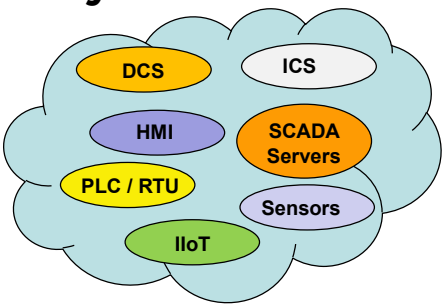
What are Zero Trust and Full Trust in Plant Control and Information Systems

MLM-018-A

Industry	– Process
Principal Role	– All
Professional Role	– Control Systems and IT
Enterprise Phase	– All



Turn on your audio and click start to begin video

START

This Micro-Learning Module discusses principles of “Zero” and “Full” Trust in Plant Control and Information Systems. It explains that although Cybersecurity Trust principles are applicable in both IT systems and ACS zones, each has different objectives and priorities, and must be implemented in a distinct manner, utilizing different infrastructure and skill sets.

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 is "Full Trust" in ACS

- **Trust is associated with Org Chart Positions and Individual Personnel**
  - The default is "Full Trust" for Key Professional Personnel working with hazardous equipment.
  - They have physical access to devices (including plant equipment and HMIs)
  - They can carry out any operation that they are trained for and according to plant operating procedures.
- **In process plants, Key Professional Roles include:**
  - 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.

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.

What is "Full Trust" in ACS

- **There are, however, many "Plant Support Roles" such as:**
  - Plant Management, Plant Engineering, Laborers, and Security staff
  - These may have physical access to hazardous devices, but are "Trusted" to not carry out actions for which they are not authorized.
- **Finally, there are many more "Non-Plant Roles such as:**
  - Clerical staff, Human Resources, Schedulers, and others who do not have physical access to hazardous plant devices.
  - These Roles may change information in systems with large impact, for example:
    - Clerical staff might authorize fraudulent financial transactions
    - Schedulers might schedule service on the wrong unit.
- Management considers that the risks do not justify any technical measures to limit Trust at their 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.

What is "Full Trust" in ACS

- **Thus, no technical measures are used to ensure that Trust is not abused.**
  - Selected physical areas or equipment may be locked ("failure mode" is well understood)
  - The only risk is from unauthorized actions of personnel (deliberate or unintentional).
- **This strategy may be chosen in mature, fully-staffed organizations if :**
  - Position descriptions are established by operating procedures.
  - Personnel who carry out actions for which they are not authorized are disciplined 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.

What is "Zero Trust"

- **Zero Trust 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.
  - Every time a connection is established, the full set of checks must be passed. If the connection attempt fails, the transaction will fail
  - Some systems also periodically check the connection and will disconnect on failure.
  - "Single Log-in" or "No Log-in" systems are not permitted.

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.

Security Questions to be Asked for "Zero Trust"

- **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?

6

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 is "Zero Trust Used in ACS

- **A "Zero Trust" Cybersecurity is rarely applied in ACS**
  - However, it is sometimes necessary to use a safer and more security reliable model than "Full Trust"
  - This might be called a "Minimum Trust Model"
- **Clearly, more cybersecurity models are needed than only "Full Trust" and "Zero Trust".**
  - This is discussed further in MLM-018-B What is minimum trust in Automation and Control Systems (ACS)

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

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

- **Additional Reference Materials**
  - Listing of all MLMs
    including video, PDF documents, PowerPoint, and SCORM downloads.
  - Listing of PERA documents
    including original manuals, recent learning and reference materials.
  - https://www.tigera.io/learn/guides/zero-trust/zero-trust-security/?gclid=Cj0KCQjwy5maBhDdARIsAMxrkw3YJfRlE3vERjdgAdUe_k07vid1CcT9K_slVkqq11y9qa2hmet9WxIaAuzHEALw_wcB

Please click here to provide feedback on this MLM.

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

Author

Gary has more than 40 years of experience with enterprise integration and optimization projects, including PERA master planning and project management.

As one of the initial authors of the PERA Handbook of Master Planning, he has used PERA Enterprise Architecture and Master Planning methodologies throughout his career including control and information systems for oil production, pipelines, refining and marine loading, petrochemicals, coal, gas, and oil-fired power plants, polyethylene, ammonia, explosives, paint, pulp and paper, food and beverage, and pharmaceuticals. LNG facilities included world-scale arctic, European, and US Gulf coast complexes.

infrastructure facilities included Fire, Police, and Emergency Response systems for major US cities, as well as emissions reporting and trading systems for more than 100 US Power Plants,