Center for Curriculum and Transfer Articulation

Introduction to Power Systems Security

Course: **CIS274DA**	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: Demonstrates distinct difference between control systems, used to control physics and computer information systems, used to process data, in the Power and Utility industry. Background information related to the Power Systems industry, elements and security risks. In-depth overview of how all elements of the power system function, as well as risks.

Requisites: Prerequisites: CIS272DB and PPT120, or permission of Instructor.

MCCCD Official Course Competencies

1. Explain the regulatory and security environment as it relates to Electric Power Systems, including the history of cyber security regulation for Power Systems (I).
2. Describe how the power system works conceptually, including all of the sub components that make up the Electric Power System (II).
3. Explain Power System specific concepts, key terms and definitions as they relate to the industry as a whole as well as in the security space (II).
4. Describe how security is implemented in Power Systems including from a compliance, threat, vulnerability and risk management perspective (III, IV).
5. Explain how risks to Power Systems are identified, managed and mitigated through the use of security principles and methodologies (IV).
6. Explain the standards which are applicable to the Power Systems Industry; NERC CIP, NEI, NIST IR 7628, NIST SP 800-82 (V).

MCCCD Official Course Outline

I. Power Systems Security Fundamentals
A. Standards and Laws
1. Energy Act of 2005
2. Energy and Security Act of 2007
3. Executive Order -- Improving Critical Infrastructure Cybersecurity
4. Federal Information Security Management Act
5. FERC Order 706
6. 10 CFR 74.54
B. Regulatory Organizations
1. Federal Energy Regulatory Commission
2. North American Electric Reliability Corporation
3. Nuclear Regulatory Commission

3. Nuclear Regulatory Commission
4. Public Utilities Commission

C. Important Government Organizations

1. US Department of Energy
2. Power Marketing Administrations
3. Bureau of Reclamation
4. Army Corp of Engineers
5. National Institute of Standards and Technology

D. Utility Services

1. Reliability Coordinator
2. Balancing Authority
3. Interchange Authority
4. Transmission Service Provider
5. Transmission Owner
6. Transmission Operator
7. Generation Owner
8. Generation Operator
9. Load-serving entity
10. Regional Entity

II. Power Systems Overview

A. Customer Enablement

1. Smart Meters
2. Home Area Networks
3. Mesh Networks
4. Wide Area Networks
5. Head end Systems
6. BackOffice
7. Meter Data Management System
8. Meter to Cash System
9. Protocols

B. Distribution System

1. Utility field sensors
2. Utility distribution and feeder meters
3. Utility field controllers
4. Local Access Networks
5. Sensor/meter aggregator
6. Wide Area Networks
7. Data Center Access
8. Sensor head end
9. Meter head end
10. Distribution SCADA master terminal units
11. Back office applications
12. Protocols

C. Transmission System

1. Energy Management System
2. Displays
3. Automatic Generation Control
4. Supervisory Control
5. Data Acquisition

5. Data Acquisition
6. Contingency Reserve Management
7. Interchange Scheduling
8. SCADA Master Terminal Unit
9. SCADA Front end processor
10. Relays
11. PLCs
12. RTUs
13. Protocols

D. Generation Systems

1. Local Area Networks
2. Wide Area Networks
3. Distributed Generation
4. Fossil Generation
5. Coal Generation
6. Gas Generation
7. Hydroelectric Generation
8. Nuclear Generation
9. Distributed Energy Resources
10. Microgrids
11. PLCs
12. RTUs
13. Control System Applications
14. Protocols

III. Security Concepts

A. Reliability

B. Operations Technology Infrastructure

1. Industrial Control Systems
2. Work Stations
3. Human/Man Machine Interface
4. Distributed Control System
5. Supervisory Control and Data Acquisition
6. Power System Applications

C. Assessments in Control System Environments

1. Vulnerability Assessments
2. Penetration Testing
3. Port Scanners
4. Wardialers

D. Control System Threats

1. Nation States
2. Environmentalists
3. Energy Thieves
4. System Instability

IV. Control Systems Security Practices

A. Security Policies

B. Access Control

1. Control System Access
2. Control System Network Access
3. Control System Remote Access

3. Control System Remote Access
4. Access to Control System Information
5. Personnel Access
6. Authorization
7. Accountability

C. Control System Network Security

1. Electronic Security Perimeter
2. Access Control Devices
3. Access Control Monitoring Devices
4. Ports
5. Network Accounts
6. Network Community Strings
7. Control System Network Vulnerability Assessment

D. Control System Security

1. Test Procedures
2. Ports and Services
3. Security Patch Management
4. Malicious Code Protection
5. Account Management
6. Security Monitoring
7. Disposal and Redeployment Policies
8. User/System Accounts
9. User/System Authentication
10. Control System Vulnerability Assessment

E. Control System Physical Security

1. Physical Security Plan
2. Protection of Physical Access Control Systems
3. Protection of Electronic Access Control Systems
4. Physical Access Control
5. Monitoring Physical Access
6. Logging Physical Access
7. Access Log Retention
8. Maintenance and Testing

F. Incident Response

1. Incident Characterization and Classification
2. Response Actions
3. Electricity Sector Information Sharing and Analysis Center (ES-ISAC)
4. Incident Response Plan

G. Recovery Plans

1. Disaster Recovery Strategy
2. Backup and Restore

H. Change Control and Configuration Management

1. Configuration Settings
2. Configuration Management
3. Managing Change
4. Hardware/Software Change Control

V. Control Frameworks

A. NIST Risk Management Framework

1. Components of Risk Management

1. Components of Risk Management
2. Multitiered Risk Management
3. Organization View of Risk
4. Business Process View of Risk
5. Control System View of Risk
6. Trust and Trustworthiness
7. Organizational Culture
8. Relationships among key risk concepts

B. NIST Security Authorization Process

1. Integrated Organization-Wide Risk Management
2. System Development Life Cycle
3. System Boundaries
4. Security Control Allocation
5. System Categorization
6. Security Control Selection
7. Security Control Implementation
8. Security Control Assessment
9. System Authorization
10. Security Control Monitoring

C. NIST Security Controls Catalogue
D. Security Control Organization and Structure
E. Security Control Baselines
F. Common Controls
G. Security Controls in External Environments
H. Security Control Assurance
I. Revisions and Extensions
J. Managing Risk
K. Categorizing the Control System
L. Selecting Security Controls
M. Monitoring Security Controls
N. NIST Security of Industrial Control Systems
O. NERC CIP
P. NEI 08/09
Q. NIST IR 7628

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