Cybersecure Operation of PLCs and RTUs

Image by Adobe Firefly

MLM-035-C

Industry	– Process
Principal Role	– Owner
Professional Role	– Control Engineer
Enterprise Phase	– Master Planning

Turn on your audio and click start to begin video

START

PRINT VERSION OF NARRATIVE

This Micro-Learning Module (MLM) discusses principles for the secure operation of PLCs and RTUs. It describes recommended precautions and procedures as well as a work process for responding to anomalous events such as operating errors or cyber attacks.

The intended audiences for this MLM are ACS engineers, IT teams dealing with ACS cyber defense, consultants, systems integrators, and managers making decisions about how to achieve ACS cyber security.

PLC and RTU Cybersecurity Measures

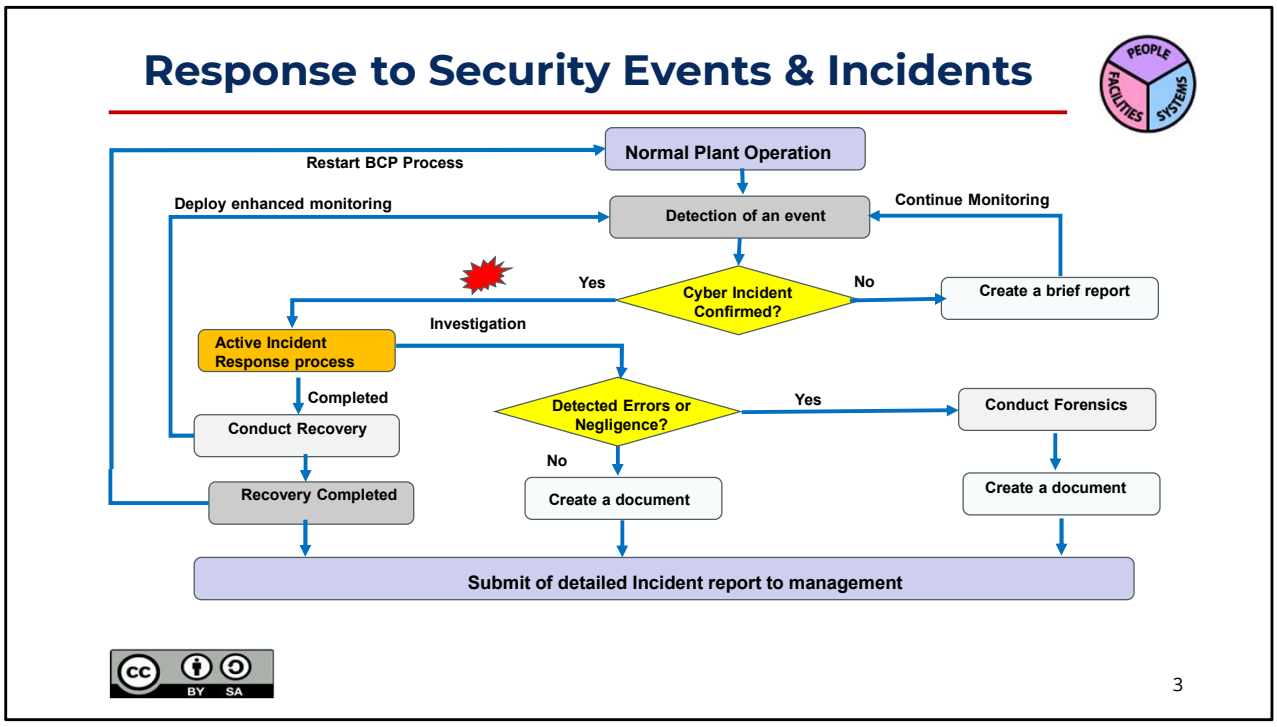
Security control

- Physical security control within defined boundaries
- Password assignment and management (different for ACS, OT, and IT zones)
- Always maintain “Golden Image copy” of PLC/RTU & HMI programs
- Permit Remote access using only secure, approved methods
- PLCs/RTUs must be “locked down” to prevent unauthorized changes
- Monitor industrial data transmission (for suspicious patterns)
- Integrate cybersecurity alarms into plant operating procedures
- Track Target Security Levels and Achieved Security Levels
- Track Maturity Level of cybersecurity practices
- Respond to cybersecurity incidents according to company policies

The following PLC cybersecurity measures are discussed:

Security control

- Physical security control within defined boundaries
- Password assignment and management (different for ACS, OT, and IT zones)
- Always maintain “Golden Image copy” of PLC/RTU & HMI programs
- Permit Remote access using only secure, approved methods
- PLCs/RTUs must be “locked down” to prevent unauthorized changes
- Monitor industrial data transmission (for suspicious patterns)
- Integrate cybersecurity alarms into plant operating procedures
- Track Target Security Levels and Achieved Security Levels
- Track Maturity Level of cybersecurity practices
- Respond to cybersecurity incidents according to company policies



This is an example of an approved workflow for addressing security incidents detected by operations.

In the event that the incident is confirmed to be a Cybersecurity Incident (e.g., a cyber attack or operating error) , the required incident response work process is described, including reporting requirements.

Recommended ACS Cybersecurity Actions

- **Control physical perimeter access**
  - Mount in a secure area, and lock cabinets where feasible
  - Block unused ports (e.g., USB and LAN ports)
  - Prevent connection of unauthorized devices to the network
- **Control Logical Security**
  - Password management (together with H/R)
  - "Golden Image" copy for all programs and validation processes for changes
  - Programming devices must never be connected to the internet
- **Asset Inventory Management**
  - Maintain accurate asset inventory for all intelligent industrial devices
  - Track Vulnerability Bulletins from CISA and applicable vendors

The following ACS Cybersecurity Actions are recommended:

Control physical perimeter access
- Mount in a secure area, and lock cabinets where feasible
- Block unused ports (e.g., USB and LAN ports)
- Prevent connection of unauthorized devices to the network

Control Logical Security
- Password management (together with H/R)
- "Golden Image" copy for all programs and validation processes for changes
- Programming devices must never be connected to the internet

Asset Inventory Management
- Maintain accurate asset inventory for all intelligent industrial devices
- Track Vulnerability Bulletins from CISA and applicable vendors

Software Patching and Updates

- **PLC / RTU Patching**
  - Apply company PLC Patching and Update procedures
  - Patching & Update instructions should be clearly defined for each device
  - In every case, a decision is required on whether patches or updates are urgent
  - If possible, conduct non-urgent patches during planned shutdowns
  - Use only certified programming devices for a specific plant
- **Testing all control devices and industrial computers**
  - As a part of the initial acceptance procedure
  - After modification of programs or hardware
  - After updates of the application program
  - After significant repairs/modifications and before equipment restart

Software patching and updates require the following:

PLC / RTU Patching
- Apply company PLC Patching and Update procedures
- Patching & Update instructions should be clearly defined for each device
- In every case, a decision is required on whether patches or updates are urgent
- If possible, conduct non-urgent patches during planned shutdowns
- Use only certified programming devices for a specific plant

Testing all control devices and industrial computers
- As a part of the initial acceptance procedure
- After modification of programs or hardware
- After updates of the application program
- After significant repairs/modifications and before equipment restart

Asset Inventory Management

- **Tracking both Hardware and software assets**
  - Adhere to the company's Asset Management process
  - Manage data in the Configuration Management System
  - Use Intrusion Detection System (IDS) for scanning
  - Use the PLC/RTU vendors' maintenance tools
- **Tracking the Vulnerability Bulletins for each device**
  - Received from the product vendor
  - Obtained from periodic publications from CISA
- **Corrective actions**
  - Always act according to urgency and criticality
  - Perform thorough operational testing after completion

An Accurate Asset Inventory is essential and requires:

Tracking both Hardware and software assets
- Adhere to the company's Asset Management process
- Manage data in the Configuration Management System
- Use Intrusion Detection System (IDS) for scanning
- Use the PLC/RTU vendors' maintenance tools

Tracking the Vulnerability Bulletins for each device
- Received from the product vendor
- Obtained from periodic publications from CISA

Corrective actions
- Always act according to urgency and criticality
- Perform thorough operational testing after completion

Monitor Operating Data Flows

- **Monitor data transmissions (for suspicious patterns)**
  - Detect anomaly conditions and behavior for each zone (ACS, OT, and IT)
  - Verify that commands are issued only from authorized locations
  - Monitor data transmissions and compare to the typical baseline
  - Monitor parameter values and rates
- **Minimize the use of "external" programming tools**
  - Use of on-site tools owned by the operator
  - Never connect through public internet, and preferably not wireless media
  - Install updates using only genuine CDs and hardware from the vendor
- **Configuration Management systems – ref; ISA 108**
  - https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa108

It is recommended to monitor and control operating data flows including:

Monitor data transmissions (for suspicious patterns)
- Detect anomaly conditions and behavior for each zone (ACS, OT, and IT)
- Verify that commands are issued only from authorized locations
- Monitor data transmissions and compare to the typical baseline
- Monitor parameter values and rates

Minimize the use of "external" programming tools
- Use of on-site tools owned by the operator
- Never connect through public internet, and preferably not wireless media
- Install updates using only genuine CDs and hardware from the vendor

Configuration Management systems – ref; ISA 108

Author

Daniel Ehrenreich

Daniel has over 33 years of experience with the control of industrial operations and the integration of cybersecurity solutions.

He is a control engineering consultant, workshop lecturer, and an expert in cyber-secure operation for ACS.

Daniel has contributed his knowledge and expertise to multiple ISA 62443 workgroups.

Since 2016, acting as the Chairman of the annual ICS-Cybersec Conference taking place in Israel

Please click here to provide feedback on this MLM.

Daniel Ehrenreich has over 32 years of experience in controlling industrial operations and integrating cybersecurity solutions.

He is a control consultant, workshop lecturer, and expert at SCCE- Secure Communications and Control Experts. Daniel has also contributed his expertise to multiple ISA 62443 workgroups and conducted free podcast sessions to educate engineers worldwide. Since 2016, acting as the Chairman of the annual ICS-Cybersec Conference taking place in Israel.