#)
    - water sources [183](#)
  - policies [13](#)
  - POTS [374](#)
  - Pounds per Square Inch, *See* PSI
  - power density [64](#)
  - power distribution
    - efficiency [108](#)
    - low voltage system [103](#)
    - medium voltage system [104](#)
    - multiple-source/feed power [104](#)
    - overview [102](#)
    - PDU's [103](#)
    - preventative maintenance [133](#)
    - redundancy [111](#)
  - power distribution topologies
    - basic [121](#)
    - concurrently maintainable [122](#)
    - fault tolerant [123](#)
    - overview of [121](#)
    - redundant [122](#)
  - power distribution unit, *See* PDU
  - power factor [59](#)
  - power sources
    - alternative [91](#)
    - battery systems [87](#)
    - electricity [52](#)
    - generators [73](#)
    - power factor [59](#)
    - prime mover [73](#)
    - types of [67](#)
    - UPSs [81](#)
  - power supply
    - single-phase [61](#)
    - three-phase [61](#)
  - power supply transfer
    - automatic transition [117](#)
    - closed transition [116](#)
    - critical power interlocks [117](#)
    - open transition [116](#)
    - soft loading [116](#)
    - soft loading closed transition [117](#)
    - static transfer [116](#)
    - Trapped Key Interlocks [118](#)
  - Power Usage Effectiveness, *See* PUE
  - PPE
    - in general [239](#)
  - PPG [239](#)
  - pressure [149](#)
  - preventative maintenance
    - filter maintenance [176](#), [199](#)
    - fire alarm systems [233](#)
    - fire system equipment [232](#)
    - plumbing [198](#)
    - system inspections [199](#)
  - Private Branch Exchange, *See* PBX
  - procedures [13](#)
  - PSI [149](#)
  - PUE [309](#)
- R**
- redundancy



- definition of [111](#)
- dual-cord supply [112](#)
- levels [111](#)
- refrigerant-based cooling systems
  - air-cooled chiller [154](#)
  - chiller [153](#)
  - direct expansion [155](#)
  - pumped refrigerant [155](#)
  - water-cooled chiller [154](#)
- risk management [20](#)

**S**

Safety Data Sheets, *See* SDS

SCADA [404](#)

SDS [250](#)

secondary systems
 

- chilled water [192](#)
- compressed air [191](#)
- humidity control [193](#)
- natural gas [193](#)
- other compressed gases [194](#)
- process water [192](#)
- radiation [194](#)
- vacuum [190](#)

security [10](#)

security procedures
 

- background checks [296](#)
- classified projects [301](#)
- confidentiality [300](#)
- entry credentials [296](#)
- fire watches [300](#)
- manual logs [299](#)
- materials and inspections [298](#)
- security patrols [299](#)
- sensitive equipment or information [300](#)
- site access control [297](#)

soft loading closed transition switch [117](#)

soft loading transfer switch [116](#)

SOP [430](#)

standard operating procedure, *See* SOP

static transfer switch, *See* STS

STS [116](#)

Supervisory Control and Data Acquisition, *See* SCADA

switchgear maintenance [133](#)

system monitoring
 

- alarm conditions [408](#)
- dashboarding [410](#)
- effects of local failures [411](#)
- measurement and verification [413](#)
- mitigating risks and failures [409](#)

- normal vs. abnormal states [407](#)
- predictive results [409](#)
- preventative maintenance [414](#)
- trending [409](#)
- trouble alarms [408](#)
- warning messages [408](#)

## T

TAB [177](#)

TCP/IP [352](#), [357](#)

temperature
 

- dry-bulb vs. wet bulb [147](#)
- measurements [144](#)

testing, adjusting and balancing, *See* TAB

testing reports
 

- commissioning reports [473](#)
- electrical systems testing reports [474](#)
- testing, adjusting, and balancing reports [474](#)

threats [3](#)

Transient Voltage Surge Suppressor, *See* TVSS

Transmission Control Protocol/Internet Protocol, *See* TCP/IP

triage [20](#)

TVSS [127](#)

## U

uninterruptible power supply, *See* UPS

UPS
 

- delta conversion [83](#)
- diesel rotary [84](#)
- double conversion [83](#)
- flywheels [82](#)
- line interactive [82](#)
- Load Bus Synchronization [84](#)
- overview [81](#)
- rotary [83](#)

utilities [45](#)

utility-source power
 

- grid [67](#)
- microgrid [70](#)
- types of [67](#)

## V

Variable Air Volume, *See* VAV

VAV [146](#)

voltage
 

- high [57](#), [69](#)
- low [56](#), [103](#)

medium [56](#), [69](#), [104](#)  
volts [55](#)

## W

WAN [363](#)

water-based cooling systems

- cooling towers [157](#)
- freeze protection [159](#)
- heat exchangers [158](#)
- primary pumping [157](#)
- secondary pumping [157](#)
- thermal storage [159](#)
- variable primary pumping [157](#)

water supply

- makeup water [185](#)
- pumps and pressurization [186](#)
- sources [183](#)
- water treatment [186](#)

Wide Area Network, *See* WAN

wired communication systems

- PBX [375](#)
- POTS [374](#)
- telephony [374](#)

wireless communication systems

- cellular [380](#)
- microwaves [378](#)
- radio systems [377](#)
- satellite [379](#)
- Wi-Fi [381](#)