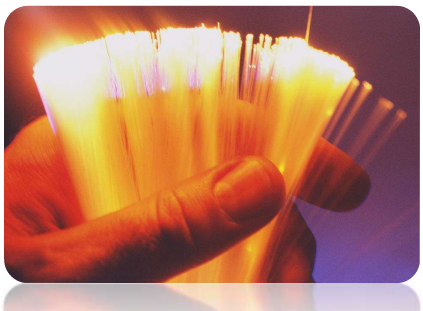
CS & ECE J444/544

Supervisory Control & Critical Infrastructure Systems

Lecture 28

23 April 2024



University of Idaho

1

Security for Control Systems

Jeff Pack

April 23,2024

2

Agenda

- Big Picture – Why Security?
- Risk Management
- Security Program
- OT vs. IT
- Security Controls
- NERC CIP
- Case Studies

University of Idaho

3

Why Security

- Business Decision
  - Electric Utilities – Major capital investments
  - Critical Infrastructure
- Return on Investment
  - Companies need to be comfortable with investment
  - Need to understand associated risks

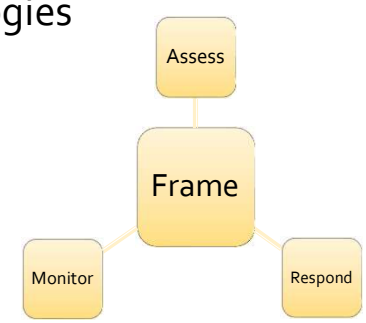
University of Idaho

4

Risk Management

- What is risk?
  - Probability vs. Consequence
  - Threat * Vulnerability * Asset Value
- Two Risk Methodologies
  - Quantitative
  - Qualitative
- Framework
  - Safety
  - Reliability

University of Idaho



5

Elements of a security program

- Security requires an organization
  - Managerial – Chief Information Security Officer and direct reports
  - Operational – Policy, strategy, regulation, audit
  - Technical – Analysts, engineers, subject matter experts
- Security Controls follow the same pattern

University of Idaho

6

OT vs. IT – Different Goals

- Communications
  - OT – Time critical
  - IT – Bandwidth critical
- Priorities
  - OT – Availability
  - IT – Confidentiality
- Foundations
  - OT – SCADA, Protection and Control
  - IT - Facebook

University of Idaho

7

OT vs. IT (continued)

- Functions
  - OT – Safety and Life Systems
  - IT – Financial and Commerce
- Environment
  - OT – Ruggedized Equipment
  - IT – Data Center
- Bottom Line – Each area has different requirements

University of Idaho

8

Security Controls

Def.: Safeguards to avoid, counteract or minimize security risks

- Organize
  - Managerial
  - Operational
  - Technical
  - Preventative
  - Detective
  - Corrective
  - Physical
  - Procedural
  - Technical
  - Legal

University of Idaho

9

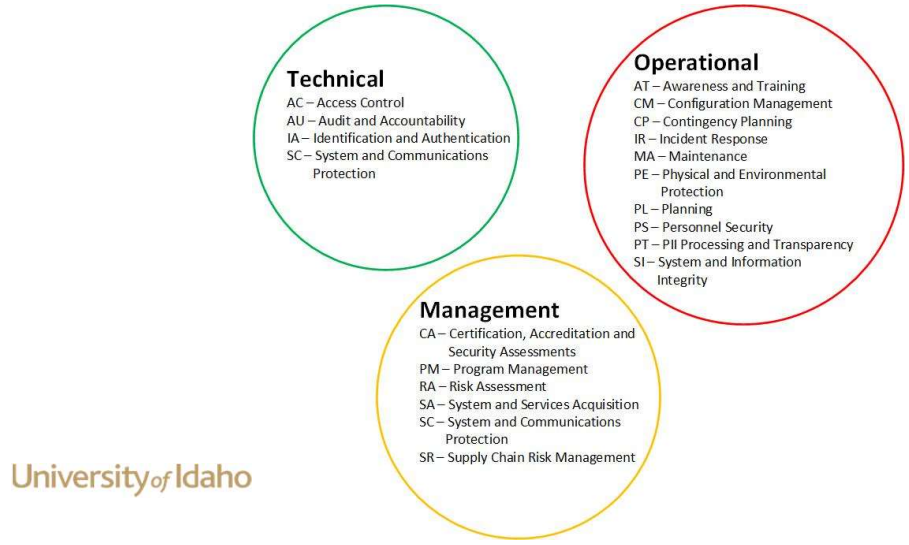
Security Controls

- Most Important Elements of Security Controls
  - Effective
  - Repeatable
  - Measurable
  - Auditable

University of Idaho

10

Examples – NIST 800-53 Rev. 5 20 control families



University of Idaho

11

Technical Control Examples

- Access Control
- Identification and Authentication
  - Identity and Access Management (IAM)
- Audit and Accountability

University of Idaho

12

Operational Control Examples

- Awareness and Training
- Incident Response
- Configuration Management
- Personnel Security

University of Idaho

13

Management Control Examples

- Risk Assessment
- System and Service Acquisition
- Supply Chain Management
- Program Accreditation

University of Idaho

14

Electric Utility Regulation

- Federal Energy Regulatory Commission - FERC
  - Regulates the interstate transmission of electricity, natural gas, and oil
- North American Electric Reliability Corporation - NERC
  - Assure the reliability of the bulk power system in North America

University of Idaho

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

15

NERC CIP Standards

- Why CIP?
  - Pop Quiz: August 14, 2003
    - Hint: This event led to the creation of the Energy Policy Act of 2005 and in turn, NERC CIP
  - CIP Goal - Identify and protect critical assets to support reliable operation of the Bulk Electric System

University of Idaho

16

NERC CIP Standards

- CIP-002-5.1a – BES Cyber System Categorization
- CIP-003-8 – Security Management Controls
- CIP-004-7 – Personnel and Training
- CIP-005-7 – Electronic Security Perimeter(s)
- CIP-006-6 – Physical Security of BES Cyber Systems
- CIP-007-6 – Systems Security Management
- CIP-008-6 – Incident Reporting and Response Planning
- CIP-009-6 – Recovery Plans for BES Cyber Systems
- CIP-010-4 – Configuration Change Management and Vulnerability Assessments
- CIP-011-3 – Information Protection
- CIP-012-1 – Communications between Control Centers
- CIP-013-2 – Supply Chain Risk Management
- CIP-014-3 – Physical Security

17

CIP 002

- CIP-002-5.1a – BES Cyber System Categorization
  - What devices are in scope?
  - What types of devices impact the Bulk Electric System?
    - Protective Relays
    - Management Systems (EMS, DMS)
    - Communications Systems
  - How much impact

University of Idaho

18

CIP 003

- CIP-003-8 – Security Management Controls
  - Policies for High and Medium Impact devices
  - Low Impact requirements
    - Incident Response
    - Awareness and Training
    - Electronic Security
    - Physical Security
    - Transient Cyber Assets and Removable Media

University of Idaho

19

CIP 004

- CIP-004-7 – Personnel and Training
  - Awareness and Training
  - Personnel Security
    - Identity Proofing
    - Background Check
    - Criminal History

University of Idaho

20

CIP 005 and 012

- CIP-005-7 – Electronic Security Perimeter
  - Access Control - Firewalls
  - Authentication
  - Authorization
  - Logging
  - Malicious Code Protection
- CIP-012-1
  - Protecting comms between control centers

University of Idaho

21

CIP 006 and 014

- CIP-006-6 – Physical Security
  - Access Control
  - Monitoring
  - Logging
- CIP-014-3 – Transmission Physical Security
  - Identify critical locations (N-1 reliability study)
  - Identify threats and vulnerabilities
  - Develop a physical security plan

University of Idaho

22

CIP-007

- CIP-007-6 – System Management
  - Logical Ports and Services
  - Patch Management
  - Malicious Code
  - Event Logging
  - Password and Account Management

University of Idaho

23

CIP-008 and CIP-009

- CIP-008-6– Incident Response
  - Identify, respond and recover from unexpected bad things
    - Attackers
    - Malicious Code
- CIP-009-6 – Recovery
  - Identify, respond and recover from expected bad things
    - Hardware and/or Software Failure

University of Idaho

24

CIP-010

- CIP-010-4 – Configuration Management
  - Baseline configuration
  - Review and approve changes
  - Vulnerability assessments

University of Idaho

25

CIP-011 and 013

- CIP-011-3 – Information Protection
  - Protect Sensitive Information
  - Device Reuse and Disposal/Sanitization
- CIP-013-2 – Supply Chain Risk Management
  - Develop Risk Management Plan
  - Implement Risk Management Plan

University of Idaho

26

Case Studies

University of Idaho

27

Colonial Pipeline

- May 2021
  - Ransomware on Business Systems
  - Business Decision to Shutdown Pipeline
  - No OT Security Issues
  - Impacted Business

University of Idaho

28

Ukraine

- December 2015 and 2016
  - 2015 Sandworm Attack
    - Sixty (60) Distribution substations
    - 230,000 out of power
    - Accessed
    - Spearphishing operators and sysadmins
    - Harvested account information
    - Disabled UPS systems
    - Flashed malicious firmware to protocol converters

University of Idaho

29

Ukraine

- December 2015 and 2016
  - 2015
    - Sent staff to manually operate equipment in substations
    - Power restored ~6 hours
  - 2016 Sandworm Attack
    - Similar attack used modular malware to gain access
    - Transmission substations
    - Restored via manual control in ~1 hour

University of Idaho

30

Ukraine

- June 2022
  - ELECTRUM compromised MicroSCADA hypervisor
  - Persistent access via backdoors
- October 2022
  - MicroSCADA used to execute malicious commands
  - Coordinated with missile attacks on critical infrastructure

University of Idaho

31

Metcalf

- April 16, 2013
  - Communication line failures
    - Fiber cut
  - 50 to 100 gunshots
    - 57 transformer radiators damaged
    - 58,000 gallons of oil spilled

University of Idaho

32

Metcalf

- Issues
  - Communications
    - Better understanding of terminology
      - They're taking out our 500 kV transformers!
        - Physical security guys think it's theft
        - T&D Operators understand transformers are out of service
  - Physical Security
    - Fencing – need larger perimeter
    - Cameras – need focus on external points of entry

University of Idaho

33

Metcalf

- Issues
  - Physical Security (continued)
    - Vegetation – blocked view
    - Signage – transformers identified lines
    - Communication Vaults not locked or alarmed
- Fixes
  - Concrete walls
  - Better video surveillance
  - Gunshot Detectors

University of Idaho

34

Stuxnet (if there is time left)

- Malware with specific target
  - Uranium enrichment centrifuges in Iran
  - Uses Siemens PLCs to control centrifuge
  - Changed speed but made display look normal
- How did it do it?
  - Utilized four zero-day exploits and four other mechanisms to get on field PCs
  - Spread via USB devices – not via network
  - Initially seeded in Iran to focus on targets
- Lots of details in how they wrote the code and kept it from detection
- World's first known ICS malware proactive attack that damaged equipment

University of Idaho

35

Future

- AI and Machine Learning
- World of Software
- Distributed Energy Resources
- Microgrids

University of Idaho

36