SCADA Fundamentals Certification

Overview

1. What is **S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition?
2. Components of a SCADA System

Field Devices

1. Remote Terminal Units (RTUs)
2. Programmable Logic Controllers (PLCs)
3. Flow Computers
4. Intelligent End Devices
5. Control Philosophies
6. Basic Feedback Control
7. Programming

Communications

1. SCADA Communication Medias
   - Radio
   - Satellite
   - Leased
   - TCP/IP

Data Acquisition Strategies

1. Protocol Fundamentals
   - Structure, Handshaking, Error Checking
2. Poll Models
   - Round Robin
   - Report by Exception
   - Spontaneous Report by Exception
   - Time Polling

Host Systems

1. Computer Operating System Choices
2. Host System Architectures and Control Strategies
   - Central Master
   - Distributed (Peer-to-Peer)
   - Hierarchical (Master/Sub-Master)
   - Hybrid
3. Host System Features
   - Polling Modules
   - Real-time Data Engines
   - Historical Data Engines
4. Standard SCADA Features
   - Alarm Management
   - Trending
   - Reporting
   - Calculation Packages
   - Audit Trails
   - Display Builders
   - Operator Interfaces

Networking

1. SCADA LANs
2. Network Protocols
3. Wide Area Networks
4. Redundancy Issues
5. Integrating SCADA LANs with Enterprise LANs
   - Decision Support Servers
   - Interfaces
   - Firewalls

Control Room Management

1. PIPES Act of 2006, Section 19
2. PHMSA ADB-05-06
   - Project Drivers
   - Control Room Management: Cross References
   - Conceptual Pipeline CRM Risk Management
3. API RP-1165, SCADA Displays
4. API RP-1167, Alarms

Alarm Management

1. Abnormal Situations, Alarms, Standards and Best Practices
2. Understanding and Evaluating Alarm Performance
3. Alarm System Design (for Enhanced Controller Support)
4. Alarm Redesign (Rationalization)
5. Implementing and Operating Alarm Systems
6. Situation Awareness (Best Practices in SCADA Screen Design)

Security

1. State of the Industry
2. Threats in the SCADA and Process Control Industries
3. Security Overview
   - Concepts: Threat Agents, Vulnerabilities, Exploits, and Risk
   - C.I.A. Triad (Confidentiality, Integrity, Availability) vs. A.I.C. Industry Priority
4. Technical Threat Agents
   - Viruses, Trojans, Worms, Malware
   - Cyber Attackers (Hackers and Insiders)
     - Classifications
     - Motivations
     - Hacker Methodology (Basic)
5. Technical Vulnerabilities in a SCADA Environment (General)
   - The Root of SCADA Application and Database Vulnerabilities
     - SCADA Protocols: Insecure by Design
     - Human Error
6. Beyond the Cyber Threat – Physical and Operational Security
   - Physical and Operational Attack Vectors to SCADA / PCN Systems
     - The Human Factor
     - Social Engineering 101
   - Case Study

Security (continued)

7. Best Practices and Beyond – A Security and Compliance Survival Guide
   - Comprehensive Security (Physical, Operational, and Cyber)
   - Due Diligence
   - Isolating Enterprise from SCADA / PCN
   - Layered Security
   - Remote Security: Using 2-Factor Authentication Coupled with Thin-Client Technology
   - Network Layer Security
   - Intrusion Detection Systems for SCADA / PCN
   - Physical Security 101
   - Security Training and Awareness Programs

Advanced Applications

1. Gas Management Systems
2. Liquids Management Systems
3. Leak Detection
4. Training Systems
5. Engineering Methods

Live SCADA System Administration Industry Best Practices

1. Skills for SCADA Professionals
2. SCADA Professionals for Job Task Analysis
3. Troubleshooting Skills for SCADA

SCADA Maintenance Planning

1. Change Requirement Identification
2. Risk Analysis
3. Detailed Execution Plan
4. Contingency Plans
5. Offline Development and Testing
6. Communications/Scheduling
7. Live System Deployment
8. Verification and Monitoring
9. Recent SCADA Advisory Bulletins

SCADA Forensics

1. Critical System Failure Analysis
2. Review of SCADA Problems and Alleviation
3. Discussion of Actual SCADA Mishaps
4. Best Practices Approach to SCADA Maintenance Activities

Revised 10-August-2009