Center for Curriculum and Transfer Articulation

# Generation and Transmission Systems Security

| | |
|---|---|
| Course: **CIS275DA** | Lec + Lab **3** Credit(s) **4** Period(s) **3.7** Load |
| | Course Type: **Occupational** |
| First Term: **2014 Fall** | Load Formula: **S- Standard** |
| Final Term: **Current** | |

**Description:** Introduction to industrial control systems and how they support Power Generation and Transmission. Risks associated with infrastructures and why it is important to reduce those risks to acceptable levels by securing supporting industrial control systems. Advanced knowledge of industrial control systems used in the power, energy and utility industry with a concentrated focus on cyber security. This experience will also be directly transferable to other industries that operate industrial control systems such as Chemical Processing, Manufacturing, Defense, etc. Partial preparation for the Certified SCADA (Supervisory Control and Data Acquisition) Security Architect (CSSA) certification provided by the Information Assurance Certification Review Board (IACRB).

**Requisites:** Prerequisites: CIS274DA or permission of Instructor.

## MCCCD Official Course Competencies

1. Describe the overall architecture associated with the power transmission and generation system (I, II, IV).
2. Explain what industrial control systems are and how they are used to support the power transmission and generation systems (IV, V).
3. Describe the makeup and anatomy of power and energy organizations that operate transmission and generation assets (III).
4. Explain threats and vulnerabilities to industrial control systems, as well as how these risks are managed (VI, VIII).
5. Explain how to develop a business case to promote security for industrial control systems (VII).
6. Explain how to implement security controls in order to secure industrial control systems and their associated infrastructures (VIII).
7. Explain security compliance regulations related to transmission and generation architectures (VIII).

## MCCCD Official Course Outline

I. The Transmission System
A. Control Centers
1. Energy Management System
2. Grid Display
3. Automatic Generation Control
4. Supervisory Control and Data Acquisition

4. Supervisory Control and Data Acquisition
5. Contingency Reserve Management
6. Interchange Scheduling

B. Transmission Substations

1. Relays
2. Programmable Logic Controllers
3. Synchrophasors
4. Remote Terminal Units

II. Generation Resources

A. Nuclear Power

1. Steam Generators
2. Control Rods
3. Fuel
4. Reactor
5. Containment
6. Safety Systems
7. Steam Lines
8. Pump Condenser
9. Turbine
10. Generator
11. Cooling Water
12. Transformer
13. Water Inlets
14. Cooling Tower
15. Cool Water Source
16. Cold Water Basin
17. Electricity

B. Coal Power

1. Coal Transport
2. Primary Crusher
3. Coal Slot
4. Secondary Crusher
5. Conveyor Belt
6. Coal Silo
7. Precipitator
8. Pulverizer
9. Boiler
10. Turbine
11. Outlet Canal
12. Condenser
13. Generator
14. Generator Transformer
15. Inlet Canal
16. Stack
17. Transmission

C. Natural Gas Power

1. Oil Storage
2. Natural Gas Line
3. Air Intake

3. Air Intake
4. Compressor
5. Combustion Chambers
6. Turbine
7. Exhaust
8. Generator
9. Transformer
10. Transmission

D. Hydroelectric Power
1. Reservoir
2. Intake
3. Penstock
4. Generator
5. Turbine
6. Tail water
7. Transformer
8. Transmission

E. Distributed Energy Resources
1. Wind Turbines
2. Diesel Engine
3. Natural Gas Engine
4. Dual Fuel Engine
5. Combustion Turbines
6. Micro Turbines
7. Fuel Cells
8. Photovoltaic

F. Energy Storage
1. UPS
2. Superconducting magnetic energy storage
3. Flywheel Systems
4. Hybrid Systems
5. Large Battery Systems

G. DER Programs
1. Peak Shaving
2. Improved Power Quality
3. Green Power

H. Micro Grids

III. Power Utility Organizational Makeup

A. Design
B. Engineering
C. Communications
D. Information Technology
E. Planning
F. Grid Operations
G. Plant Operations
H. Substation Operations
I. Accounting
J. Marketing
K. Substation Maintenance

K. Substation Maintenance
L. Generation Maintenance
M. Construction
N. Metering Support
O. Smart Grid Operations
IV. Distributed Control Systems
A. Fuel Supply
B. Boiler
C. Turbine
D. Condenser
E. Water Treatment
F. Handling
G. Emission Monitoring
V. Industrial Control Systems
A. Control Server
B. SCADA Server or Master Terminal Unit (MTU)
C. Remote Terminal Unit (RTU).
D. Programmable Logic Controller (PLC)
E. Intelligent Electronic Devices (IED)
F. Human-Machine Interface (HMI)
G. Data Historian
H. Input/Output (IO) Server
I. Fieldbus Network
J. Control Network
K. Communications Routers
L. Firewall
M. Modems
N. Remote Access Points
VI. Threats and Vulnerabilities
A. Comparing ICS and IT Systems
1. Performance Requirements
2. Availability Requirements
3. Risk Management Requirements
4. Architecture Security Focus
5. Physical Interaction
6. Time Critical Responses
7. System Operation
8. Resource Constraints
9. Communications
10. Change Management
11. Managed Support
12. Component Lifetime
13. Access to Components
B. ICS Threats
1. Attackers
2. Bot-network operators
3. Criminal Groups
4. Foreign Intelligence Service
5. Insiders

5. Insiders
6. Phishers
7. Spammers
8. Spyware/malware authors
9. Terrorists
10. Industrial Spies

C. ICS Vulnerabilities

1. Policy and Procedure Vulnerabilities
2. Platform Configuration Vulnerabilities
3. Platform Hardware Vulnerabilities
4. Platform Software Vulnerabilities
5. Platform Malware Protection Vulnerabilities
6. Network Configuration Vulnerabilities
7. Network Hardware Vulnerabilities
8. Network Perimeter Vulnerabilities
9. Network Monitoring and Logging Vulnerabilities
10. Communication Vulnerabilities
11. Wireless Connection Vulnerabilities
12. Standardized Protocols and Technologies
13. Increased Connectivity
14. Insecure and Rogue Connections
15. Public Information

D. ICS Incident Scenarios

1. Worcester Air Traffic Communications
2. Maroochy Shire Sewage Spill
3. Stuxnet Worm
4. CSX Train Signaling System
5. Davis-Besse
6. Northeast Power Blackout9
7. Zotob Worm
8. Taum Sauk Water Storage Dam Failure
9. Bellingham, Washington Gasoline Pipeline Failure
10. Vulnerability Scanner Incident
11. Penetration Testing Incident

VII. Business Case for Security

A. Benefits

B. Consequences

1. Physical Impacts
2. Economic Impacts
3. Social Impacts

C. Key Business Case Components

1. Prioritized Threats
2. Prioritized Business Consequences
3. Prioritized Business Benefits
4. Estimated Annual Business Impact
5. Resources for Building Business Case
6. Presenting the Business Case to Leadership
7. Developing a Security Program
8. Senior Management Buy-in

8. Senior Management Buy In
9. Creating the Security Team
10. Policies, Processes and Procedures
11. Inventory and Asset Management
12. Risk and Vulnerability Assessment
13. Mitigating Controls Identification
14. Training and Awareness

VIII. Securing the Control System Network

A. Firewalls
1. Packet Filtering Firewall
2. Stateful Inspection Firewalls
3. Application-Proxy Gateway Firewalls

B. Logically Separated Network Control

C. Network Segregation
1. Dual-Homed Computer/Dual Network Interface Cards (NIC)
2. Firewall between Corporate Network and Control Network
3. Firewall and Router between Corporate Network and Control Network
4. Firewall with DMZ between Corporate Network and Control Network
5. Paired Firewalls between Corporate Network and Control Network

D. Recommended Defense-in-Depth Architecture

E. Recommended Firewall Rules for Specific Services
1. Domain Name System (DNS)
2. Hypertext Transfer Protocol (HTTP)
3. FTP and Trivial File Transfer Protocol (TFTP)
4. Telnet
5. Simple Mail Transfer Protocol (SMTP)
6. Simple Network Management Protocol (SNMP)
7. Distributed Component Object Model (DCOM)

F. SCADA and Industrial Protocols
1. DNP 3.0
2. IEC 61850
3. Modbus
4. ASCII
5. IEEE 60870
6. Proprietary Protocols

G. Known ICS Issues
1. Data Historians
2. Remote Support Access
3. Multicast Traffic
4. Single Points of Failure
5. Redundancy and Fault Tolerance
6. Man-in-the-Middle Attacks
7. Redundancy and Fault Tolerance

H. Security Controls
1. Security Assessment and Authorization
2. Planning
3. Risk Assessment
4. System and Services Acquisition
5. Program Management

5. Program Management
6. Personnel Security
7. Physical and Environmental Protection
8. Contingency Planning
9. Configuration Management
10. Maintenance
11. System and Information Integrity
12. Media Protection
13. Incident Response
14. Awareness and Training
15. Identification and Authentication
16. Access Control
17. Audit and Accountability
18. System and Communications Protection

I. NERC CIP

1. Cyber Security - Critical Cyber Asset Identification
2. Cyber Security - Security Management Controls
3. Cyber Security - Personnel & Training
4. Cyber Security - Electronic Security Perimeter(s)
5. Cyber Security - Physical Security of Critical Cyber Assets
6. Cyber Security - Systems Security Management
7. Cyber Security - Incident Reporting and Response Planning
8. Cyber Security - Recovery Plans for Critical Cyber Assets

Last MCCCD Governing Board Approval Date: **June 24, 2014**