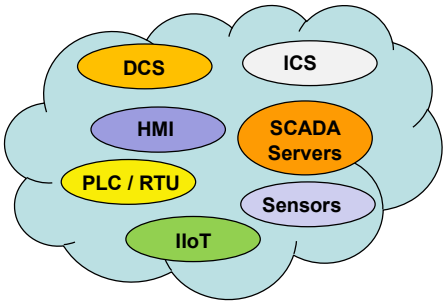
How to Implement Minimum Trust in Automation and Control Systems (ACS)

MLM-018-C

Industry	– All
Principal Role	– All
Professional Role	– Control Engineer
Enterprise Phase	– All



Turn on your audio and click start to begin video

START

This Micro-Learning Module discusses how to apply “Zero-Trust” principles to Industrial Automation and Control Systems (ACS). It explains that although Zero Trust principles are applicable in both IT systems and ACS zones. Each has different objectives and priorities, and must be implemented differently.

The intended audience for this MLM includes Control Engineers, System Integrators, and managers making decisions related to secure ACS, as well as IT personnel interfacing with these ACS.

Click the START button to advance.

Cyber-security Model for Industrial Organizations

- **Zero Trust IT Cyber-security Model**
  - The term "Zero Trust Model" or Zero Trust Network Access (ZTNA) was defined by Gartner ™ as "Never Trust-Always Verify".
  - This aims to prevent access to IT systems unless the user and device are authenticated and authorized.
- **Minimum Trust ACS Cyber-security Model**
  - Some principles of an IT-related Zero Trust Model cannot be applied to ACS, and a different model is required
  - For ACS, it is necessary to use a safer and more reliable model that might be called a "Minimum Trust Model"
- **Both Models are needed in an industrial enterprise**
  - New cyber threats mean that industrial enterprises must upgrade the cyber defense of both IT and ACS zones. However these have different objectives and require different solutions.

The Zero-trust Model is designed to prevent unauthorized access to IT systems. It adheres to the guideline "Never Trust-Always Verify." Using this Zero-trust model, every connection is authenticated before it is allowed.
For example, employees and service providers are increasingly required to remotely connect to IT systems on the enterprise network. This created increased risks that the Zero-trust model is proposed to address.

At the same time, remote maintenance and support of ACS is becoming more common, even including the remote operation of facilities. However, the safety and reliability requirements of an ACS meant that a Zero-trust model is not practical.

While both IT and ACS cybersecurity models are necessary in an industrial enterprise, they have different objectives and priorities. With IT systems, Confidentiality, Integrity, and Availability objectives are prioritized as CIA. However, with ACS, safety of the facility is by far the most important objective, and objectives are prioritized as Safety, Availability, Integrity, and Confidentiality, or S A I C.

Key Security Questions to be Asked

- **Who is requesting access?**
  - To which ACS zone and/or device the access is requested
  - Should the user and their device be authenticated and authorized?
- **Which device will be accessed ?**
  - Referring to a specific targeted zone of the industrial plant?
  - Different defense measures are needed for ACS (e.g., HMI, PLC)
- **What is the purpose for connecting?**
  - Referring to a specific device in the targeted zone?
  - Is the connecting entity authorized for that action?
- **From where is the connection initiated?**
  - Can the originating location be authenticated and certified?

3

The following are some key security questions that are asked to determine whether access can safely be granted.

Who is requesting access?

Is the requester authenticated, and if authenticated, is the requester authorized?

Is the requesting device authenticated, and if so, is it authorized?

To which ACS zone is access requested?

Which device in this zone will be accessed?

Different defense measures are needed for different ACS zones and devices (e.g., HMI, PLC)

What is the purpose for connecting

Referring to a specific device in the targeted zone?

Is the connecting entity authorized for that action?

From where is the connection initiated?

Can the originating location be authenticated and certified?

Reference to the Architecture Model 1/2

- **Specific defense may be selected for each Architecture Level**
  - The technology solution must be specifically adapted to the system architecture, the deployed products, and subsystems
  - Assume that threats exist inside and outside the network
  - No single failure may take down the whole Automation and Control System (ACS)

- **PERA Level 0 & 1 hardware, software and networks**
  - The defense methodology must not rely on the integrity of any single device serving a critical function
  - All critical devices must be physically protected to prevent unauthorized access.
  - Failed Access attempts to these devices must be monitored, and an alert must be sent to the HMI and the Alarm Management System in the control room
  - If a controller fails, or operates outside of its configured limits, an alert must be sent to the HMI and the Alarm Management System in the control room

Specific defense is selected for each Architecture Level

The technology solution must be specifically adapted to the system architecture, the deployed products, and subsystems.

Assume that threats exist inside and outside the network

No single failure nay take down the whole ACS operation

PERA Level 0 & 1 hardware, software, and networks

The defense methodology must not rely on the integrity of any single device serving a critical function

All critical devices must be physically protected to prevent unauthorized access.

Access attempts to these devices must be monitored, and an alert must be on the HMI screen in the control room

In case a controller operates outside of its safety boundary, an alert must be on the HMI screen in the control room

Reference to the Architecture Model 2/2

- **Level 2 hardware, software and networks**
  - All computers serving the ACS architecture must be hardened according to instructions of the vendor
  - The defense methodology must not rely on the regular operation of any single computer serving a critical function
  - Direct Remote access must be prevented.
  - Authenticated connection sessions via the IT network shall be supervised, minimized, and conducted subject to approval.
- **Level 3 hardware, software and networks**
  - All computers serving the ACS architecture must be hardened according to instructions of the vendor
  - Authenticated connection sessions via the IT network shall be supervised, minimized, and conducted subject to approval.
  - All actions and sessions related to the ACS must be documented

Level 2 hardware, software and networks

All computers serving the ACS architecture must be hardened according to instructions of the vendor

The defense methodology must not rely on the regular operation of any single computer serving a critical function

Direct Remote access must be prevented.

Authenticated connection sessions via the IT network shall be supervised, minimized, and conducted subject to approval.

Level 3 hardware, software and networks

All computers serving the ACS architecture must be hardened according to instructions of the vendor

Authenticated connection sessions via the IT network shall be supervised, minimized, and conducted subject to approval.

All actions and sessions related to the ACS must be documented

Defense Model for Cyber Secured ACS

- **Deploying Minimum Trust Model for ACS**
  - The solution must meet the Safety-Availability-Integrity and Confidentiality (SAIC) requirements for each ACS zone.
  - This is likely to require a different strategy than "Zero Trust" used in IT systems

- **The SAIC Model Principles**
  - Must ensure the safety of people, plant, equipment, and the environment
    - Regardless of a human's attack, failure, or mistaken action.
  - Availability is critical for uninterrupted operation
    - To ensure consistent and quality products in the facility
  - Data Integrity is critical to ensure reliable operation
    - Preventing frequent downtime for maintenance as well as ensuring safety integrity
  - Data Confidentiality is often less critical
    - Adversaries might use the information to prepare large attacks

Now let's dive deeper into deploying a Minimum-trust model for the ACS, but before that, we must make it clear that any solution one may select must meet the principles of Safety-Availability-Integrity and Confidentiality (SAIC) as applicable for each system.

To comply with the SAIC Principles, the top priority requirement is that it must assure the safety of people and the machinery. Safety must be guaranteed regardless of whether the incident was caused by an attack, failure, or mistaken action.
The availability of the ACS is critical for uninterrupted operation and to assure consistency and quality production in the facility.

Data Integrity is critical to ensure reliable operation and prevent frequent downtime for maintenance.

Data Confidentiality is usually less critical for most industrial plants, but adversaries might use the acquired information to prepare large attacks.

Minimum Trust Model for Secure ACS 1/2

- **Reaching the Minimum Trust goals for ACS**
  - ACS zones must be segregated from each other and IT networks to improve "Resilience"
- **Strong Segregation**
  - May require Controlled Gateways, data diodes, Managed Firewalls, or a Demilitarized Zone (DMZ)
- **Integration with IIoT**
  - All IIoT devices linked to the ACS zone must have a unique identity.
  - May never control hazardous equipment or directly influence process operations.
- **Secured remote access**
  - Remote monitoring of ACS must be protected through a secure, audited perimeter defense
  - Remote control access must be subject to full authorization and authentication.

Now let's outline a couple of technology-based practices for deploying the Zero Trust model for ACS.

Each ACS zone must be segregated from the lower hierarchy ACS zone and the IT zone in the organization exposed to the internet. The segregation process aims to minimize the risk of unauthorized access to the ACS network. It can be achieved by deploying a unidirectional appliance (Diode) or a Next-Generation Firewall (NGFW). All IIoT devices (regardless of where they reside) must be defined by the system integrator with a unique identity that the ACS recognizes. No matter where the IIoT devices live, they must be protected against unauthorized access and manipulation of their operation process.

For cloud-based processes used for analyzing an industrial function (vibration, flow, heat, noise, etc.), the IIoT device securing that process needs to be defined for least privilege permission.

Where applicable, and specifically for safety-critical processes, the Purdue level-0 defense shall be considered.

Minimum Trust Model for Secure ACS 2/2

- **The ACS should include a Network Intrusion Detection System (NIDS) to detect suspicious activity**
  - The data flow from and to each ACS and IIoT device should be monitored for anomalous behavior.
  - ACS should avoid non-secured or lightly secured wireless communications.
- **External service providers must validate any service device that could be infected.**
  - For critical facilities, use a dedicated laptop and/or dedicated engineering workstation for supporting ACS devices
  - ACS support laptops may never be used for email, web search, etc.
  - Unused physical ports and non-essential protocols must be disabled
- **HW & SW must be received in factory-secured packages**
  - Prevent the possibility of unauthorized manipulation

Let's continue with a few more ACS-related topics.

The secured ACS architecture shall include a Network Intrusion Detection System (NIDS) for detecting vulnerable transactions and actions. The data flow to/from all IIoT ecosystem devices and the ACS must be consistently monitored to detect anomalous behavior. The ACS architecture shall minimize the use of unsecured wireless media. External service providers must not be authorized to connect their laptops, which are often used in other facilities, and might be accidentally infected. It is essential to note that if an anomaly is detected, do not take panic action, as this could lead to a safety incident.

When purchasing hardware and software for your ACS, always ensure that it is received in its factory-original sealed package. This will prevent the possibility of unauthorized manipulation before delivery. Furthermore, important to mention that software updates must be obtained only from an authorized vendor and delivered to the ACS via a secure channel.

Further Information and Reading

- **Related MLMs**
  - MLM-007-A ACS Architectures
  - MLM-014-A Definition of IT, OT, and ACS Terms
  - MLM-034-A – Understanding IT-ACS Integration

- **References and Further Information**
  - https://www.tigera.io/learn/guides/zero-trust/zero-trust-security/?gclid=Cj0KCQjwy5maBhDdARIsAMxrkw3YJfRlE3vERjdgAdUe_k07vid1CcT9K_slVkqq11y9qa2hmet9WxIaAuzHEALw_wcB

  - Please CLICK HERE to provide a comment to the author.

Thank you for taking the time to interact with this MLM.

Readers are invited to provide comments on how this content can be improved. The Comment link is directed to a permanent record attached to this document. This is routed to the author and subject matter experts for attention in revising the content and is an essential input to our quality control.

About the Author

Daniel Ehrenreich

Consultant, workshop lecturer, SCCE- Secure Communications and Control Experts. Daniel has over 32 years of experience with control solutions of industrial operations and integration with Cyber security.

Acting as an expert and volunteer contributor to multiple PERA 62443 workgroups.

My name is Daniel Ehrenreich, and I'm acting as a consultant and workshop lecturer at SCCE-Secure Communications and Control Experts, based in Israel.

I have over 32 years of experience with control solutions for industrial operations and integration with cybersecurity solutions. I also act as an expert and volunteer contributor to PERA and multiple ISA 62443 workgroups.