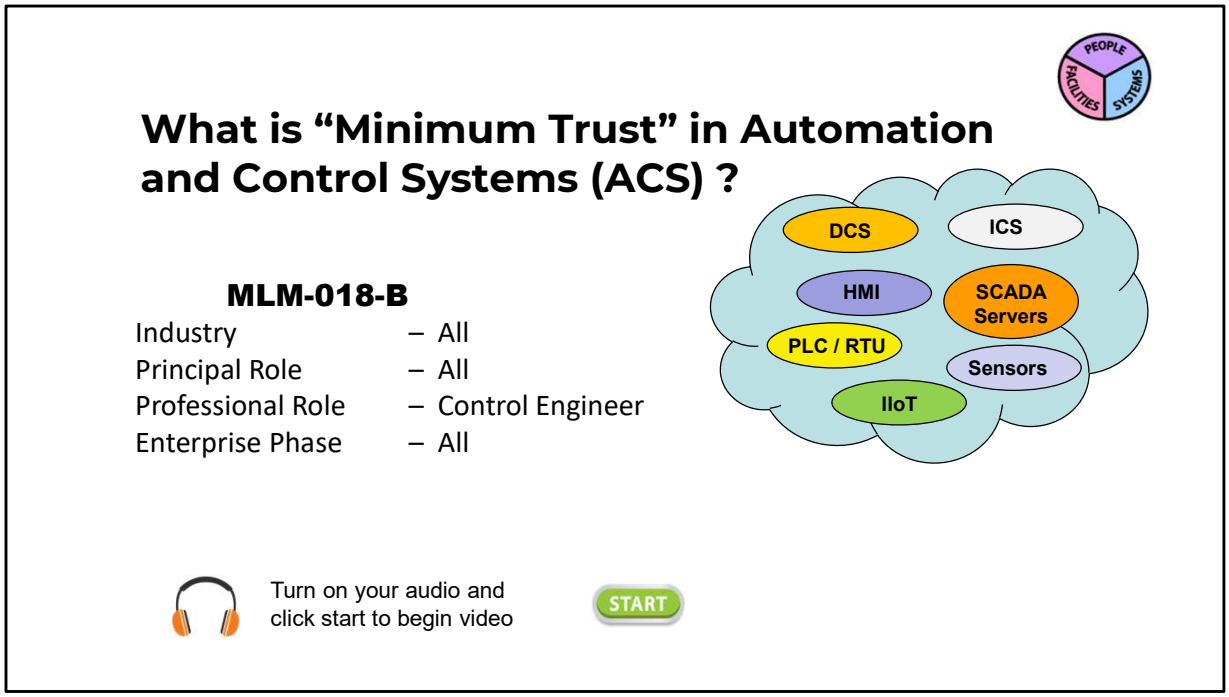

This Micro-Learning Module discusses the concept of “Minimum-Trust” in Industrial Automation and Control Systems (ACS).

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.

What Does "Minimum Trust" Mean?

ISA 62443-1-1 defines "Least Privilege" for ACS systems as:

A security principle that a system or component restricts the access privileges of users to the **minimum** necessary to accomplish assigned tasks.

- In order to align with "Zero Trust" as defined by IT systems: PERA defines "Minimum Trust" as the minimum privilege necessary for a user to accomplish assigned tasks.
- This "Minimum Trust" definition will facilitate communication between ACS and IT professionals when designing OT systems that involve both groups.

ISA 62443-1-1 defines "Least Privilege" for ACS systems as: "a security principle that a system or component restricts the access privileges of users to the minimum necessary to accomplish assigned tasks".

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.

Why may “Minimum Trust” be Necessary in ACS?

- **Key Professional Roles may require Limited Trust such as:**
  - **Process Operator**
    - Equipment is remotely operated
    - Fully trained Operators are not available, and personal certifications must be checked.
  - **Process Engineer**
    - May optimize settings, but procedures require operators to make all adjustments
    - Need remote optimization support such as UOP™ Remote Process Optimization
  - **Maintenance Technicians**
    - May repair equipment but not start or adjust it.
    - May connect and use diagnostic equipment (even in hazardous environments)
    - May order parts and supplies using IT purchasing and Inventory systems

Key Professional Roles may require Limited Trust such as:

Process Operator
Equipment is remotely operated
Fully trained Operators are not available, and personal certifications must be checked.

Process Engineer
May optimize settings, but procedures require operators to make all adjustments
Need remote optimization support such as UOP™ Remote Process Optimization

Maintenance Technicians
May repair equipment but not start or adjust it.
May connect and use diagnostic equipment (even in hazardous environments)
May order parts and supplies using IT purchasing and Inventory systems

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?
- **To which ACS Zone is access requested ?**
  - Which device in this zone will be accessed?
  - 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?

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?

How "Minimum Trust" May be Implemented

- **"Limited Trust" may be implemented by:**
  - 1) People (written instructions),
  - 2) Automation and Control Systems themselves (that limit actions by "workstation" or "Login", or
  - 3) IT systems (e.g., checkout of stores equipment by user).
- **Some means to identify individuals** and their Professional Roles is necessary with 2) and 3).
- **Must first assess Risks** from:
  - incorrect actions (errors or malicious actions)
  - limitations placed on Individuals or failure of enforcement systems.

"Limited Trust" may be implemented by:
1) People (written instructions),
2) Automation and Control Systems themselves (that limit actions by "workstation" or "Login", or
3) IT systems (e.g., checkout of stores equipment by user).

Some means to identify individuals and their Professional Roles is necessary with 2) and 3).

Must first assess Risks from:
incorrect actions (errors or malicious actions)
limitations placed on Individuals or failure of enforcement systems.

How "Minimum Trust" May be Implemented

- **Clearly, more cybersecurity models are needed than only "Full Trust" and "Zero Trust".**
  - However, too many different trust models in one facility may confuse personnel
- **Consider the following Example Trust Levels, TL0 to TL3**
  This is similar to the Security Levels SL1 to SL4 used in ISA 62443
  - Trust Level 3 - Full Trust
  - Trust Level 2 - Limited Trust
  - Trust Level 1 - Minimum Trust
  - Trust Level 0 - Zero Trust
- **What precautions are applied for each Trust Level** can be defined in the company's Cybersecurity Master Plan, or in Operating Practices at each facility

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.

Example of "Trust Level 3"

- **The default is "Full Trust" for trained personnel who are physically at the plant**

- **In process plants, key Professional Roles including:**
  - Process Operator – may adjust equipment and processes but not maintain it.
  - Process Engineer – may optimize settings but must direct operators to make adjustments
  - Maintenance Technicians – may repair and replace equipment but not adjust it.

- **In mature, fully-staffed organizations:**
  - These roles are established by operating procedures and enforced by management
  - Staff are physically present, trained, and qualified for their roles
  - Roles are implemented by people who know each other and their respective roles.
  - contractors or vendors come to the plant to perform their roles.

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.

Example of Trust Level 2 "Limited Trust"

- **"Limited Trust" may be given to Professional Roles or Individuals:**
  - If there is not a full compliment of Professional roles physically at the plant
  - If some of the staff are not fully trained or certified for their roles.
  - Some means to identify individuals and their Professional Roles is necessary with 2) and 3).
  - Risks may result from incorrect actions (errors or malicious actions)
  - However, limitations placed on Roles or Individuals may also cause risks.

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.

Example of Trust Level 1 – Minimum Trust?

- **Key Professional Roles may require Limited Trust such as:**
  - Process Operator
    - Equipment is remotely operated
    - Operator training on some units is not available, and remote support is required.
  - Process Engineer
    - may optimize settings but must direct operators to make adjustments
  - Maintenance Technicians – may repair and replace equipment but not adjust it.

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.

Example of Trust Level 0 – Zero Trust

- **Limited to plant personnel responsible for high value non-time critical transactions:**
- **Examples might include:**
  - Authorizing pipeline transfers
  - Releasing Quality test data to clients
  - Authorizing tanker truck loading

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.

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.