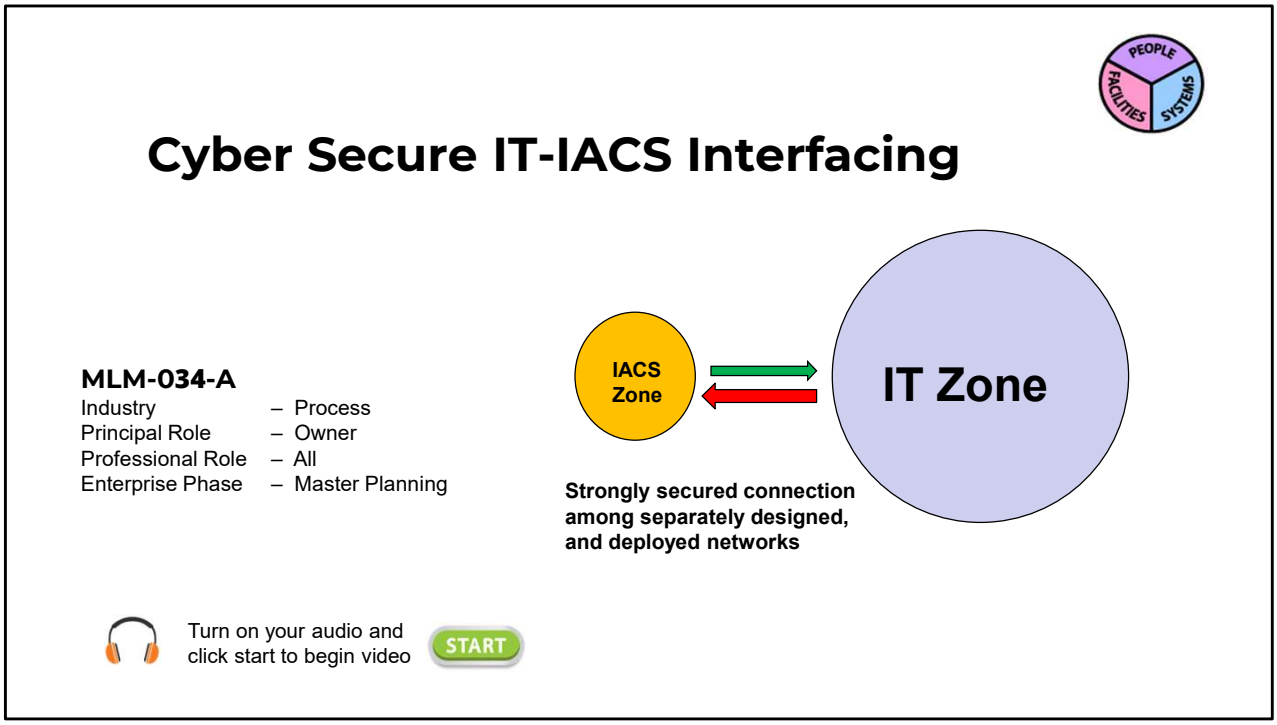


PRINT VERSION OF NARRATIVE

This Micro-Learning Module discusses principles for interfacing between IT and Industrial Automation and Control Systems networks. It explains that IT and I A C S networks can be securely interfaced, but they should never be "converged" or "merged."

Note that the acronym I A C S may be pronounced as "eye-ax".

This MLM is the first of the "Cybersecure Interfacing" series. It describes general goals and principles intended to address all eye-ax systems. Although the term "plant" is used in this MLM, it can equally apply to any physical equipment or facility, including pipelines, medical equipment, buildings, etc.

Additional MLMs in this series provide "Use Case" examples for specific industries such as process industries, manufacturing, transportation, or medical.

The intended audiences for this MLM are eye-ax engineers, IT teams dealing with eye-ax cyber defense, consultants, systems integrators, and managers making decisions about achieving I A C S cyber security.

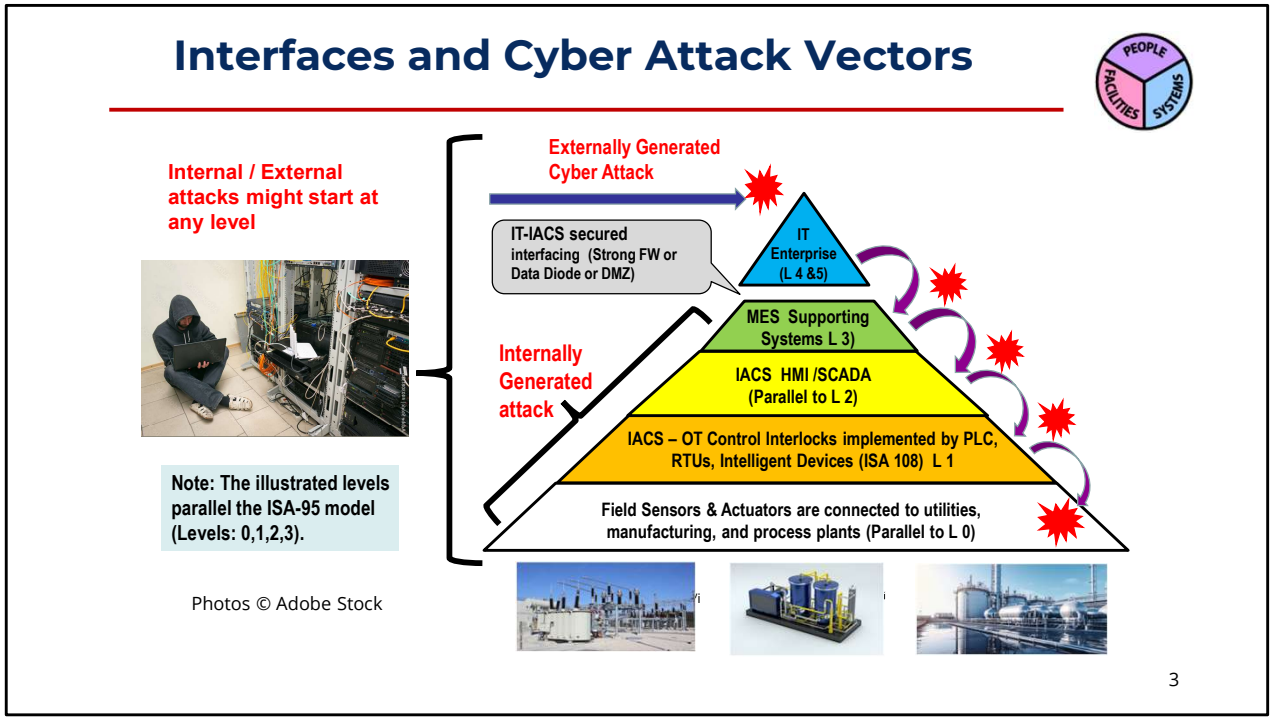
Interfacing IT and IACS networks

- **The main goals of IACS are:**
  - Assure operating Safety and Reliability.
  - Detect anomalous conditions in the IACS zone
  - Respond quickly to incidents in the IACS zone
  - Report real-time information to the IT zone
- **IACS network principles**
  - IACS must be designed by specialists with experience in industrial processes and networks
  - Collaboration among IACS and IT specialists is important
- **Principle of secure IT and IACS interfacing**
  - The data flow between the IACS and IT networks may only be allowed through a secured interface between these networks

PRINT VERSION OF NARRATIVE

Let's discuss the principles and goals for interfacing IT and IACS networks. Among the main goals of the IACS is Controlling industrial plant operations, with a special focus on operating Safety and Reliability. In order to achieve these goals, the IACS must include measures for detecting anomalous conditions and responding to incidents in the IACS zone. Furthermore, the IACS must provide consistent reporting of real-time information to the IT zone

The IACS must be designed and deployed by experts who understand the industrial process at the facility. To achieve the listed goals of the securely interfaced system, the IACS, and IT experts must collaborate. The result of that collaboration shall include secure data flow between the IACS and IT zones.



PRINT VERSION OF NARRATIVE

Let's discuss the most common attack vectors that may harm the IT or IACS operation. This slide illustrates a simplified version of the ISA 95 model, focusing on the three bottom levels, 0, 1, and 2, where the industrial operations and level 3, where the process optimization resides. In addition, as shown, the top triangle belongs to the IT operation and the supporting functions residing at levels 4 and 5.

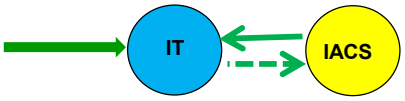
Attacks against the industrial organization may start internally at Purdue levels 0,1,2 or 3 or externally, in most cases through levels 4 and 5. However, to cause an operating outage, damage to machinery, or risk lives, the cyber-attack must proceed to the lowest levels, 0 or 1, where the heavy machinery resides.

In addition, we must consider a range of supply chain-related attacks, which might involve service providers with infected hardware or software.

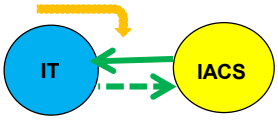
To cause damage to machinery or manipulate the process, the attackers must understand the industrial process. Specific knowledge is required when attacking a power grid using DNP 3.0 or IEC 61850 protocols, Similarly, other knowledge is required when attacking a pipeline or a chemical facility, where safety-related consequences must be considered according to IEC 61508 and IEC 61511. Such an attack may also involve "insiders" with in-depth knowledge of IACS.

Cyber Secured IT & IACS Interfacing

- **Guidelines for Interfacing**
  - The data from IACS and IT zones is communicated between the IT layer (L 4) and the IACS Network in L 3)
- **IACS and IT architectures must be:**
  - Separately designed with their own objectives
  - Separately deployed in their respective zones
  - Separately tested prior to commissioning
  - May be securely interfaced but not converged.



- **Secured IACS and IT interfacing provides:**
  - Improved operation and maintenance
  - Transfer of operation data to and from the IT zone
  - Allow secure remotely conducted IACS support



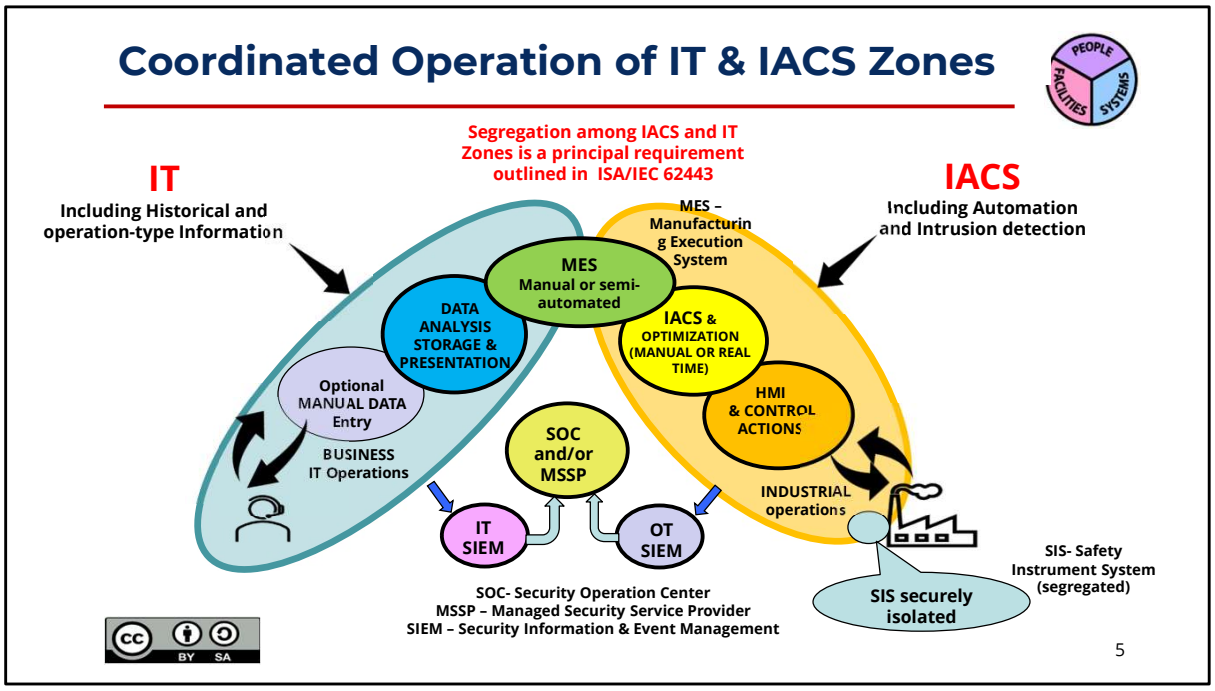
PRINT VERSION OF NARRATIVE

As defined in ISA 62443, the IACS in levels 1,2,3, and then IT networks in levels 4 and 5 must be segregated. However, if needed for specific purposes, they may interface through a secure connection.

To address their respective objectives and priorities, IACS and IT systems must be separately designed and deployed in their respective zones and tested individually prior to the commissioning process.

However, to assure operation safety and reliability of the industrial organization, the IACS, and IT networks must not “converge.” Secure interfacing among these networks can be implemented using a DMZ, a Next Generation Firewall, a Data Diode, or a Jump-host server.

Secure interfacing among these networks is typically done for 3 reasons. To achieve improved productivity, for consistent transfer of operation data to the IT zone, and to allow remote support and convenient maintenance.



PRINT VERSION OF NARRATIVE

This illustration shows how the IT and the IACS zones are related.

The IT Zone, marked in light blue, provides goals and high-level analysis and deals with the storage and publishing of process-related data.

The IACS zone is shown in yellow and orange colors on the right side. It may receive real-time field-related data from the Manufacturing Execution Systems (MES) or specific inputs the operator enters.

The IT Zone exchanges data with MES, and the IACS-related controllers create, receive, and exchange data with the Human Machine Interface (HMI). The MES-related systems, such as production or maintenance scheduling, are related to the industrial process but do not directly participate in real-time process control.

For enterprises that require Security Information and Event Management (or SIEM) systems (the magenta and grey circles), data is received independently from the IT and IACS zones. The output of the SIEMs may then be securely forwarded to the Security Operations Center (or SOC) greatly improving operations management and resilience to failures and attacks.

It is important to remind ourselves that segregation and secured interfacing among IACS and IT Zones are principal requirements outlined in the ISA/IEC 62443. The actual interfacing among these zones may utilize a Next-generation Firewall, a Demilitarized Zone DMZ, or a unidirectional data diode but must not be built as converged networks.

Finally, it is important to explain that Safety Instrument systems (SIS) must be segregated from the rest of the IACS zone. If remote access is required for upgrade or patching, such action must involve careful design and human supervision.

Key Messages from this MLM

- IACS and IT systems may be securely interfaced but not converged or integrated
- IACS Must be designed, implemented, and maintained by people who understand the Industrial process and are responsible for its Safe operation.
- Cybersecurity is a critical precondition for operation safety, and it must be correctly deployed and monitored.
- The IACS and IT teams must assist each other in addressing their respective priorities, but IT cybersecurity practices must not be forced on the IACS environment.
- Decisions related to cyber-secured IACS architecture and safe and reliable operation are the responsibility of the IACS Team.

PRINT VERSION OF NARRATIVE

Let's summarize the key messages from this MLM.

- IACS and IT systems may be securely interfaced but not converged or integrated.
- IACS design, implementation, and maintenance must be conducted by people who understand and are responsible for the industrial process.
- It is important to emphasize that industrial cyber security is a critical precondition for operation safety, and it must be correctly deployed and monitored.
- The IACS and IT teams must collaborate to address their respective priorities, but IT cybersecurity practices must not be forced on the IACS environment.
- Decisions related to cyber-secured IACS architecture and safe and reliable operation are the responsibility of the IACS Team.

Author

Daniel Ehrenreich

Daniel has over 33 years of experience with control of industrial operations and integration of cyber security solutions.

He is a control engineering consultant, workshop lecturer, and an expert in cyber secured operation for IACS.

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.

PRINT VERSION OF NARRATIVE

Daniel Ehrenreich has over 32 years of experience with control of industrial operations and integration of cyber security solutions.

He is a control consultant, workshop lecturer, and expert at SCCE (Secure Communications and Control Experts). Daniel is also contributing his expertise to multiple ISA 62443 workgroups and conducting free of charge podcast sessions for educating engineers worldwide. Since 2016, he has also been acting as Chairman of the annual ICS Cybersecurity Conference in Israel.