Center for Curriculum and Transfer Articulation

Smart Grid and Distribution System Security

Course: **CIS275DB**	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: Information security risks associated with a modernized electric power grid. Provides detailed overview of the modern electric power grid including its components, functions and features. Focuses on security risks related to distribution automation and smart meters including smart grid components, interfaces and interactions between components with differing levels of security. Architecture, protocols and security impacts associated with this infrastructure are stressed.

Requisites: Prerequisites: CIS274DA or permission of Instructor.

MCCCD Official Course Competencies

1. Explain what the importance of the smart grid (I, III, V).
2. Explain the security implications of using automation to control the grid (I, III, V).
3. Describe the risks associated with automation of electric grid components and why the security posture of these systems is important (II, V).
4. Explain threats to smart grid including vulnerabilities and impacts that increase its risk profile (II, V).
5. Describe how smart grid components interact with one another and how to apply security controls to protect these interfaces (III, IV).

MCCCD Official Course Outline

I. Elements of a Modern Grid
A. Customer enablement
1. Energy Services Interface
2. Programmable Communicating Thermostat
3. Customer Premise
4. Load Control and Smart Appliances
5. Plug-in Electric Vehicle and Electric Vehicle Supply Equipment
6. Mobile HAN
7. Home Area Networking
8. Smart Meters
9. Neighborhood Area Networking
10. Smart Meter Collectors
11. Wide Area Networking
12. Utility DMZ
13. Head-end System

13. Head end System
14. Meter Data Management System
15. Back office

B. Distribution Automation

1. Utility Field Sensors
2. Utility Distribution and Feeder Meters
3. Utility Field Controllers
4. Local Access Network
5. Sensor/Meter Aggregator
6. Wide Area Network
7. Data Center Access
8. Sensor Head-End
9. Meter Head-End
10. Distribution SCADA
11. Back Office

C. Transmission Automation

1. Energy Management System
2. Energy System Display
3. Automatic Generation Control
4. Supervisory Control
5. Contingency Reserve Management
6. Interchange Scheduling
7. SCADA Master Terminal
8. SCADA Front-End Processor
9. Synchrophasors
10. Relays
11. Programmable Logic Controllers
12. Remote Terminal Units
13. Control Center

D. Smart Grid Benefits

1. Enables Consumer Participation
2. Accommodates All Generation & Storage Options
3. Enables New Markets
4. Meets Power Quality Needs
5. Optimizes Assets & Operates Efficiently
6. Self Heals
7. Resists Attack

II. Smart Grid Threats

A. Nation States
B. Hackers
C. Terrorists/Cyber Criminals
D. Organized Crime
E. Other Criminal Elements
F. Industrial Competitors
G. Disgruntled Employees
H. Careless Poorly Trained Employees

III. Smart Meter Logical Reference Model

A. Operations

1. Wide Area Measurement

1. Wide Area Measurement
2. Transmission SCADA
3. Distribution Operator
4. Distributed Generation and Storage Management
5. Distribution Engineering
6. Distribution Management System
7. Work Management System
8. Transmission Engineering
9. Outage Management
10. Load Management
11. Customer Portal
12. Customer Service Representative
13. Customer Information System
14. AMI Head End
15. Meter Data Management System
16. ISO/RTO Operations
17. Metering/Billing/Utility Back office
18. Bulk Storage Management
19. Energy Management System

B. Service Provider

1. Billing
2. Third Party
3. Aggregator / Retail Energy Provider
4. Energy Service Provider

C. Markets

1. ISO/RTO Wholesale Market
2. Energy Market Clearing House

D. Transmission

1. Phasor Measurement Unit
2. Transmission RTU
3. Transmission IED

E. Bulk Generation

1. Plant Control System

F. Distribution

1. Field Crew Tools
2. Geographic Information System
3. Distribution RTUs
4. Distributed Intelligence Capabilities
5. Distribution Data Collectors
6. Distribution Sensors

G. Customer

1. Customers
2. Customer Premise Display
3. Customer Appliances and Equipment
4. Meter
5. Sub meter
6. Electric Vehicle
7. Customer DER
8. Water/Gas Meters

8. Water/Gas Meters
9. Energy Services/HAN Gateway
10. Customer Energy Management System

IV. Securing Smart Grid Security

A. Access Control

1. Remote Access
2. Account Management
3. Access Enforcement
4. Information Flow Enforcement
5. Separation of Duties
6. Least Privilege
7. Unsuccessful Login Attempts
8. System Use Notification
9. Previous Logon Notification
10. Concurrent Session Control
11. Session Lock
12. Remote Session Termination
13. Permitted Actions without Identification and Authentication
14. Access Control for Portable and Mobile Devices
15. Control System Access Restrictions
16. Publically Accessible Content
17. Passwords
18. Wireless Access

B. Configuration Management

1. Baseline Configuration
2. Configuration Change Control
3. Monitoring for Configuration Changes
4. Access Restrictions for Configuration Change
5. Configuration Settings
6. Configuration for Least Functionality
7. Component Inventory
8. Factory Default Settings Management

C. Identification and Authentication

1. Identifier Management
2. Authenticator Management
3. User Identification and Authentication
4. Device Identification and Authentication
5. Authenticator Feedback

D. System and Communications Protection

1. Communications Partitioning
2. Security Function Isolation
3. Information Remnants
4. Denial of Service Protection
5. Resource Priority
6. Boundary Protection
7. Communication Integrity
8. Communication Confidentiality
9. Trusted Path
10. Cryptographic Key Establishment

10. Cryptographic Key Establishment
11. Use of Validated Cryptography
12. Transmission of Security Parameters
13. Public Key Infrastructure Certificates
14. Mobile Code
15. System Connections
16. Message Authenticity
17. Secure Name/Address Resolution Service
18. Fail in Known State
19. Thin Nodes
20. Honeypots
21. Operating System-Independent Applications
22. Confidentiality of Information at Rest
23. Heterogeneity
24. Application Partitioning

E. System and Information Integrity

1. Flaw Remediation
2. Malicious Code Protection
3. Security Alerts and Advisories
4. Security Function Verification
5. Information Input Validation

V. Smart Grid Risk

A. Privacy Concerns

1. Fraud
2. Personal Behavior Patterns
3. Unauthorized Surveillance
4. Non-Grid Commercial Use of Data

B. Smart Grid and Electric Delivery Regulations

1. Alabama Title 37 Public Utilities
2. Arizona 42-5063
3. California General Provisions and Definitions
4. Colorado Article 25 Public Utility Commission Power to regulate utilities
5. Connecticut Chapter 98 and 101
6. Delaware Title 26 Public Utilities
7. District of Columbia Title 34
8. Florida Title 27 Regulated Utilities
9. Georgia Article 2 and 6
10. Hawaii 269-16 Regulation of utility rates
11. Idaho Title 61
12. Illinois Chapter 220
13. Indiana title 8
14. Kansas 66-101
15. Kentucky Title 24 Public Utilities Generally
16. Louisiana Public Utilities Definition
17. Maine Public Utilities
18. Maryland Statute 1-101 Definitions
19. Michigan Chapter 460
20. Minnesota Chapter 216-217
21. Montana Title 69 Public Utilities and Carriers

21. Montana Title 69 Public Utilities and Carriers
22. Nevada Title 58 Chapter 701
23. New York Electric Utility Cooperatives and Corporations
24. North Dakota Title 49
25. Ohio Chapter 743
26. Oregon Title 57
27. Pennsylvania Title 66
28. Rhode Island Title 39
29. South Carolina Article 3 Electric Systems
30. South Dakota Title 49
31. Tennessee Title 65 Chapter 4 Public Utility Commission Authority
32. Texas Code Title 2
33. Utah Title 54
34. Virginia Title 56 Section 580
35. Washington Title 54
36. Wisconsin Chapter 196
37. Wyoming Title 37

C. Smart Grid Vulnerabilities

1. Code Quality Vulnerabilities
2. Authentication Vulnerabilities
3. Authorization Vulnerabilities
4. Cryptographic Vulnerabilities
5. Environmental Vulnerabilities
6. Error Handling Vulnerabilities
7. General Logic Errors
8. Business Logic Vulnerabilities
9. Logging and Auditing Vulnerabilities
10. Path Vulnerabilities
11. Protocol Errors
12. Range and Type Error Vulnerabilities
13. Sensitive Data Protection Vulnerabilities
14. Session Management Vulnerabilities
15. Concurrency, Timing and Synchronization Vulnerabilities
16. Buffer Overflow Vulnerabilities

D. Smart Grid Risks

1. People
2. Training
3. Insufficient Background Checks
4. Inadequate Policies
5. Inadequate Patch/Firmware Processes
6. Inadequate Change Management
7. Inadequate Integrity Checking
8. Inadequate Network Segmentation
9. Inappropriate Protocol Selection
10. Weaknesses in Authentication Process or Keys
11. Insufficient Redundancy
12. Unnecessary System Access
13. Inadequate Audits
14. Inadequate Disaster Recovery

14. Inadequate Disaster Recovery
15. Inadequate Risk Management
16. Inadequate Incident Response

E. Use Cases

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