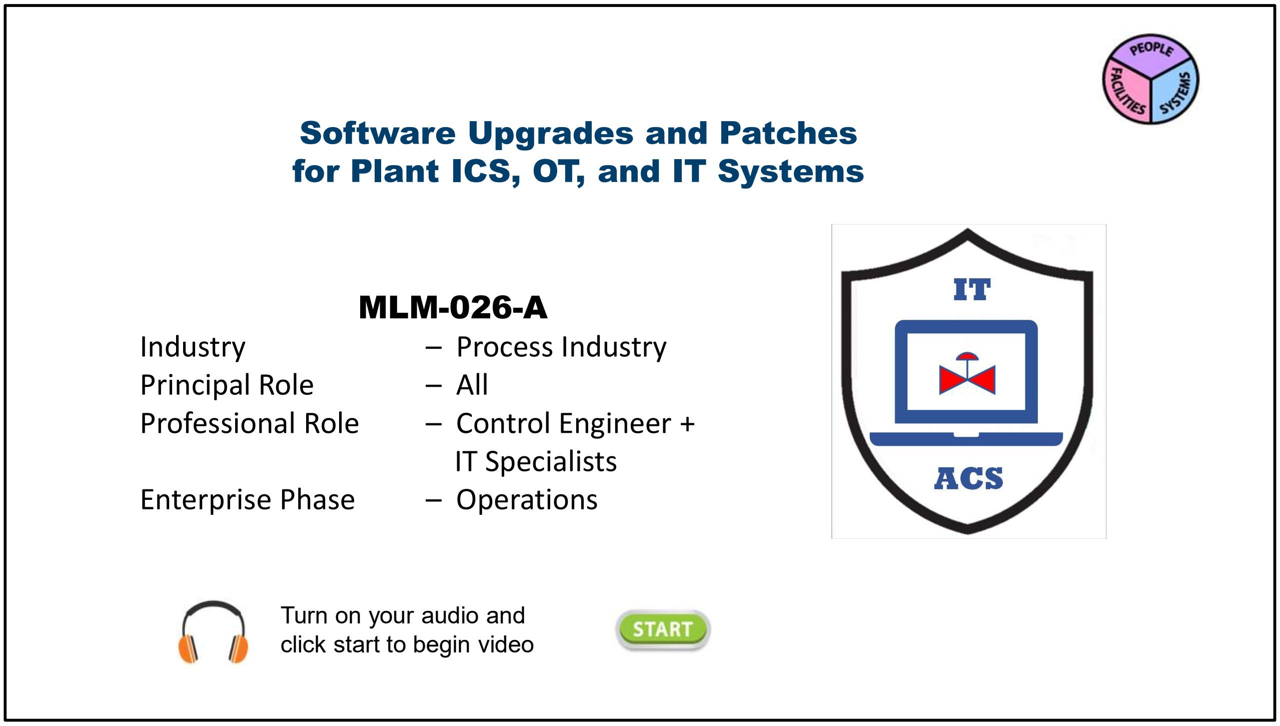


Software Upgrades and Patches for Plant ICS, OT, and IT Systems

MLM-026-A

Industry	– Process Industry
Principal Role	– All
Professional Role	– Control Engineer + IT Specialists
Enterprise Phase	– Operations

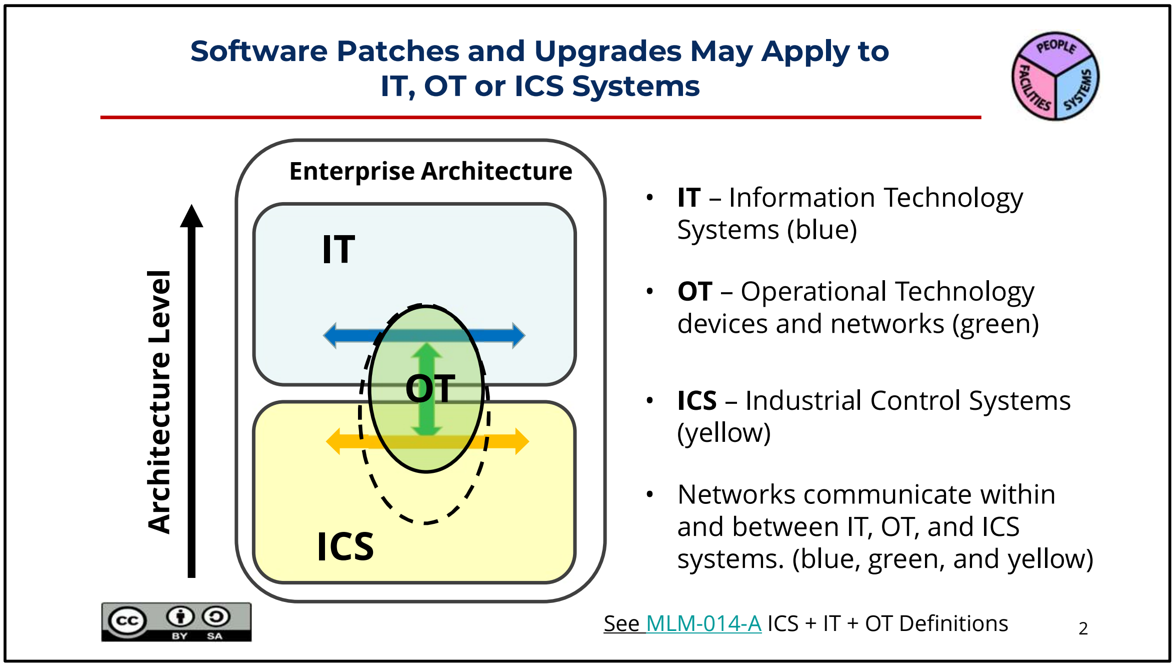
Turn on your audio and
click start to begin video

PERA addresses all levels in the Enterprise Architecture. This MLM addresses Software Updates and Patch Management) for

- Automation and Control Systems (ICS),
- Operational Technology (OT) including both IT and ICS infrastructure, and
- IT systems including plant and corporate architecture levels.

The intended audience is ICS asset owners along with integration and maintenance service providers supporting the asset owner.

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



Software Patches and Upgrades May Apply to IT, OT or ICS Systems

- **IT** – Information Technology Systems (blue)
- **OT** – Operational Technology devices and networks (green)
- **ICS** – Industrial Control Systems (yellow)
- Networks communicate within and between IT, OT, and ICS systems. (blue, green, and yellow)

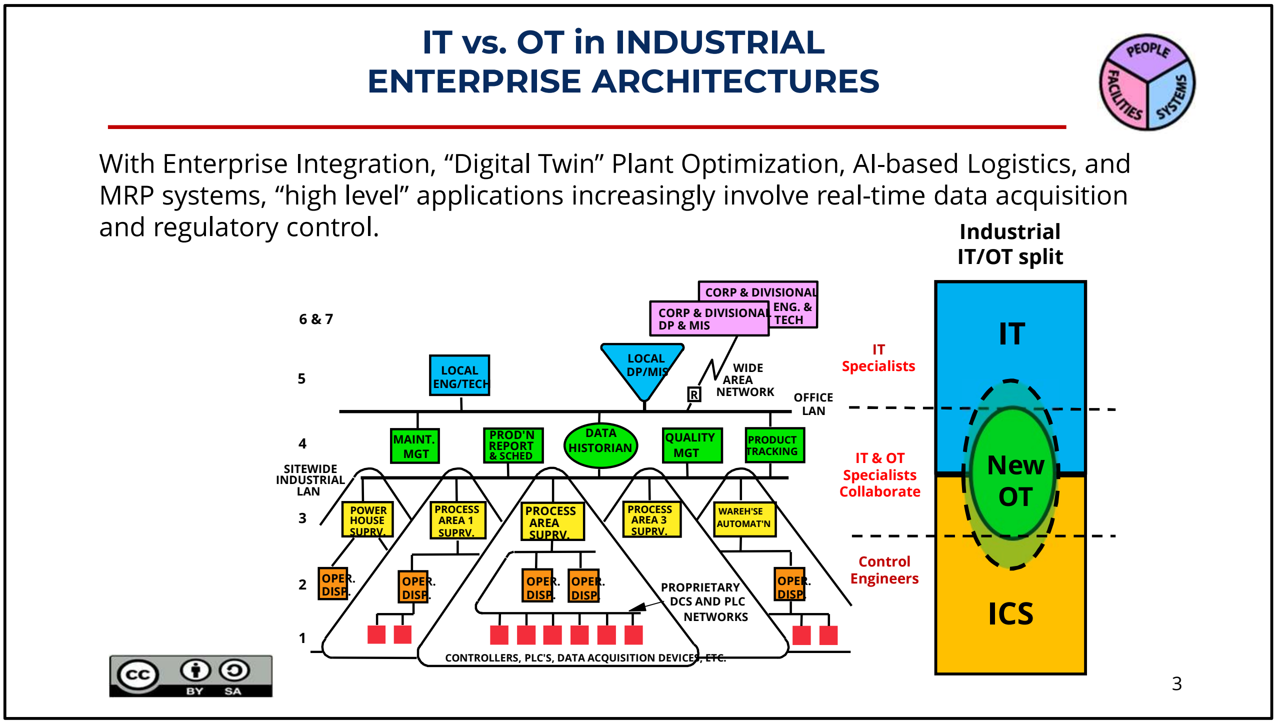
See MLM-014-A ICS + IT + OT Definitions

It is important to define IT, OT, and ICS clearly.

Good working definitions of these are:

- An IT system is used for data-centric computing that does not control equipment.
- An ICS is used to monitor events, processes, and devices and to make adjustments to equipment and operating targets.
- OT systems may “overlay” both ICS and IT areas. They may use IT infrastructure and technologies in ICS Architectural areas and ICS technologies in IT Architectural areas.

See MLM-014-A for more detailed definitions of IT, OT, and ICS.



IT vs. OT in INDUSTRIAL ENTERPRISE ARCHITECTURES

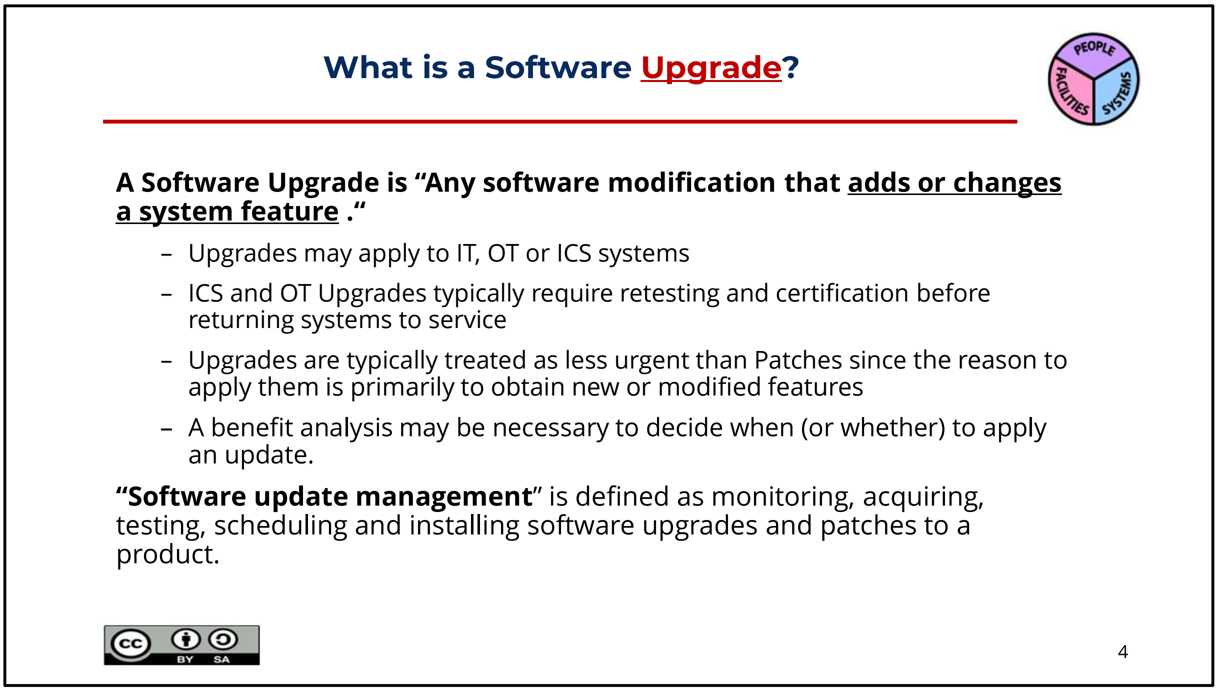
With Enterprise Integration, “Digital Twin” Plant Optimization, AI-based Logistics, and MRP systems, “high level” applications increasingly involve real-time data acquisition and regulatory control.

With increased Enterprise Integration, “Digital Twin” Plant Optimization, AI-based Logistics, and MRP systems, “high level” applications increasingly involve real-time control of plant operations.

This requires expertise in real-time control algorithms, model-based control, loop instability and other Industrial Control System (ICS) technologies that have “grown” from plant regulatory control.

Similarly, IT specialists are implementing IT systems in plant environments (like bar code readers or building access badge readers). This requires IT specialists to learn more about intelligent device specifications and real-time data acquisition.

Thus, it is not possible to “draw a line” where Control Engineers stop and IT Specialists begin (if it ever was). Increasingly, systems at levels 3 and 4 must be designed and supported as a “partnership” between ICS and IT resources. We are even seeing IIoT and IoT devices implemented at Levels 1 and 2, and control engineering expertise applied at level 4 and above.



What is a Software Upgrade?

A Software Upgrade is “Any software modification that adds or changes a system feature .“

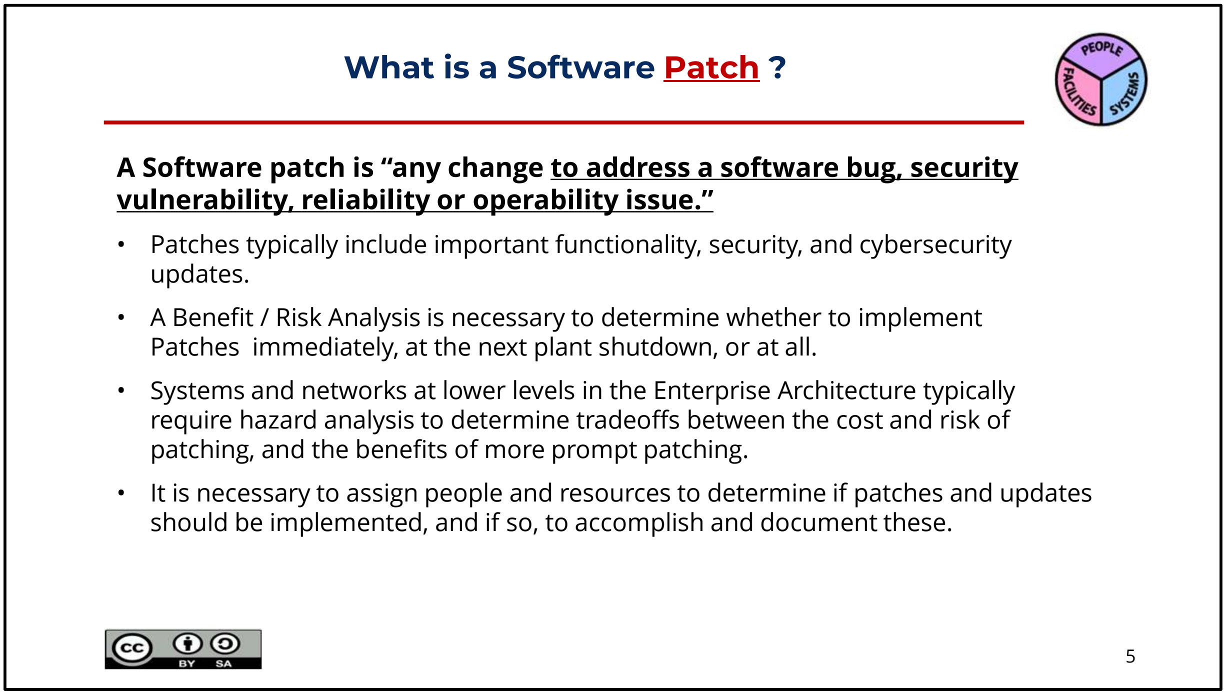
- Upgrades may apply to IT, OT or ICS systems
- ICS and OT Upgrades typically require retesting and certification before returning systems to service
- Upgrades are typically treated as less urgent than Patches since the reason to apply them is primarily to obtain new or modified features
- A benefit analysis may be necessary to decide when (or whether) to apply an update.

“Software update management” is defined as monitoring, acquiring, testing, scheduling and installing software upgrades and patches to a product.

A Software Upgrade is “Any software modification that adds or changes a system feature .“

- Upgrades may apply to IT, OT or ICS systems
- ICS and OT Upgrades typically require retesting and certification before returning systems to service
- Upgrades are typically treated as less urgent than Patches since the reason to apply them is primarily to obtain new or modified features
- A benefit analysis may be necessary to decide when (or whether) to apply an update.

“Software update management” is defined as monitoring, acquiring, testing, scheduling and installing software upgrades and patches to a product.



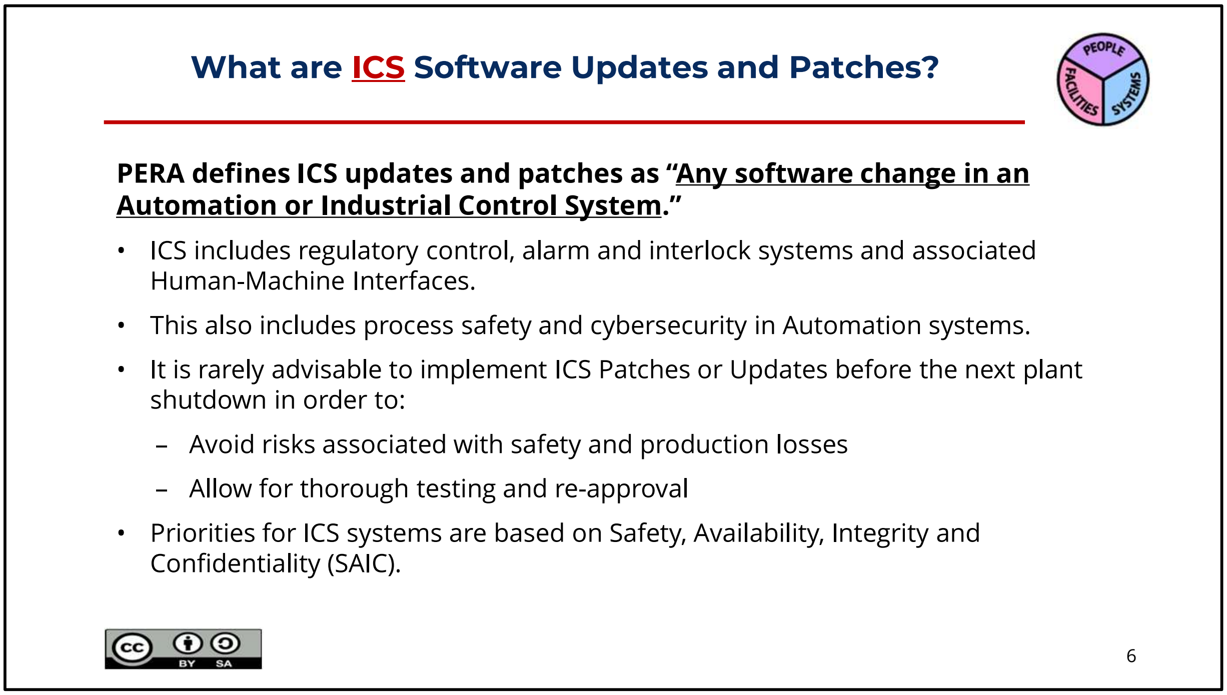
What is a Software Patch ?

A Software patch is "any change <u>to address a software bug, security vulnerability, reliability or operability issue."</u>

- Patches typically include important functionality, security, and cybersecurity updates.
- A Benefit / Risk Analysis is necessary to determine whether to implement Patches immediately, at the next plant shutdown, or at all.
- Systems and networks at lower levels in the Enterprise Architecture typically require hazard analysis to determine tradeoffs between the cost and risk of patching, and the benefits of more prompt patching.
- It is necessary to assign people and resources to determine if patches and updates should be implemented, and if so, to accomplish and document these.

A Software patch is "any change <u>to address a software bug, security vulnerability, reliability or operability issue."</u>

- Patches typically include important functionality, security, and cybersecurity updates.
- A Benefit / Risk Analysis is necessary to determine whether to implement Patches immediately, at the next plant shutdown, or at all.
- Systems and networks at lower levels in the Enterprise Architecture typically require hazard analysis to determine tradeoffs between the cost and risk of patching, and the benefits of more prompt patching.
- It is necessary to assign people and resources to determine if patches and updates should be implemented, and if so, to accomplish and document these.



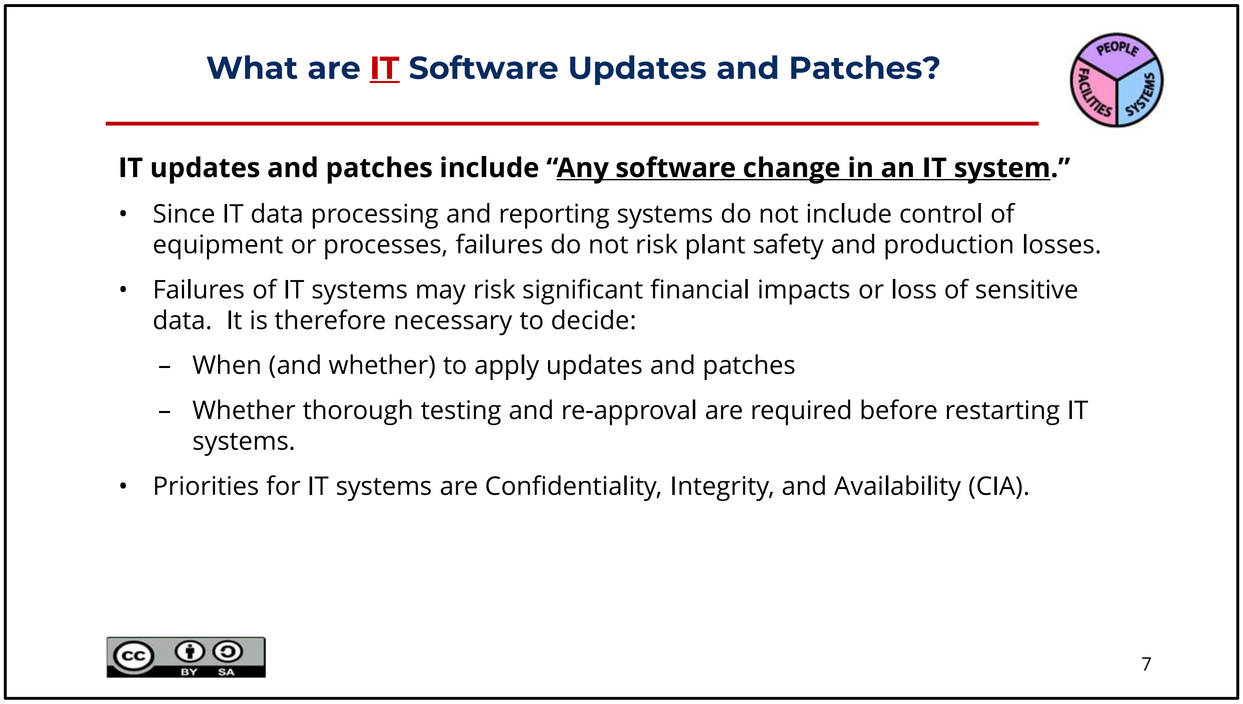
What are ICS Software Updates and Patches?

PERA defines ICS updates and patches as “<u>Any software change in an Automation or Industrial Control System</u>.”

- ICS includes regulatory control, alarm and interlock systems and associated Human-Machine Interfaces.
- This also includes process safety and cybersecurity in Automation systems.
- It is rarely advisable to implement ICS Patches or Updates before the next plant shutdown in order to:
  - Avoid risks associated with safety and production losses
  - Allow for thorough testing and re-approval
- Priorities for ICS systems are based on Safety, Availability, Integrity and Confidentiality (SAIC).

PERA defines ICS updates and patches as “<u>Any software change in an Automation or Industrial Control System</u>.”

- ICS includes regulatory control, alarm and interlock systems and associated Human-Machine Interfaces.
- This also includes process safety and cybersecurity in Automation systems.
- It is rarely advisable to implement ICS Patches or Updates before the next plant shutdown in order to:
  - Avoid risks associated with safety and production losses
  - Allow for thorough testing and re-approval
- Priorities for ICS systems are based on Safety, Availability, Integrity and Confidentiality (SAIC).



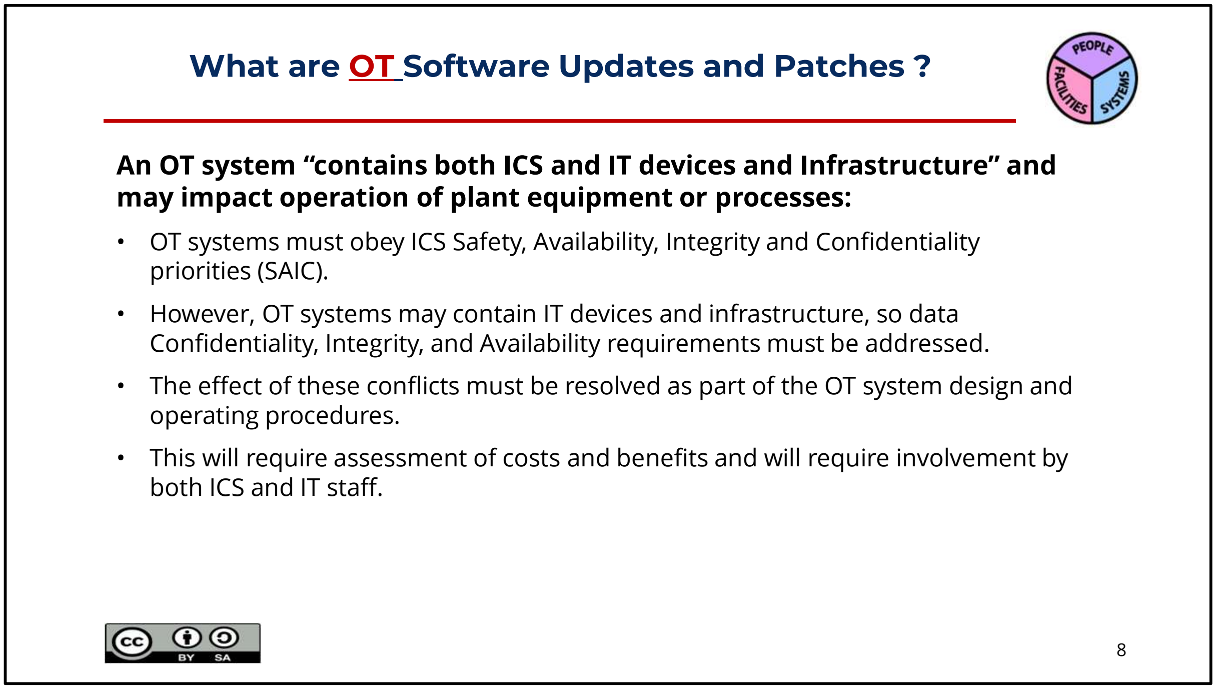
What are IT Software Updates and Patches?

IT updates and patches include "<u>Any software change in an IT system</u>."

- Since IT data processing and reporting systems do not include control of equipment or processes, failures do not risk plant safety and production losses.
- Failures of IT systems may risk significant financial impacts or loss of sensitive data. It is therefore necessary to decide:
  - When (and whether) to apply updates and patches
  - Whether thorough testing and re-approval are required before restarting IT systems.
- Priorities for IT systems are Confidentiality, Integrity, and Availability (CIA).

IT updates and patches include "<u>Any software change in an IT system</u>."

- Since IT data processing and reporting systems do not include control of equipment or processes, failures do not risk plant safety and production losses.
- Failures of IT systems may risk significant financial impacts or loss of sensitive data. It is therefore necessary to decide:
  - When (and whether) to apply updates and patches
  - Whether thorough testing and re-approval are required before restarting IT systems.
- Priorities for IT systems are Confidentiality, Integrity, and Availability (CIA).



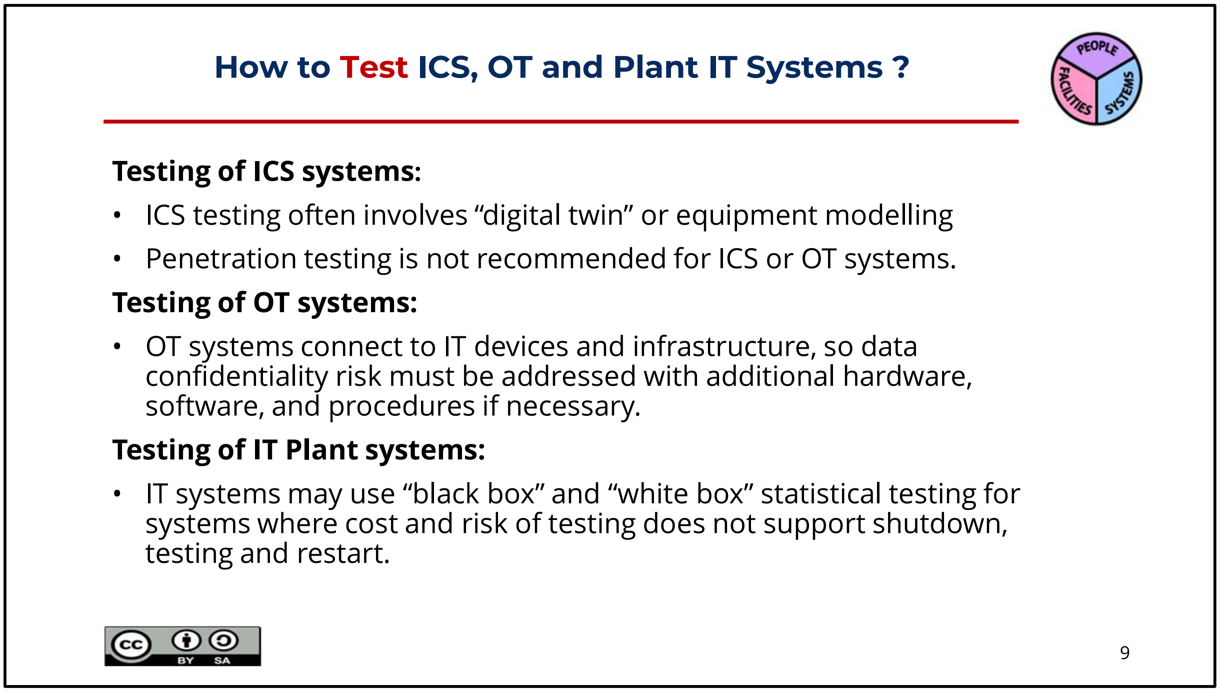
What are OT Software Updates and Patches ?

An OT system “contains both ICS and IT devices and Infrastructure” and may impact operation of plant equipment or processes:

- OT systems must obey ICS Safety, Availability, Integrity and Confidentiality priorities (SAIC).
- However, OT systems may contain IT devices and infrastructure, so data Confidentiality, Integrity, and Availability requirements must be addressed.
- The effect of these conflicts must be resolved as part of the OT system design and operating procedures.
- This will require assessment of costs and benefits and will require involvement by both ICS and IT staff.

An OT system “contains both ICS and IT devices and Infrastructure” and may impact operation of plant equipment or processes:

- OT systems must obey ICS Safety, Availability, Integrity and Confidentiality priorities (SAIC).
- However, OT systems may contain IT devices and infrastructure, so data Confidentiality, Integrity, and Availability requirements must be addressed.
- The effect of these conflicts must be resolved as part of the OT system design and operating procedures.
- This will require assessment of costs and benefits and will require involvement by both ICS and IT staff.



How to Test ICS, OT and Plant IT Systems ?

Testing of ICS systems:

- ICS testing often involves "digital twin" or equipment modelling
- Penetration testing is not recommended for ICS or OT systems.

Testing of OT systems:

- OT systems connect to IT devices and infrastructure, so data confidentiality risk must be addressed with additional hardware, software, and procedures if necessary.

Testing of IT Plant systems:

- IT systems may use "black box" and "white box" statistical testing for systems where cost and risk of testing does not support shutdown, testing and restart.

Testing of ICS systems:

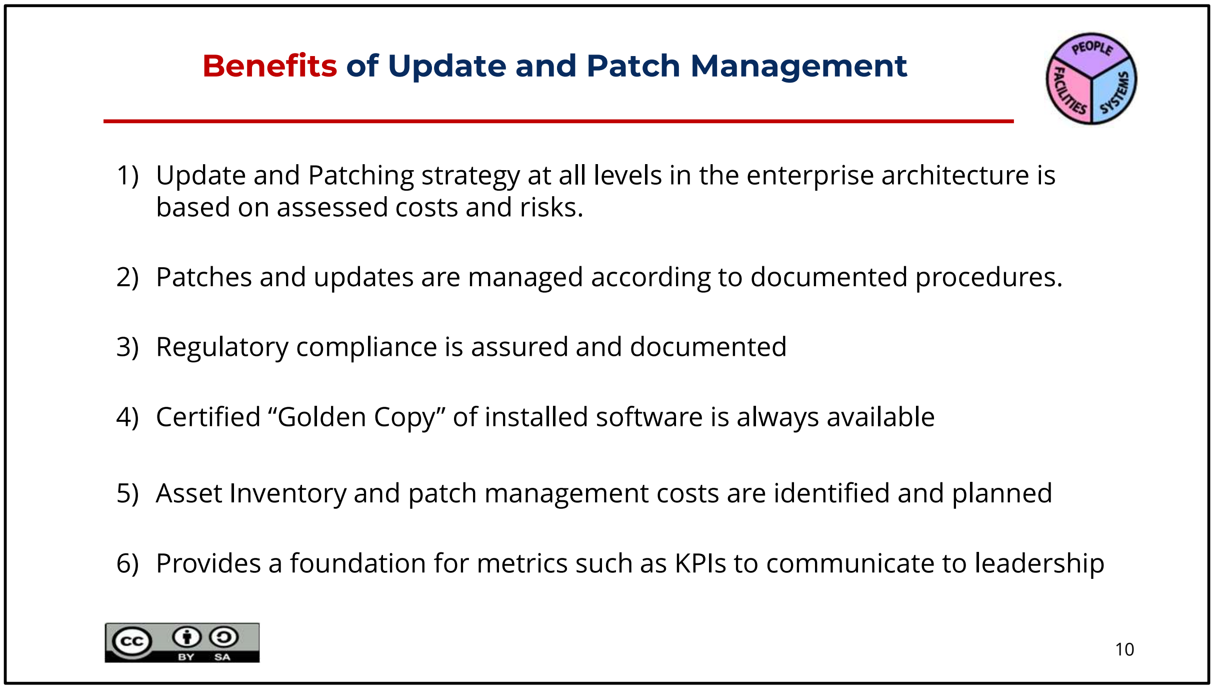
- ICS testing often involves "digital twin" or equipment modelling
- Penetration testing is not recommended for ICS or OT systems.

Testing of OT systems:

- OT systems connect to IT devices and infrastructure, so data integrity risk must be addressed with additional hardware, software, and procedures.

Testing of IT Plant systems:

- IT systems may use "black box" and "white box" statistical testing for systems where cost and risk of testing does not support shutdown and thorough acceptance testing.

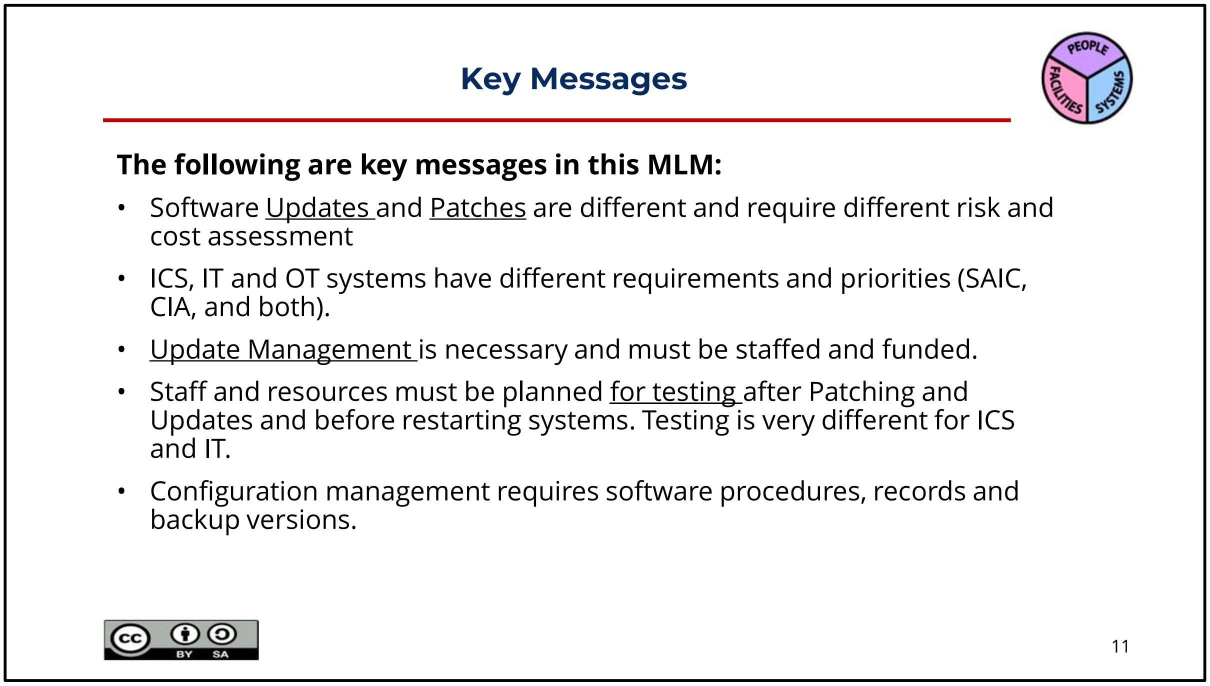


Benefits of Update and Patch Management

1) Update and Patching strategy at all levels in the enterprise architecture is based on assessed costs and risks.
2) Patches and updates are managed according to documented procedures.
3) Regulatory compliance is assured and documented
4) Certified “Golden Copy” of installed software is always available
5) Asset Inventory and patch management costs are identified and planned
6) Provides a foundation for metrics such as KPIs to communicate to leadership

Benefits of Update and Patch Management

- Update and Patching strategy at all levels in the enterprise architecture is based on assessed costs and risks.
- Patches and updates are managed according to documented procedures.
- Regulatory compliance is assured and documented
- Certified “Golden Copy” of installed software is always available
- Asset Inventory and patch management costs are identified and planned
- Provides a foundation for metrics such as KPIs to communicate to leadership



Key Messages

PEOPLE
FACILITIES
SYSTEMS

The following are key messages in this MLM:

- Software Updates and Patches are different and require different risk and cost assessment
- ICS, IT and OT systems have different requirements and priorities (SAIC, CIA, and both).
- Update Management is necessary and must be staffed and funded.
- Staff and resources must be planned for testing after Patching and Updates and before restarting systems. Testing is very different for ICS and IT.
- Configuration management requires software procedures, records and backup versions.

The following are key messages in this MLM:

- Software Updates and Patches are different and require different risk and cost assessment
- ICS, IT and OT systems have different requirements and priorities (SAIC, CIA, and both).
- Update Management is necessary and must be staffed and funded as part of maintenance management.
- Staff and resources must be planned for testing after Patching and Updates and before restarting systems. Testing is very different for ICS and IT.
- Configuration management requires software procedures, records and backup versions.

Further Information

- **Related MLMs**
  - MLM-014-A : ICS + IT + OT Definitions
  - MLM-026-B : Security Update and Patch Management of Plant Systems for Vendors
  - MLM-026-C: Update, Testing, and Patching of plant systems for EPC and Service Providers.
- **References:**
  - ISA TR62443-2-3 Patch Management in the ICS Environment
  - Also search for cybersecurity articles at ISA Global Cybersecurity Alliance

Please click here to provide feedback on this MLM.

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,