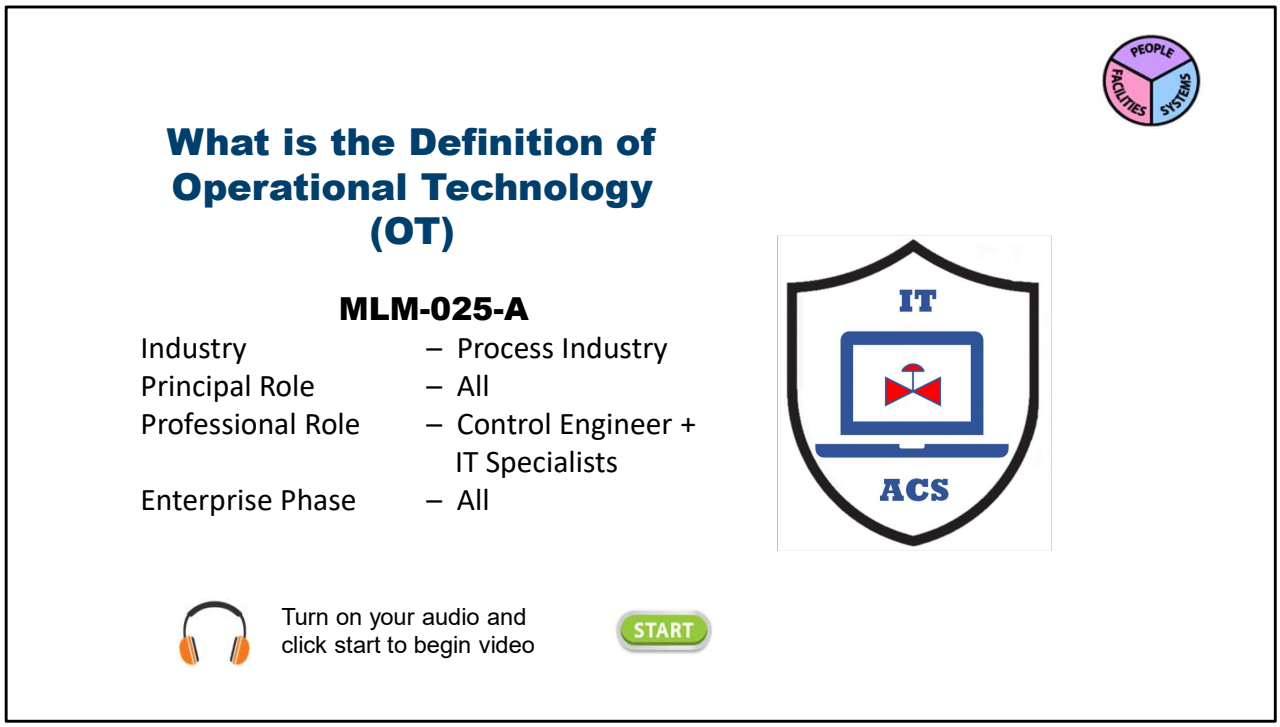


This MLM provides an introduction to the use of Artificial Intelligence in Process Industry plants. It is intended for design engineers and plant engineers who will encounter these systems today and probably use them or develop them in the future.

Click the NEXT button when you are ready to advance to the next slide.

What's the Big Deal ?

There is considerable disagreement and confusion about:

1) What is the best definition of IT and OT?
2) What skills are required for IT and OT systems?
3) Who should be responsible for specific IT / OT systems?

What is needed is an easily understood answer to each of these questions.

2

There are two common uses of the Operational Technology (OT) term:

1) Computer systems connected to "industrial equipment"
2) Real time measurement and control systems"

I prefer the second, and suggest the following definition

> *OT includes systems at all levels of the Corporation that gather operational data in real time and then make automated changes to these operations.*

While many OT systems are "connected" to industrial equipment, they are certainly not limited to this, and may exist at any level in the Enterprise Architecture.

What is Operational Technology (OT)?

There are two common uses of the Operational Technology (OT) term:

1) Computer systems connected to "industrial equipment"
2) Real time measurement and control systems"

I prefer the second, and suggest the following definition.

OT includes systems at all levels of the Corporation that gather operational data in real time and then make automated changes to these operations through ACS.

Currently, most OT systems are "connected" to industrial equipment. However, using the second definition, such OT systems may exist at any level in the Enterprise Architecture, and with development of "Industry 4.0" this is a major growth area.

3

There are two common uses of the Operational Technology (OT) term:

1) Computer systems connected to "industrial equipment"
2) Real time measurement and control systems"

I prefer the second, and suggest the following definition

OT includes systems at all levels of the Corporation that gather operational data in real time and then ***make automated changes to these operations***.

Currently, most OT systems are "connected" to industrial equipment. However, using the second definition, such OT systems may exist at any level in the Enterprise Architecture, and with development of "Industry 4.0" this is a major growth area.

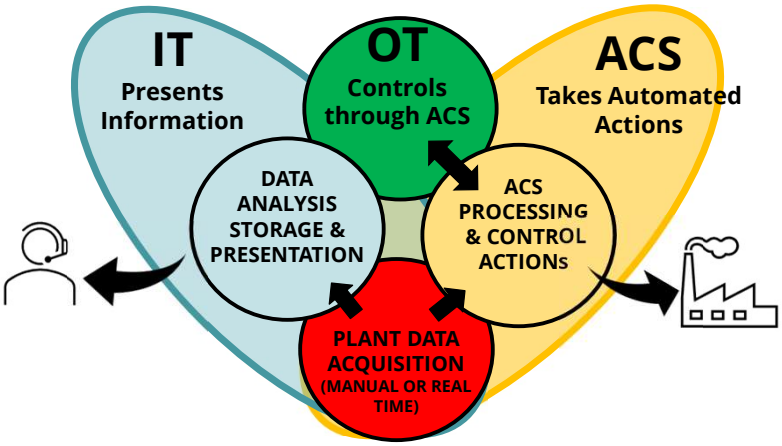
What is the Definition of AI ?

Artificial intelligence (**AI**) is the capability of computational systems to perform tasks typically associated with human intelligence, such as learning, reasoning, problem-solving, perception, and decision-making.

Source: Wikipedia

AI was founded as an academic discipline in 1956,[6] and the field went through multiple cycles of optimism followed by periods of disappointment. Funding increased after 2012 when graphics processing units (GPUs) were used to accelerate neural networks, and deep learning outperformed previous AI techniques.[11] This growth accelerated further after 2017 with the transformer architecture.[12] In the 2020s, the period of rapid progress marked by advanced generative AI became known as the AI boom. Recently, generative AI and its ability to create and modify content have exposed ethical concerns about copyright.

Information Technology vs. Operational Technology ?



5

Narrative:

Both IT and ACS receive real time plant data.

IT systems then do programmed analysis, storage, and presentation of that data to humans. THEY DO NOT, HOWEVER CONTROL PLANT EQUIPMENT

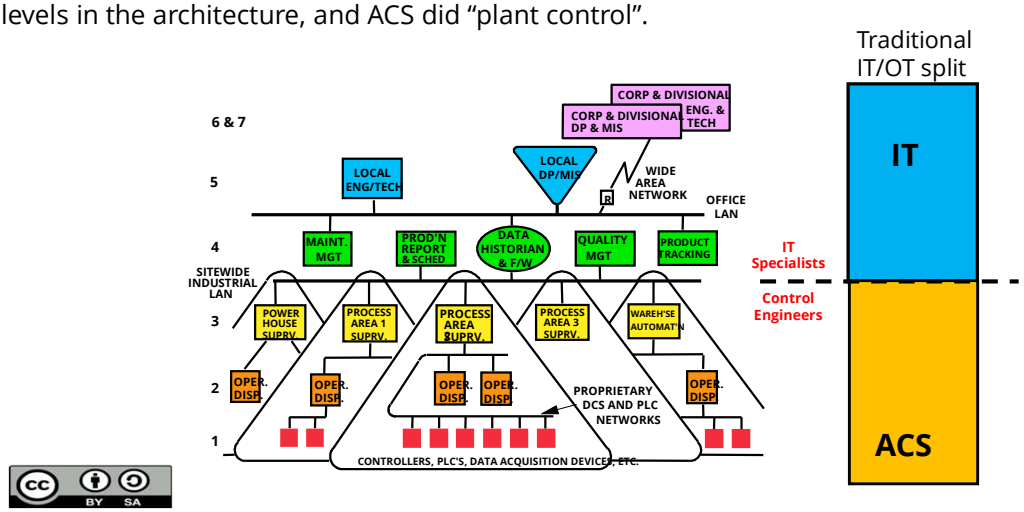
ACS also receive real time plant data and DIRECTLY CONTROL PLANT EQUIPMENT.

OT systems receive real-time data from ACS systems, analyze 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?

WHAT DOES THIS LOOK LIKE IN AN ENTERPRISE ARCHITECTURE

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



6

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".

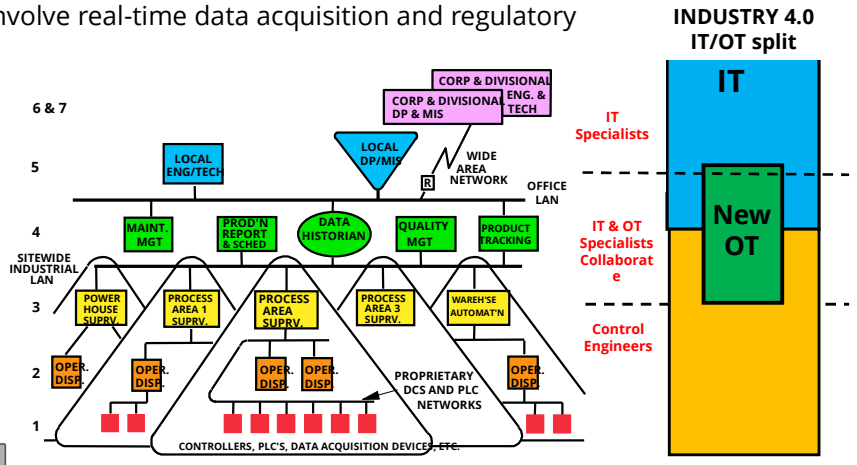
In general, computing systems and networks below the Industrial LAN were the responsibility of Control System Engineers, and systems above this were the responsibility of IT specialists. Applications connected to either office LAN or industrial LANs and there were few connections between IT and ACS systems.

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.

IT vs. OT in "INDUSTRY 4.0" ENTERPRISE ARCHITECTURES

With Enterprise Integration, "Digital Twin" Plant Optimization, AI-based Logistics and MRP systems, "high level" applications increasingly involve real-time data acquisition and regulatory control.



With increased Enterprise Integration, "Digital Twin" Plant Optimization, AI-based Logistics and MRP systems, more and more "high level" applications involve real-time control of 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 increased use of Internet of Things (IoT) for real time data acquisition, IT specialists are implementing many non-hazardous IT systems in plant environments (like bar code readers or access badge readers). This requires them to learn more about automated real-time data acquisition.

Thus, Industry 4.0, IoT, IIoT and related technologies, mean that it is not possible to "draw a line" where Control Engineers stop and IT Specialists begin (if it ever was). Increasingly, systems at all levels must be designed and supported as a "partnership" between IT and OT resources.

2) WHAT SKILLS ARE REQUIRED FOR IT AND OT SYSTEMS

- IT and OT applications exist at all levels of the Enterprise..
- Responsibility for a project or support of an operational system shall be assigned to a single Role (e.g. Control Engineer).
- Similarly, for systems that are assigned to IT, Engineering supporting skills may be needed where:
  - the environment poses special risks
  - Special real-time control experience is necessary.

• OT and IT applications exist at all levels of the Enterprise. The Risks associated with each application determine what Skills are needed to mitigate those Risks to meet company standards.

• Required Engineering skills might include Control Engineers, Industrial Network Engineers, Electrical Engineers, etc.

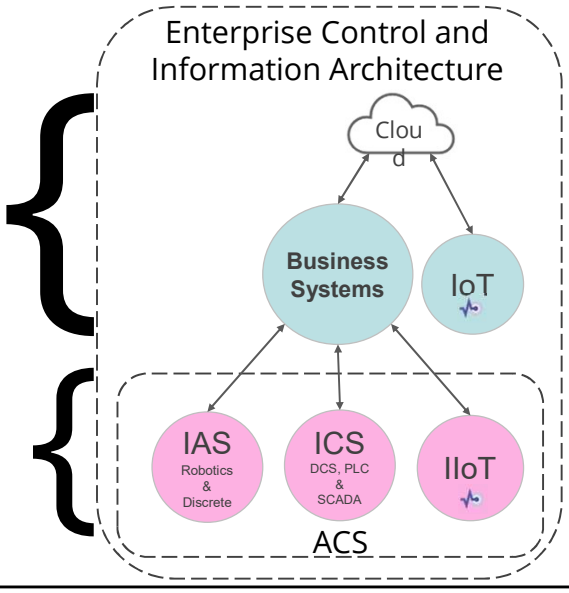
•Industrial (Engineering) skills may be needed where:

- •Failures have severe consequences (at any level in the Enterprise Architecture. For example,
  - • Control of Reactors, compressors or other hazardous equipment
  - • Environmental Emissions monitor and reporting that results in fines and/or plant shutdown.
- •Hazardous Physical plant areas where special equipment and network design is required (e.g. Industrial networks, firewalls, etc.).

ASSIGNMENT OF RESPONSIBILITY FOR SAFETY & CYBERSECURITY OF ACS

Business Systems, IoT, as well as corporate and non-industrial cloud networks are typically the responsibility of IT Groups with support from Engineering.

ACS systems including ICS, IAS and IIoT applications are typically the responsibility of Engineering Groups with support from IT.



9

Narrative:

As illustrated in Topic A, Item 2, use underlines rather than bold font for emphasis, to avoid confusion with topic headings.

KEY MESSAGES

The following are the key messages in this MLM:

- Definitions:
  - IT Analyzes and presents information
  - OT takes automated control actions
- ACS may contain OT and IT systems.
- Responsibility for these systems must assigned according to Risk as defined by company standards.

Narrative:
The following are the key messages to take away from this MLM.

Definitions

Topics

Key "Take-away" Messages

1. ACS = ICS + IAS + IIoT
2. ACS require the skills and experience of Industrial Control System Engineers to design and maintain.
3. Information Technology (IT) specialists must work with Control Engineers to securely interface ACS to:
   1) Business Systems, 2) IoT and 3) the Internet.
4. A pile of bricks is not a building. A Cybersecure Architecture should be built-in as the facility is designed.
5. Control Engineers are responsible for all ACS
6. ACS Architectures are a key aspect of Cybersecurity.

11

Let's quickly review the key messages discussed in this MLM.

1. Review the definitions of ACS, ICS, IAS and IIoT. ACS consist of ICS +IAS + IIoT systems.
2. The skills and experience of Control Engineers are required to design and manage the ACS architecture. Without a well-planned and maintained structure, ACS will become unreliable and unsafe.
3. Control Engineers and Industrial Network Engineers are responsible for interfacing ACS to Business Systems, IoT and the Internet. However, they should collaborate with Business IT and Network Specialists to define functional specifications.
4. A pile of bricks is not a building, and a random set of hardware and software is not an ACS Architecture. ACS must be planned beginning with conceptual engineering and continuing through operations and maintenance. Cybersecurity requirements should be established for all enterprise industrial facilities. It is nearly impossible to "bolt on" Cybersecurity after the fact.
5. The responsibility for ACS must rest with the Control Engineering Role and cannot be shared. If more than one individual is responsible, then no one is responsible. However, the Control Engineer should seek Industrial Network Engineering input when appropriate such as Plant-wide Networks, Pipeline and Powerline SCADA, Radio signal propagation maps, Satellite Networks, etc.
6. Industrial Architectures are a key aspect of Cybersecurity. To be defensible, the ACS must have a minimum number of hardware and software interface points that may be attacked. Industrial networks should also allow for secure monitoring and forensic analysis.

More Reading

Related MLMs:

- MLM-090-B AI Applications in Process Industry.
- MLM-091-A Plant AI and Human Interfaces.

References

- PERA 18 Management of Alarms Standard
- Fareed Khan offers an extensive library describing the development of AI applications on the Medium.com publishing platform.

:

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.

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,