Tradeoffs in Use of ACS vs. OT

MLM-014-B

Industry	– Process Industries
Principal Role	– All
Professional Role	– Control Engineers & IT
Enterprise Phase	– All

Turn on your audio and click start to begin video

START

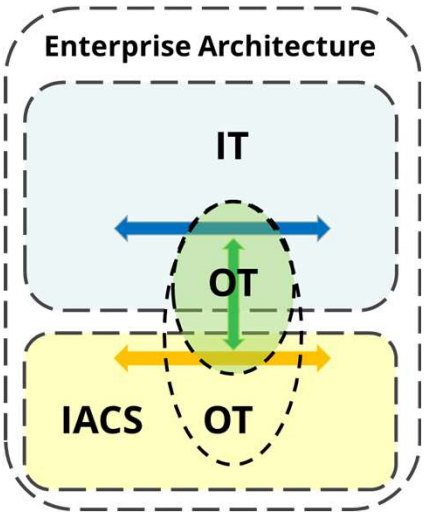
This MLM describes common terms used in Enterprise Control and Information Systems, including Automation and Control Systems (or ACS), Information Technology (or IT systems) and Operational Technology (OT systems)

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

Clear Definition of Terms, Architectures, and Human Factors are Required

To compare tradeoffs in their use, exact definitions of OT and ACS are required including:

- Formal definitions by bodies originating each term
- Architectural concepts associated with each alternative
- Human and organizational aspects of the use of each



2

To be able to compare tradeoffs exact definitions of OT and ACS are required including:

- Formal definitions by bodies originating each term,
- Architectural concepts associated with each alternative,
- Human and organizational aspects of use of each.

Note that the possibility of extending OT to sensors (PERA Level 1) is included here, however in hazardous industries this is not advisable.

Formal Definition of OT

In 2006 Gartner coined the term Operational Technology

- Initially the term was applied to power utility control systems (particularly in Electrical power distribution rather than power generation).
- Over time the term was adopted by other industrial sectors and used in combination with IoT.
- A principal driver of the adoption of the term was that the nature of operational technology platforms had evolved from bespoke proprietary systems to complex software portfolios that rely on IT infrastructure.

The term operational technology as applied to industrial control systems was first published in a research paper from Gartner in May 2006 (Steenstrup, Sumic, Spiers, Williams) and presented publicly in September 2006 at the Gartner Energy and Utilities IT Summit.[2] Initially, the term was applied to power utility control systems, but over time, it was adopted by other industrial sectors and used in combination with IoT. A principal driver of the adoption of the term was that the nature of operational technology platforms had evolved from bespoke proprietary systems to complex software portfolios that rely on IT infrastructure.

Formal Definition of ACS

ISA has coined the term ACS or Automaton and Control Systems

- defined as “a collection of processes, personnel, hardware, and software that influence the safe, secure, and reliable operation of an industrial process.
- essentially encompassing all components involved in automating an industrial operation, including sensors, controllers, actuators, and communication networks.”

Initially, the term was applied to continuous process industries like refining where it was compatible with:

- Enterprise Integration Standards like ISA95
- Networking standards like ISA100
- Industrial device configuration standards like ISA108

According to the International Society of Automation, ACS is defined as a collection of processes, personnel, hardware, and software that influence the safe, secure, and reliable operation of an industrial process. This essentially encompasses all components involved in automating an industrial operation, including sensors, controllers, actuators, and communication networks.

Initially, the term was applied to continuous process industries like refining where it was compatible with:
Enterprise Integration Standards like ISA95
Networking standards like ISA100
Industrial device configuration standards like ISA108

How do OT and ACS Concepts Compare

Neither OT or ACS definitions (above) specify an Architecture or the Professional Skills involved, so it is difficult to assess:

- Where they should fit in the Enterprise Architecture
- Who should be responsible for design, support, and maintenance

Sometimes OT and ACS terms are used as synonyms; however, this may be misleading or even dangerous.

- Depending on the Enterprise Architecture, they may actually be opposites
- As a general rule, an ACS approach is better for hazardous facilities like refineries or fossil power plants, and
- An OT approach may be better for specialized environments like electrical distribution or renewables generation.

Unfortunately, neither definition is tied to a system architecture or the responsible professional groups involved. However, these are important to understanding how to use both.

As a result, it is challenging to compare these terms, as neither identify where they fit in the Enterprise Architecture nor even who is responsible for them. Unfortunately, the two terms are sometimes used as synonyms. However, this may be untrue, misleading, or even dangerous, as ACS may be better suited for dangerous industrial facilities.

As stated above, "A principal driver of the adoption of the OT term was that the nature of operational technology platforms had evolved from bespoke proprietary systems to complex software portfolios that rely on IT infrastructure." Thus, ACS and OT are, at best, complementary approaches and, in many cases, may even be opposites.

By contrast, ISA 95, ISA99, and ISA 84 primarily addressed process industries where "bespoke proprietary systems" (such as DCS, SCADA, PLCs, etc.) were the norm. Since these vendors were used to working with dangerous processes, they implemented secure architectures with high-integrity, thoroughly tested hardware and software. In fact, it was these secure systems that OT wished to displace. ISA also clearly established who is responsible for the safe design, operation, and maintenance of the ACS. These professions include Control Engineers (for control strategies and Operator HMIs), Electrical Engineers for hazardous area explosion safety, and Process Engineers for Optimization Strategies).

It is true, however, that better interfaces between ACS and IT are desirable (see MLM-007-A), and an "OT approach" may sometimes be appropriate. However, PERA proposes that this is better done with better interfacing rather than "integration". At the very least, the designers should be clear about which approach they are taking, and why.

Characteristics of IT Infrastructure

OT evolved for "complex software portfolios that rely on IT infrastructure"

PRO	CON
• Designs are modern and vendor architectures are flexible	• Products not intended for hazardous environments or industrial networks.
• Equipment is low cost (Moore's law)	• Equipment less reliable than ACS
• Rapid product development cycles	• Short cycles reduce product stability and increase training costs
• Software used is modern and programmers are widely available	• IT software failures are high (66% according to Standish annual report)

6

As stated above, "A principal driver of the adoption of the OT term was that the nature of operational technology platforms had evolved from bespoke proprietary systems to complex software portfolios that rely on IT infrastructure."

This results in both PROs and CONs for the use of IT infrastructure for OT applications.
PROs include:

- Designs are modern and vendor architectures are flexible
- Equipment is low cost (Moore's law)
- Rapid product development cycles
- Software used is modern and programmers are widely available

CONs Include:

- Products are not intended for hazardous environments or industrial networks.
- Equipment is likely to be less reliable and robust than ACS
- Short development cycles reduce product stability and increase training requirements
- IT software failures are high. "According to the Standish Group's Annual CHAOS 2020 report, 66% of technology projects end in partial or total failure (based on the analysis of 50,000 projects globally). While larger projects are more prone to encountering challenges or failing altogether, even the smallest software projects fail one in ten times.

Characteristics of ACS Infrastructure

ACS evolved from "bespoke proprietary systems" (such as DCS, SCADA, PLCs, etc.).

PRO	CON
• ACS are designed to run dangerous and costly equipment and facilities • Products are reliable, robust, and certified to engineering standards • Longer development cycles improve product stability and reduce training • Software is configured rather than programmed reducing software bugs and improving cybersecurity.	• ACS products are typically more expensive. • ACS products are typically one generation behind "state-of-the-art" • Plant personnel require training in specialized devices and networks • Software configuration is less flexible than custom programming.

7

By contrast, ACS evolved from "Bespoke proprietary systems (such as DCS, SCADA, PLCs, etc.)." These were designed to work with dangerous processes in facilities that cost millions or even billions of dollars.

This results in both PROs and CONs for the use of ACS Infrastructure for OT systems.
PROs include:

- ACS are designed to work with dangerous processes costing millions or billions of dollars.
- Products are reliable, robust, and certified to engineering standards for industrial environments, including ISA 95 (Process Plant Enterprise Integration), ISA 99 (Automation Cybersecurity), ISA 100 (industrial Networks), ISA 108 (Industrial device and network Configuration), and ISA 84 (Safety Systems).
- Longer development cycles improve product stability and reduce training costs.
- Software is configured rather than programmed, reducing software bugs and improving cybersecurity.

CONs Include:

- ACS products are typically more expensive.
- ACS products are typically one generation behind "state-of-the-art".
- Plant personnel require training in specialized devices and networks.
- Software configuration is less flexible than custom programming.

ISA (and other engineering standards) clearly establish who is responsible for the safe design, operation, and maintenance of the ACS. These professions include Control Engineers (for control strategies and Operator HMIs), Electrical Engineers for hazardous area explosion safety, and Process Engineers for Optimization Strategies).

Two of the most basic parameters for comparison of ACS and IT infrastructure are:

- Performance (measured as 4Rs, Reliability, Repairability, Response, and Resolution), and
- Cybersecurity

The next two slides compare the Performance and Cybersecurity of ACS and IT infrastructures.

4R Performance of ACS & IT Infrastructure

4Rs	Control Systems	Control Networks	IT Systems	IT Networks
RELIABILITY (Mean Time Between Failure)	MTBF (mean time between control failures) (months to years)	MTBF (mean time between link failures) (months to years)	MTBF (mean time between application restarts) (days to weeks)	MTBF (mean time between link failure) (months)
REPAIRABILITY Mean Time To Repair)	MTTR -time to backup switchover (milli-secs to hrs)	MTTR -time to backup switchover) (milli-sec to secs)	Mean time between application updates (weeks to months)	Mean time between Link failures (days to weeks)
RESPONSE	Time from poll to response (milli-sec to secs)	Latency (milli-sec)	Time from <Enter> to response (seconds)	"Long loop" Response time (fractions of seconds)
RESOLUTION	A to D converter bits (typically 12 bits)	Band width (Points per second)	Floating Point number (32 or 64 bits)	Bandwidth (Carrier frequency Ghz)

8

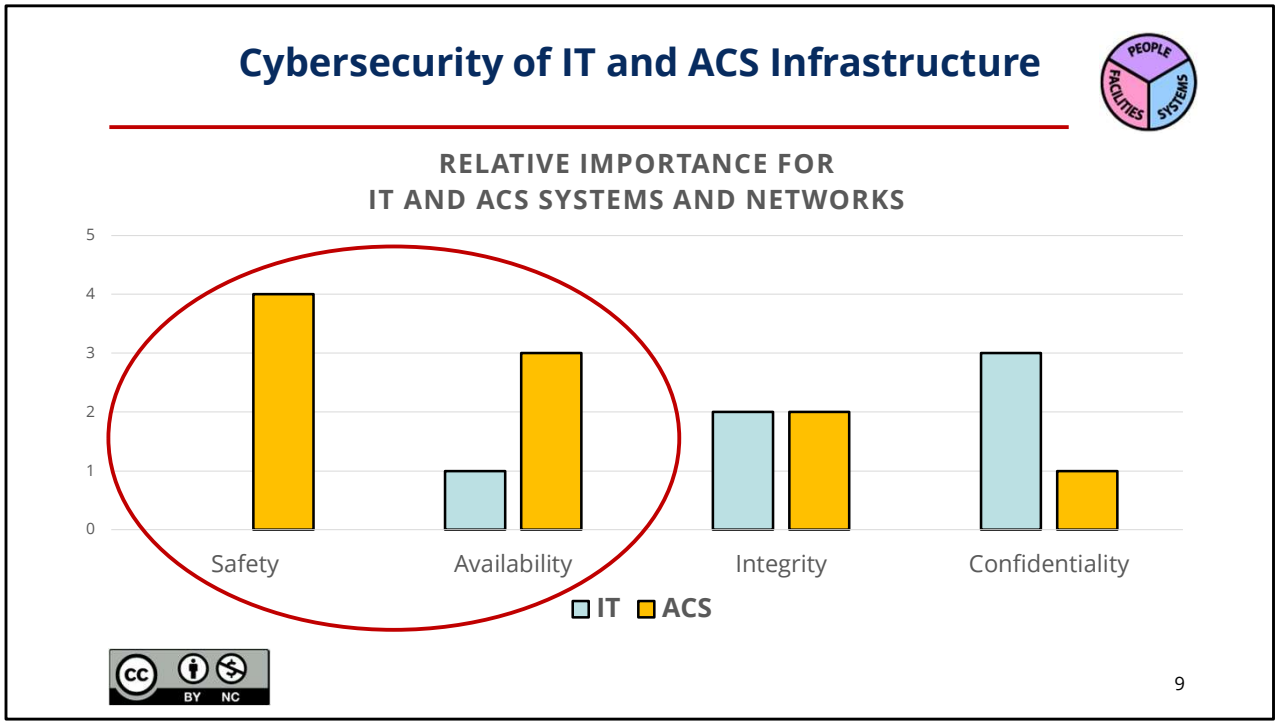
1. **Reliability** is measured as Mean Time Between Failures.
   For Control Systems, this is typically of the order of months to years, Similarly, Control Networks are expected to work reliably for months or years.
   For IT systems the mean time between application restarts would typically be weeks. IT networks will likely be more reliable, failing every few months.
   Note that network failures or speed reductions may degrade all devices on that network, so small networks are actually better.

2. **Repairability –** Control systems are often "backed up" at both the sensor power supply and the processor. If so, the switchover can be instantaneous, but if not, hardware replacement can take some hours. Industrial Control Networks are usually backed up with automated switchover.
   In the event of a workstation failure, IT applications may be run on a different PC. However, software updates, particularly on servers or network failures, may result in downtime. Network updates or device upgrades on Industrial networks are, therefore, usually delayed until plant shutdowns.

3. **Response** – Control systems "poll" large numbers of sensors and other control devices, making "latency" a key performance parameter.
   Control networks are set up to minimize response time. Data packets are

often optimized to send information efficiently in high-noise electrical environments.
IT systems usually exchange large “screens of data” where the response time of the host is the controlling factor.
IT networks are, therefore, configured to maximize total throughput rather than minimize latency.

4. **Resolution** - Control systems often receive data from sensors as low-resolution “integers” (typically 12 to 14 bits). Checksums and error correction are optimized for this type of data.
Control data is then transmitted to HMIs and historians using control networks that work efficiently in high-noise electrical environments.
IT systems deal primarily with numbers and ASCII characters in traditional formats.
IT networks are configured to maximize Giga-Hertz throughput for large numbers of workstations.



1. **The Cybersecurity Goals for the IT infrastructure of an enterprise** are defined as Confidentiality, Integrity, and Availability, In that order. These are also called the CIA triad. Although these are not quantified with any units or measurement, for the purpose of this comparison, we have assigned Confidentiality an importance of 3, Integrity as 2, and Availability as 1.

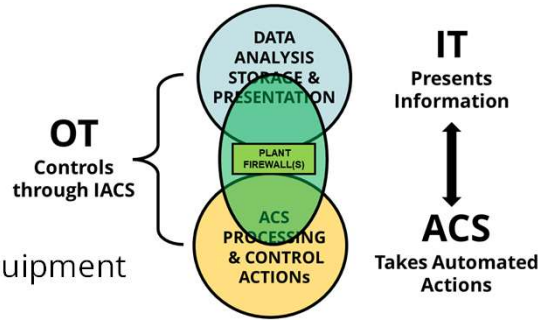
2. **The Cybersecurity Goals for the ACS infrastructure** were determined by ISA99 as SAIC (Security Availability, Integrity, and Confidentiality). Safety is the highest priority and was assigned an importance of 4. Availability, Integrity, and Confidentiality were assigned 3,2 and 1, respectively.

3. **The priority of IT and ACS cybersecurity goals (CIA and SAIC)** are in fact, reversed, with Safety added for ACS as the highest priority.

4. **For OT systems, Safety and Availability will be the highest priorities** (shown by red oval). It is, therefore, unlikely that the use of IT infrastructure is viable for OT applications with high safety or availability requirements. Availability is the lowest priority for IT infrastructure, and Safety is not prioritized at all.

Key "Take-away" Messages

1. **OT may be Advantageous for:**
   1. Sophisticated optimization
   2. Interfaces to IT systems
   3. Patching and updating
2. **ACS may be Advantageous for:**
   1. Control of hazardous or costly equipment
   2. Reliability and maintainability
   3. Cybersecure operation



10

1. **OT may be Advantageous for:**
   - Sophisticated optimization
   - Interfaces to Corporate IT systems
   - Patching and updating

2. **ACS may be Advantageous for:**
   - Control of hazardous or costly equipment
   - Reliability and maintainability
   - Cybersecure operation

OT may provide optimization and improve interfaces between ACS and IT systems (see MLM-007-A).
PERA promotes secure interfaces rather than "Enterprise integration".
Secure interfaces ensure that control and security can be maintained, even if OT applications fail or are compromised.
At the very least, designers must be clear about which approach they are taking, and why.

Key "Take-away" Messages

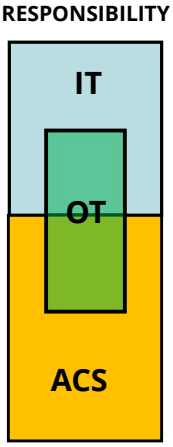
3. It is essential to clearly identify professional roles

1. IT applications are developed and supported within the IT Infrastructure
2. OT applications require skills from both ACS and IT environments including loop tuning and stability, Human Machine Interfaces, process optimization strategies, etc.
3. ACS responsibilities are clearly established including skills and tools for working in hazardous environments, equipment and controls troubleshooting,

IT Specialists

IT & OT Specialists Collaborate

Control Engineers



11

3. It is essential to clearly identify professional roles

- IT applications are developed and supported within the IT Infrastructure
- OT applications require skills from both ACS and IT environments including loop tuning and stability, Human Machine Interfaces, process optimization strategies, etc.
- ACS responsibilities are clearly established including skills and tools for working in hazardous environments, equipment and controls troubleshooting,

More Reading

Related MLMs:

- MLM-014-A ACS, IT and OT Definitions
- MLM-014-C What are Cloud, IoT and IIoT Systems
- MLM-014-D When to use Cloud, IoT and IIoT Systems
- MLM-034-A Cybersecure IT and ACS Interfacing

3d Party References

- ISA 62443-1-1 Concepts and Models

:

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,