Enterprise Control and Information Architecture Concepts and Terms

MLM-007-A

Industry	– process
Principal Role	– All
Professional Role	– All
Enterprise Phase	– All

Turn on your audio and click start to begin video

START

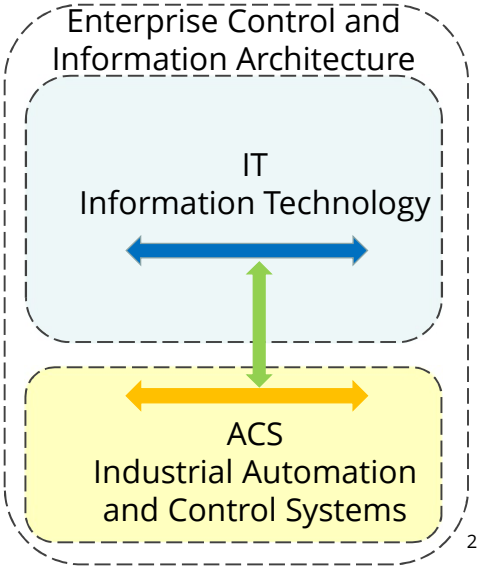
This MLM describes Enterprise Control and Information System concepts and terminology including Industrial Automation and Control Systems (ACS), Information Technology (IT), and Operational Technology (OT).

Click the START button when you are ready to advance.

Foundation Definitions

Control and Information Architectures typically include:

- IT – Information Technology Systems
- ACS – Industrial Automation and Control Systems in Hazardous Industrial Areas
- Networks to communicate within and between IT and ACS systems



2

Enterprises can be divided into Data processing systems often called “IT” (for Information Technology), and “ACS” (for Industrial Automation and Control Systems). IT and ACS networks communicate within and between these regions.

It is important to clearly define IT and ACS. A good working definition of these are:
- IT systems are used for data-centric computing that does not control equipment.
- ACS systems are used to monitor events, processes and devices, and to make adjustments in equipment and industrial operations targets.

Why Distinguish IT and ACS?

Because they are fundamentally different:

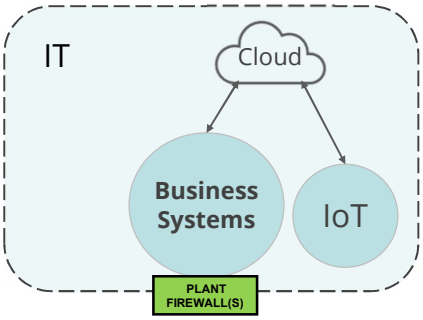
1) **Cybersecurity of ACS must be "designed in".** It cannot be "bolted on" or evolved "as needed".
2) **ACS must prioritize safety above cybersecurity.** They are intimately involved in equipment regulatory control.
3) **ACS failures are more dangerous than IT failures.**
   IT failures result in financial loss, while ACS directly impacts facilities, the environment and human life.
4) **Cybersecurity of IT systems and ACS have different goals.** Cybersecurity Integrity and Availability (CIA) vs.
   Safety, Integrity, Reliability, and Availability (SAIC).
5) **IT and ACS are at different levels** in the Enterprise Architecture.

Why do we need to distinguish between IT and ACS

1) Secure ACS must be "designed in". They cannot be "bolted on" or evolved "as needed".
2) ACS must prioritize safety. They are intimately involved in equipment regulatory control.
3) ACS failures are more dangerous than IT failures.
   IT failures result in financial loss, while ACS directly impacts facilities, the environment, and human life.
4) Cybersecurity of IT systems and ACS have different goals. Cybersecurity Integrity and Availability vs.
   Safety, Integrity, Reliability, and Availability.
5) IT and ACS are at different levels in the Enterprise Architecture.

Information Technology (IT)

- IT consists of Business Systems + Cloud + IoT
- Business systems consist of a set of applications that receive manual and real time data and process this to provide results, reports and displays to humans and other systems.
- Cloud computing applications run on Internet servers and deliver data to Business Systems
- IoT devices and networks may gather real-time "edge" data and deliver this to Business Systems via the Internet.



IT is defined as Business Systems + Cloud + IoT

Business systems consist of a set of applications that receive manual and real-time data and process this to provide results, reports, and displays to humans and other systems.

Cloud computing applications run on Internet servers and deliver data to Business Systems.

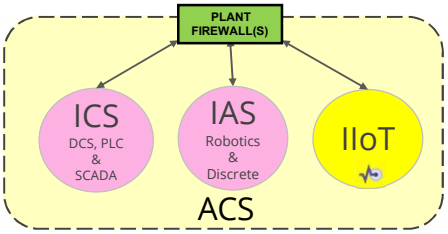
IoT devices and networks may gather real-time "edge" data and deliver this to Business Systems via the Internet.

Although plant Firewalls are considered part of ACS, IT network specialists may have a role in the setup and operation of Plant Firewalls. For example, separate configuration tables may be managed on both the ACS and IT side. Also, set-up and monitoring of data paths to and from ACS via Business or Public Networks may also require their involvement.

Automation & Control Systems (ACS)

ACS are defined as ICS + IAS + IIoT + Plant Firewalls

- Each of these require the skills and experience of Control Engineers to design and maintain.
- ICS, IAS, and IIoT devices and networks should not be directly connected.
  - ACS includes plant Firewalls that connect ACS networks to Business Systems.



Industrial Control and Automation Systems (ACS) are defined as Industrial Control Systems (ICS) + Industrial Automation Systems (IAS)+ Industrial Internet of Things (IIoT) + Plant Firewalls.

- ICS is a term used to describe Industrial Control Systems implemented with Distributed Control Systems (DCS), Programmable Control Systems (PLC) and Supervisory Control and Data Acquisition Systems (SCADA).
- IAS is a term for Industrial Automation Systems, such as discrete automation on conveyors or robots, and
- IIoT is used to describe “edge computing” devices for remote data acquisition and human interfaces connected with the Internet Protocol (TCP/IP).

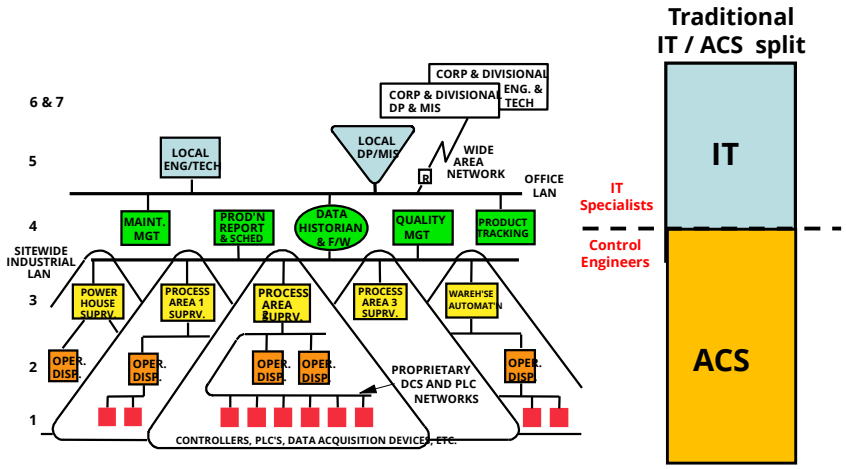
Each of these requires special skills and experience from the Control System Engineers responsible for their design and maintenance.

ICS, IAS, and IIoT devices and networks should not be directly connected. This is because ICS, IAS devices, and networks are each designed for different environments, speeds, and protocols. Thus, it is unlikely that adequate Reliability, Repairability, Response, and Resolution can be assured without the use of firewalls and monitoring software.

Connectivity can, however, be achieved through managed Firewalls as shown between ACS networks and Business Systems. Control Engineers may work with Industrial Network specialists who have the skills and experience to interface many different ICS, IAS, and IIoT networks. ISA 95 defines software Interface Standards between ACS and Business Systems.

A Business IT Network Specialist may be required to set up and operate Plant Firewalls. For example, separate configuration tables may be managed on both the ACS and IT sides of some firewalls or gateways. Also, set-up and monitoring of data paths to and from ACS via Business or Public Networks may also require their involvement.

What does this look like in an Enterprise Physical Architecture



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

Traditionally, IT (data storage, analysis & presentation) predominated at higher levels in the architecture, and ACS did "plant control".

In general, computing systems and networks below the Industrial LAN were the responsibility of Control System Engineers, and systems above this were the responsibility of IT specialists. Applications connected to either office LAN or industrial LANs and there were few connections between IT and ACS systems.

It was common for Control Engineers to get support from IT specialists in their areas of responsibility "below the Plant Firewall" such as IP network configuration or Company Computer and network standards.

However, it was relatively unusual for IT specialists to ask for support from Control Engineers "above the Plant Firewall", unless for basic Engineering for server rooms or network wiring.

What is Operational Technology (OT) ?

There are several definitions of the Operational Technology (OT) term, including:

1) Any computer system at a production facility (results in confusion with both IT and ACS definitions)
2) Any computer system connected to “industrial equipment” (results in confusion with ACS)
3) Any computer system having IT and ACS systems working together in real-time

Option 3 was selected because:

- **It defines who is responsible (both IT and ACS, with the lead decided by project management).**
- **The OT term originated with Gartner’s view of IT infrastructure integrated with power equipment, and this concept is retained.**

7

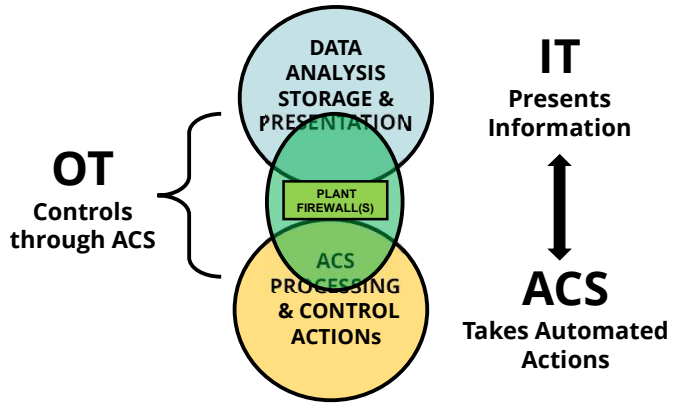
There are several definitions of the Operational Technology (OT) term, including:

1) Any computer system at a production facility (results in confusion with both IT and ACS definitions)
2) Any computer system connected to “industrial equipment” (results in confusion with ACS)
3) Any computer system having IT and ACS systems working together in real-time.

Option 3 was selected because

- It defines who is responsible (both IT and ACS with the lead discipline decided by project management)
- OT term originated with Gartner’s concept of IT infrastructure integrated with electrical power distribution, and this concept is retained.

Operational Technology Concept



8

Both IT and ACS receive real-time plant data.

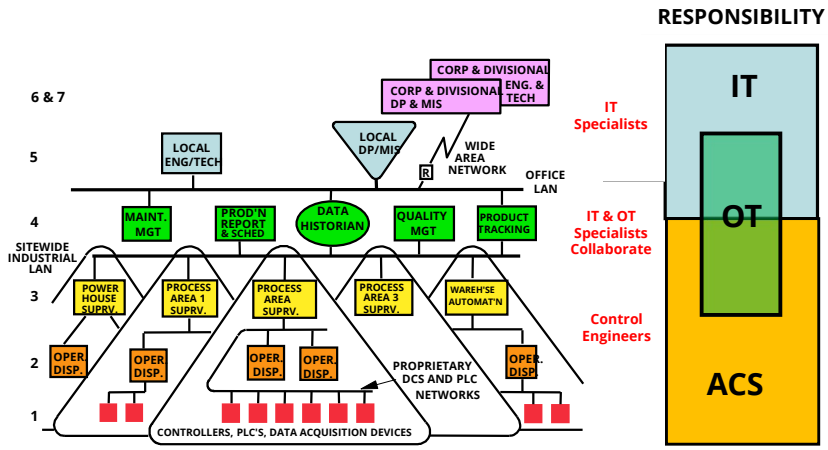
IT systems analyse, store, and present that data to humans. THEY DO NOT, HOWEVER CONTROL PLANT EQUIPMENT

ACS also receives real-time plant data and uses it to DIRECTLY CONTROL PLANT EQUIPMENT.

OT systems receive real-time data from ACS systems, analyse this data, and send new operating targets back to ACS systems (through a secure interface).

What does this look like in a typical process enterprise architecture?

IT vs. OT in "Industry 4.0"
Process Enterprise Architectures



With the increased use of Enterprise Integration, Plant Optimization, AI-based Logistics, and MRP systems, more and more "high-level" applications involve real-time operating targets for plant operations. This requires expertise in real-time control algorithms, model-based control, loop instability, and other control technologies that have "grown up" from plant regulatory control.

Similarly, with the increased use of the Internet of Things (IoT) for real-time data acquisition, IT specialists are implementing many non-hazardous IT systems in plant environments (like barcode readers or Video Cameras). This requires them to learn more about automated real-time data acquisition.

Thus, increased optimization, IoT, IIoT, and related technologies mean that it is often not possible to "draw a line" where Control Engineers stop, and IT Specialists begin. Increasingly, OT systems at all levels must be designed and supported as a "partnership" between IT and ACS resources.

Key "Take-away" Messages

1. **ACS = ICS + IAS + IIoT + Industrial Firewalls.**
   - ISA 62443 defines ACS to identify what this standard covers
   - It was first used in process industries, but is intended for use in all industries
   - requires the skills and experience of Industrial Control Engineers
2. **IT = Business Systems + Cloud + IoT + Commercial Firewalls**
   - Does not control hazardous equipment
3. **OT = Control Engineers and IT specialists collaborate.**
   - Gartner defined this term in 2006 for power utilities
   - The Project Manager decides which discipline leads.

10

Let's quickly review the key messages discussed in this MLM.
ACS = ICS + IAS + IIoT + Industrial gateways and firewalls.
- ISA 62443 defined this term in 2007 to identify what this standard covers
- It is intended for use in all industries
- requires the skills and experience of Industrial Control Engineers

IT = Business Systems + Cloud + IoT + Commercial firewalls
- Does not control equipment

OT = Control Engineers and IT specialists collaborate.
- Gartner defined this term in 2006 as control using IT infrastructure, and expanded in power distribution utilities
- The Project Manager (or Plant Manager in existing operations) decides which discipline leads.

Further Information

- **Related MLMs**
  - MLM-072-A, Cybersecurity importance of Field Devices
  - MLM-074-A, ISA 62443 Applicability to Level 0, 1 SAIC Devices
- **References**
  - IEC PAS 63325 Ed1, Lifecycle Requirements for Functional Safety and Security of ACS
  - ISA 95 – Enterprise-Control System Integration
  - ISA TR84.00.09-2017, Cybersecurity Related To The Functional Safety Lifecycle

Thank you for taking the time to view this Micro Learning Module.

The feedback link gathers feedback on the ISA Workbench about this MLM, which will be used by the author in updating this document.

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,

Please click here to provide feedback on this MLM.