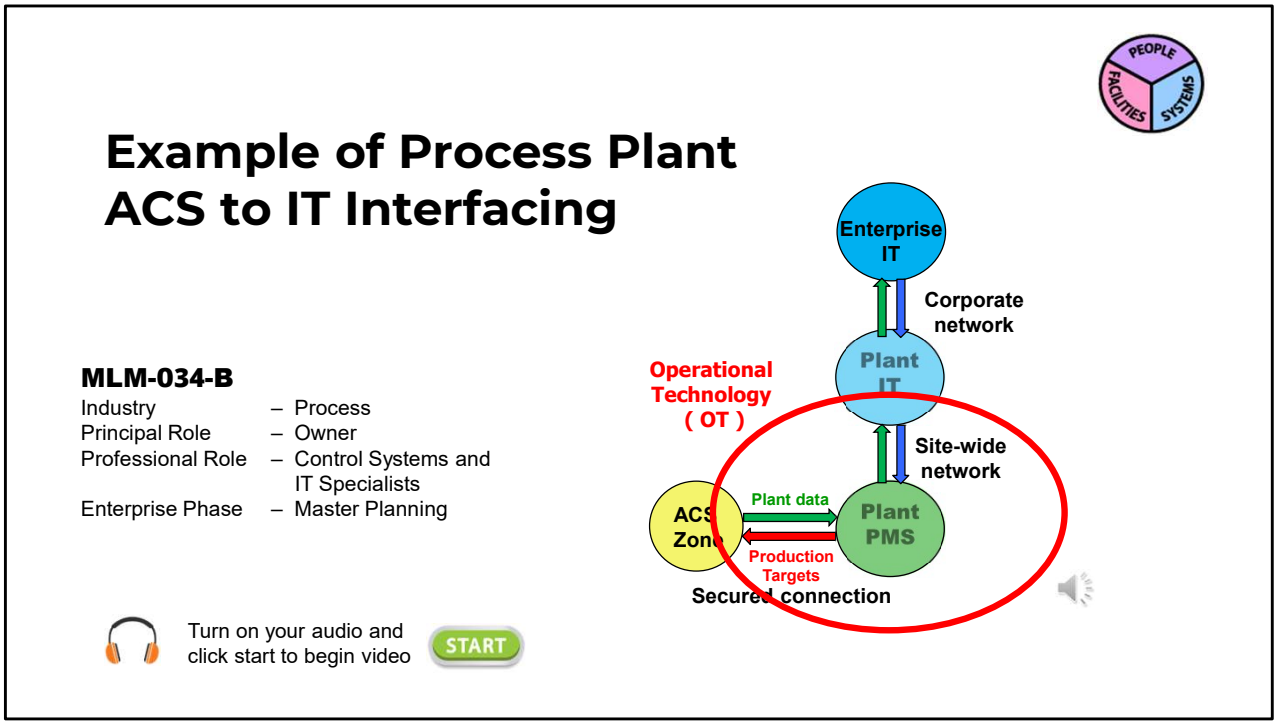


This Micro-Learning Module provides an example of interfacing ACS and IT systems and networks in a continuous Process Plant. Process Plants have industry-specific requirements, standards, and practices, especially around how ACS and IT networks can be securely interfaced.

This MLM is part of the "Cybersecure Interfacing" series. It describes general goals and principles intended to address all ACS 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 ACS engineers, IT teams involved in ACS cyber defense, consultants, systems integrators, and managers responsible for decisions related to achieving ACS cyber security.

Process Plant Definitions

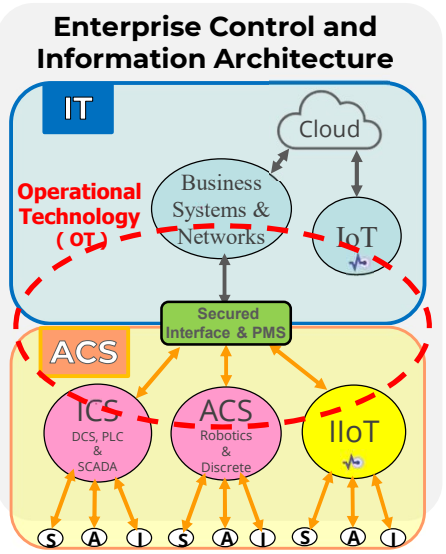
OT (Operational Technology) includes ACS and some plant IT

Enterprise IT systems may include:

- **Cloud Computing** (Internal + Internet)
- **Business Systems** (Finance, Office, HR, Asset Mgt., Info only IT networks)
- **IoT** (Internet of Things)
- **PMS** (Maintenance Scheduling, Data Warehouse, Internet Firewalls. Office networks, etc.)

Plant ACS systems may include:

- **Secured Interface & PMS** Industrial Firewalls, Sitewide Production Management Systems and Networks
- **ICS (Industrial Control Systems)**
- **ACS (Automation & Control Systems)**
- **IIoT (Industrial Internet of Things)**
- **Sensors, Actuators, & Interfaces**



In a process industry enterprise, IT Systems (the blue area) typically consist of:
Cloud Computing and Internet – including internal and outsourced applications,
Business Systems and Networks such as finance, Office, Human Resources, etc., including both IT and some shared OT applications,
IoT - Internet of Things Devices and Networks in non-hazardous environments and non-control applications, and
IT Plant Management Systems such as maintenance scheduling, data warehousing, Internet firewalls and associated office networks.
Plant ACS (the yellow area) may include:
Plant Production Management Systems including production scheduling and reporting, process data historians, industrial firewalls, etc.,
Industrial Control Systems (ICS), including continuous and batch DCS, PLC, and SCADA Control,
Automation & Control Systems (ACS), including discrete manufacturing and robotics,
Industrial Internet of Things (IIoT) devices and Networks in industrial environments, and
Level 0 equipment includes Sensors, Actuators and Interfaces, including industrial networks and gateways.
The architecture shown in this diagram is one alternative for a process industry plant that uses the concepts and principles of ISA 62443.

Goals and Principles of ACS and IT Systems and Networks are Different

As described in MLM-034-A, there are basic differences between the main goals and principles of:

- Industrial Automation and Control Systems and networks and
- IT Systems and networks

As a result:

- ACS and IT systems should be designed, implemented, and tested separately.
- Different design standards and expertise are necessary for each
- Secure Interfaces between ACS and IT networks are essential

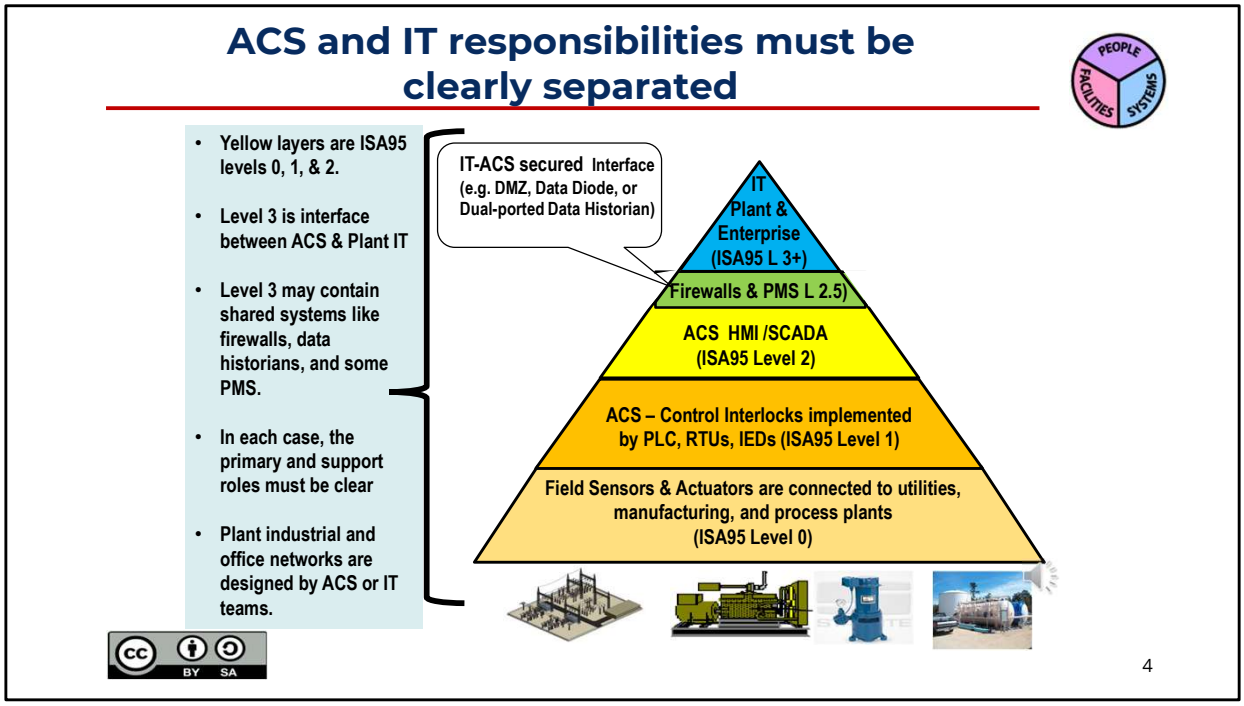
3

As described in MLM-034-A, there are basic differences between the main goals and principles of:

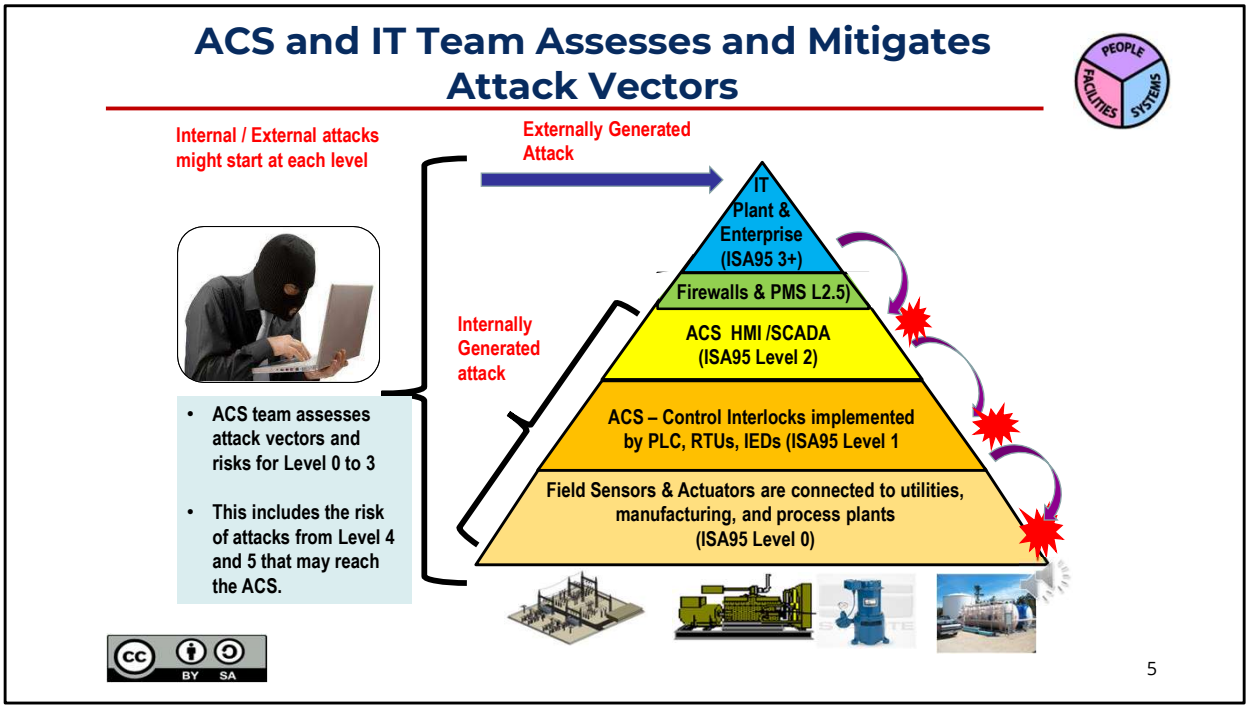
Industrial Automation and Control Systems and networks and
IT Systems and networks.

As a result:

ACS and IT systems should be designed, implemented, and tested separately.
Different design standards and expertise are necessary for each, and
Secure Interfaces between ACS and IT networks are essential.



- The yellow and orange areas correspond to ISA95 levels 0, 1, & 2.
- ISA95 standards are specifically designed for process industry plants including Business to Process Markup Language (B2PML).
- Level 2.5 is shown as the interface between ACS & Plant IT systems and networks, although some numbering systems may designate this as level 3.
- Level 3 might contain shared systems like firewalls, data historians, and parts of various Plant Manufacturing Systems (P M S) or Manufacturing Execution Systems (MES).
- The responsibility for design, maintenance, and technical support of ACS and IT systems must be clearly defined in the Enterprise Cybersecurity Program. Similarly, plant industrial networks and office networks should be designed by ACS or IT specialists with the requisite training and experience.



Let's discuss attack vectors that may harm the IT or ACS operation. This slide illustrates a simplified version of the ISA95 model, Layers 0, 1, and 2, where the industrial control and process optimization reside, are the responsibility of the ACS team.

The top blue triangle is the responsibility of the IT group.

Responsibility for Level 3 (shown in green) is shared between ACS and IT groups.

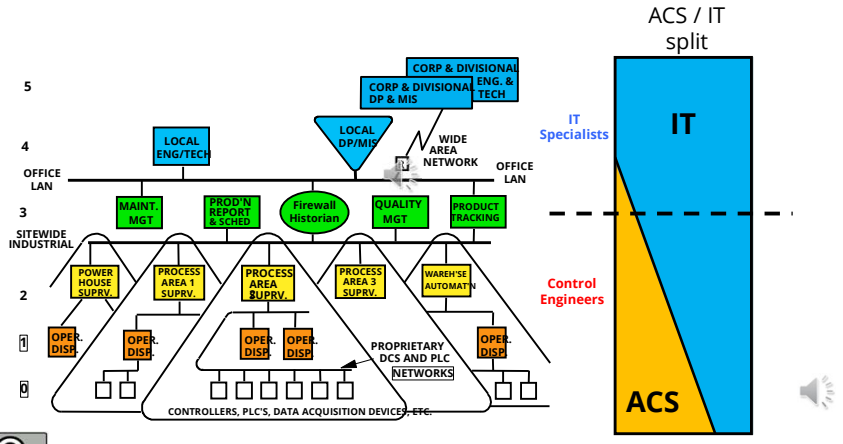
Cyber adversaries might attack at any level of hardware or software. Therefore, risk analysis and mitigation, along with ongoing monitoring and support, are part of the responsibilities for that level.

Attackers might penetrate any of the layers illustrated here. However, to damage machinery or risk lives, the attack must typically penetrate the layers where production equipment resides.

Considering such threats requires an additional level of expertise compared to IT system hacking.

WHAT DOES THIS LOOK LIKE IN AN ENTERPRISE ARCHITECTURE

IT systems (data storage, analysis & presentation) connect to networks at higher levels.
ACS (Real-time control, HMI, and online optimization) connect to networks at lower levels.



A Typical Architecture for a Process Industry Enterprise might look like this.

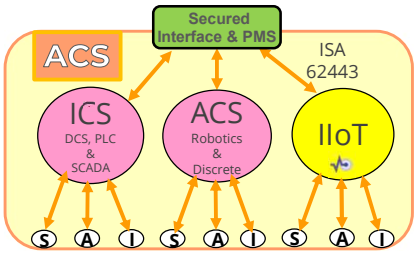
IT systems (data storage, analysis & presentation) connect at higher levels in the architecture, while ACS systems connect at lower levels.

In general, computing systems and networks below the Industrial Firewall are the responsibility of the ACS team, and systems above this are the responsibility of IT specialists.

ACS Skill Requirements

Each component of an ACS requires experienced, certified specialists:

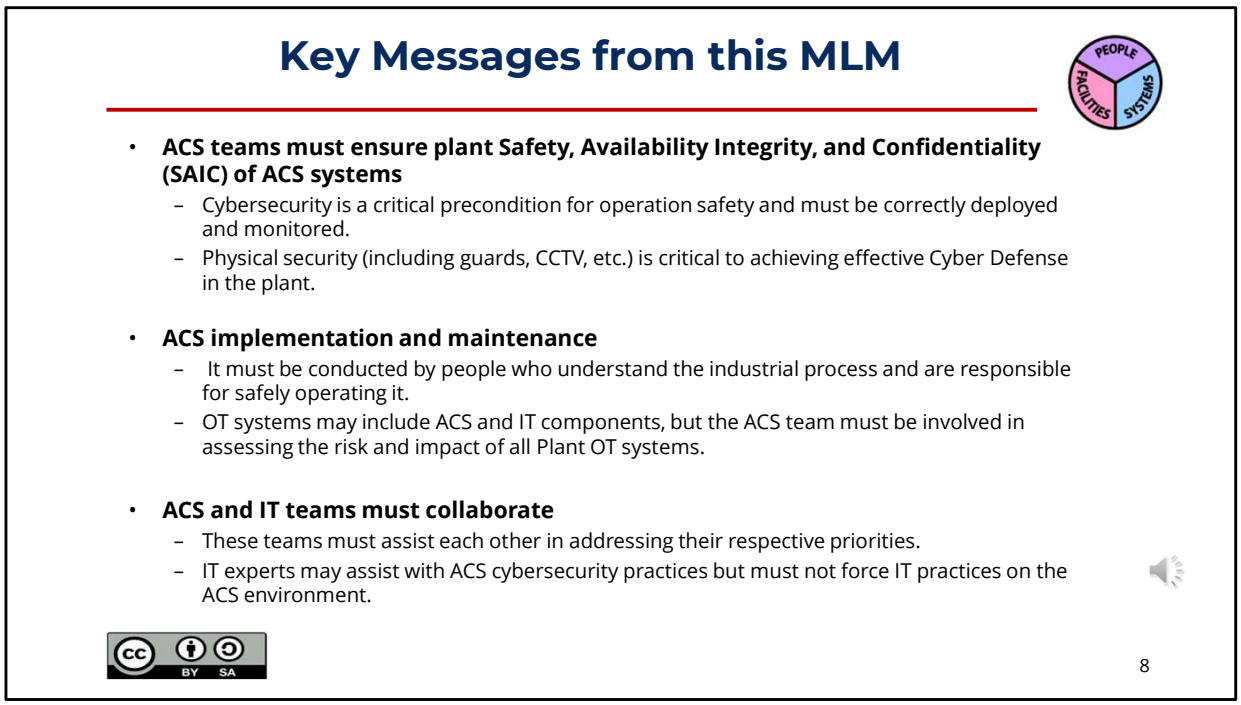
- ICS: Control System Engineers, Instrument Engineers & analyzer specialists
- ACS: Robotics, vision, and discrete automation engineers
- IIoT: Regulatory and safety requirements for industrial environments
- Industrial Networks: Telecom Engineers experienced with Industrial LANs, including wired, radio, and satellite networks.
- Plant Firewalls and interfaces: Both Engineering and network skills



Each of these industrial systems requires special skills and experience for its design and maintenance. Furthermore, these professional skills may also be specialized by industry. For example, since ACS are implemented in hazardous plant areas, knowledge is required in Process Safety, Cyber Security, and Electrical Safety. Many engineering standards bodies exist to help define and develop these skills, including ISA, NEC, API, and NFPA.

The ACS team typically shares responsibility for the secure plant Firewalls. The team may include an Industrial Network specialist who will also specify and configure secure industrial networks, interfaces, fiber optic backbones, and radio networks.
Control Engineers have the skills and experience to design and configure different ICS, IAS, and IIoT devices. (See ISA 95 for Interfacing Standards from ACS to Business Systems.).
Instrumentation and analyzer specialists typically design, procure and commission plant sensors and actuators.

Business IT Network Specialist may also have a role in set-up and operation of Plant Firewalls. For example, separate configuration tables may be managed on both the ACS and IT side of the firewall. Also, set-up and monitoring of data paths to and from ACS via Business or Public Networks may require IT involvement.



Having outlined the key goals and guidelines, let's summarize the key messages from this MLM.

The ACS team must ensure plant Safety, Availability, Integrity, and Confidentiality (SAIC).

It is important to emphasize that industrial cybersecurity is a critical precondition for operational safety, and physical perimeter security, including guards and CCTV, is essential for achieving cybersecurity in the plant.

System implementation and ongoing maintenance must be conducted by people who understand and are responsible for the industrial process.

The ACS and IT teams must collaborate to address their respective priorities. However, IT cybersecurity practices must not be forced on the ACS environment, and decisions regarding the cyber-secured ACS architecture for safe and reliable plant operation are the responsibility of the ACS Team.

Further Information

- **Related MLMs**
  - MLM-007-A ACS Architectures
  - MLM-010-C Fundamental Concepts of ISA-62443
  - MLM-014-A Definition of IT, OT, and ACS Terms
  - MLM-035-A Cybersecure PLC and RTU Principles
  - MLM-035-B Cybersecure PLC and RTU Programming

Please CLICK HERE to provide a comment to the author.

Here are some related MLMs that you may find of interest.

Please use the last link on this page to comment on this Micro-Learning Module. These comments will be directed to the author and will form part of a permanent record that will be used to help us improve.

Author

Gary Rathwell

Gary is a past co-chairman of ISA99 WG13 (Industrial Cyber Security Learning Materials) and has participated in the development of many ISA standards including ISA95 (Enterprise Integration), and ISA108 (Intelligent Device Management).

He has been president of Enterprise Consultants since 2000, offering PERA master planning and project services to dozens of world-scale national and international projects. He is experienced in oil refining, pipelines, and oil field operations, as well as Petrochemical and Power Industries.