Learning Map-012

"Trust" in ACS and IT Plant Systems

Intended Audience:

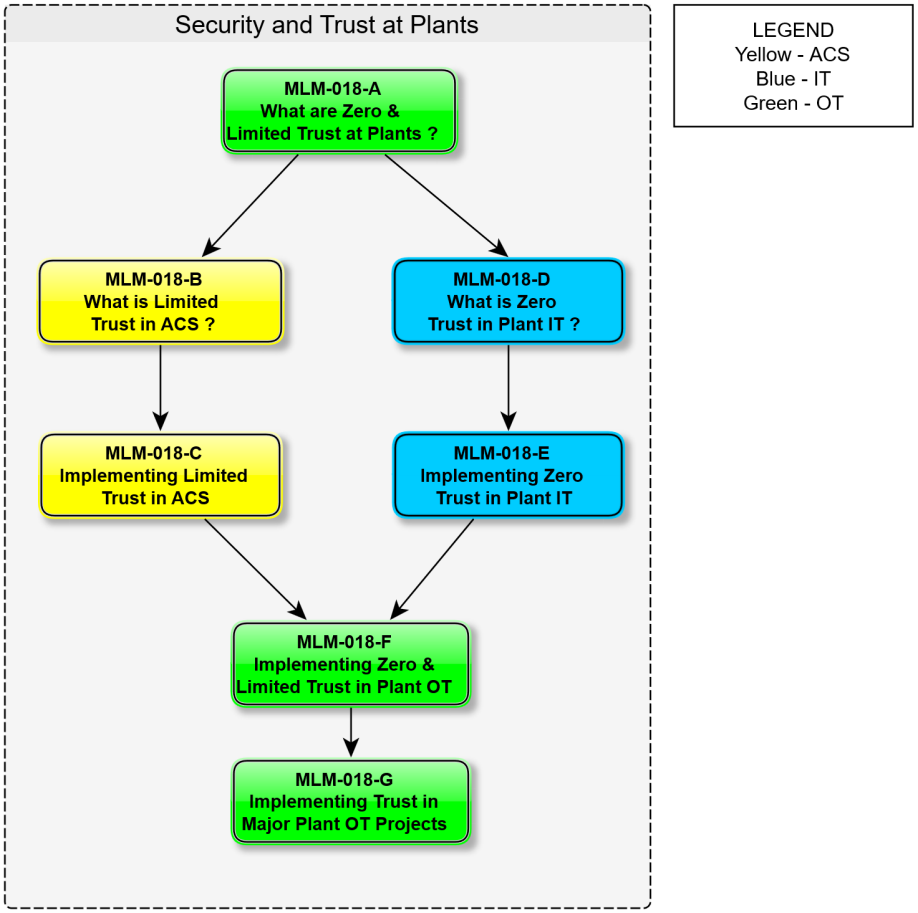
Anyone currently involved in cybersecurity including

1. Control Engineers
2. IT Specialists working on OT systems (involving ACS and IT)
3. Plant Personnel involved in Plant Safety and Security
4. CISO and other Head Office Staff involved in Industrial Cybersecurity

Context and Objectives of this Learning Map

The objective of this learning map is to promote understanding of the concepts and priorities of "Trust" in ACS and IT in plant systems. It addresses plant applications requiring expertise in ACS (shown in yellow), and IT (shown in blue).

Applications requiring both ACS and IT expertise are defined as "OT" (Operational Technology). These often occur at PERA Levels 3 to 5 and are color-coded as green on Learning Maps (see below), Architecture Drawings, Workflow Diagrams and wherever the responsible discipline for design and implementation is shown.



MLM-18-A It describes "Full Trust" and "Zero Trust" as they might be found in plants.

- Control Engineers usually prefer the idea of "Full Trust" as they fear what might happen if an operator forgets a password or the "Zero Trust" mechanisms fail.
- IT specialists require "Zero Trust as it facilitates data protection and meets corporate cybersecurity security rules.

However, these to alternatives are not adequate, and the concept of "Managed Trust" is introduced that includes:

0) Zero Trust
   Requires identification of user on initial "Logon" before granting access to any resource. After successful Logon, rights of the requestor must be verified before every transaction. In the event of internet or other remote users, end-to-end encryption (https) and address checking before every transaction may be necessary.

1) Minimum Trust
   Requires identification of user on initial Logon before accessing any resource, but no further verification is required. Logon is terminated after a set period of inaction.

2) Limited Trust
   After successful Login by a user at a workstation, all resources available from that physical workstation are available (no check for rights to specific resources).

3) Full Trust
   Only Physical access to the workstation is necessary. Any user gets full access to all resources available to that workstation.

MLM-18-B describes the concept of "Managed Trust" in Plant Automation and Control Systems (ACS) and OT systems including the following examples.

0) Zero Trust
   This is rarely used in ACS because the risk of failure of the protection systems, or human errors in their use are likely to result in unacceptable risk and costs.
   It might be necessary where ACS systems like truck loading stations have work processes that require authorization of financial transactions involving outside personnel and systems.

1) Minimum Trust
   This is used for multi-use OT workstations such as Engineering Workstations. It allows access to applications like maintenance, H/R, or Email that require authorization of users

for each application.

2) Limited Trust
   This is used in limited-access areas like control rooms with operators who are certified to access all resources available to that workstation. Badge readers are sometimes used to simplify logon procedures and avoid human errors.

3) Full Trust
   This is used for remote devices in locked cabinets or equipment rooms. It ensures that emergency actions may be accomplished even in the event of failure of protection systems. Most PLCs or other Level 0 and 1 devices use this method, although there are new standards such as ISA 108 that recommend use of passwords to change device and HMI settings.

MLM-18-C describes how "Managed Trust" might be implemented in ACS or OT systems where a Control System Engineer Leads the Project, and IT specialists to provide specifications and support as requested.

This might include plant environment applications such as:

- process optimization and diagnostics
- remote diagnostics and emergency response for high-speed rotating equipment,

It also describes how to implement requires both ACS infrastructure and IT infrastructure, but where the most demanding part of the project requires a Control System Engineer to Lead the Project, and IT specialists provide specifications and support as required.

MLM-18-D describes "Zero Trust" from an IT perspective. It also describes Why Zero Trust may be required for IT and/or OT systems in a plant environment, such as remote access from uncontrolled devices or internet locations where there is significant risk of cyber attack.

<Note: David, please look at attached "MLM-018-B 24-1-26 Dans revision" that provides more detail about Zero Trust definitions. I also moved the last couple of slides from MLM-018-D to MLM-018-E as they were about implementation.>

MLM-18-E describes how "Zero Trust might be implemented for an IT application in a plant environment. Although Active Directory may be used in IT systems, below the plant firewall, a different mechanism is needed (this is described in an article I found recently).

This MLM describes an application that requires the skills of an IT specialist who serves as the Project Leader, and a Control Engineer to provide ACS Engineering specifications and other support as requested.

One possible example might be a remote water pumping station that requires a secure fence with a CCTV camera and badge reader to allow for secure entry of maintenance personnel. A remote process operator may also need additional sensors to determine whether the pump is operating or if the backup unit has been "locked out" by maintenance staff. Status of an internal Fire Alarm Panel might also be provided.

MLM-18-F describes an "OT" (Operational Technology) application containing both IT infrastructure and ACS (Automation and Control Systems) devices and networks. This application includes a sophisticated OT system that requires the skills and certifications of both an ACS Control Engineer and an IT Specialist.

In this example, a Truck Loading facility requires a (Remote) Process Operator to "line up" and monitor the transfer of hazardous liquids, and to deal with alarms and emergencies such as fires and explosions. This requires the remote Process Operator to have "Managed Trust" to operate the pumps, automated valves and safety systems.

However, the driver of the Truck Driver may work for different companies and should have "Zero Trust" as he and his truck may never have been at this facility before.

The Truck Driver must identify himself and verify that he is personally certified to load the dangerous materials on his bill of lading. His truck must also be validated for this material. The requested transaction must be financially authorized (as it may be worth tens of thousands of dollars).

There may also be a "backup check" where the Security Guard at the plant gate must confirm the truck number (and weight) that was actually loaded before releasing the truck and driver to leave the loading facility.

This application requires ACS and IT professionals to collaborate in the design and support of the facility, as neither can accomplish all of the requirements alone.

The project manager responsible for design of the facility, or the plant manager responsible for operation of this "shared" OT system, must decide whether the Control Engineer or IT specialist are responsible for the safety and security of the ACS and IT systems. In the event of conflict of company standards or priorities for ACS or IT systems, Project Management or Plant Management must resolve and document the decision.

MLM-018-G describes ACS and IT participation in a major projects requiring teams of specialists including many professional disciplines such as control Engineer, Analyzer Specialist, Industrial telecom Engineer, PLC programmer, IT specialists with expertise in Quality Control Systems, and Process Data Historians, as well as Process Engineers and others.

In such projects, the interfaces between different organizations and specialists within these organizations become a major source of errors and require clearly defined deliverables including timing and approval mechanisms.

The Project Manager plays a crucial role in helping coordinate schedules, manage budgets, and ensure smooth information sharing.