Learning Map-014

Reliability and Security of Plant Systems

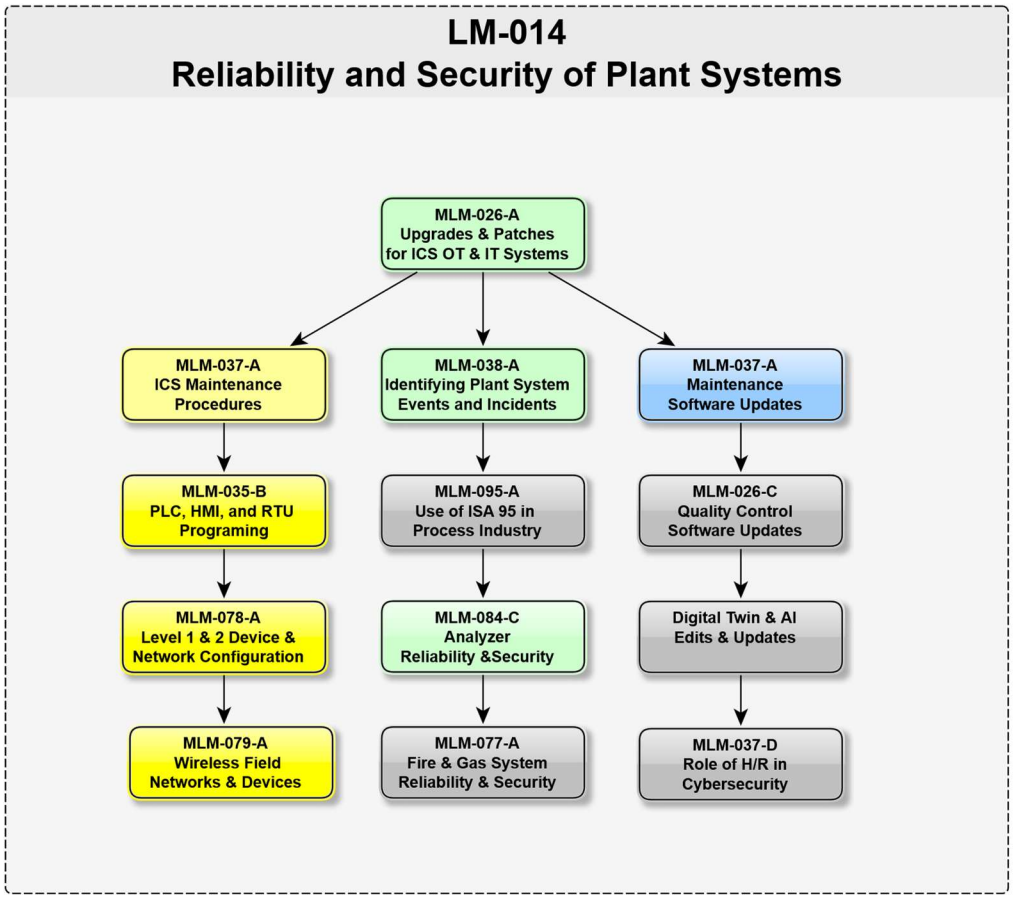
Intended Audience:

Plant personnel involved in Maintenance of Control and Information Systems during Operations Phase, particularly reliability and security including

1. Plant Control Engineers working on ICS and OT systems
2. Plant IT Specialists working on OT systems (involving ICS and IT)
3. Human Resources Personnel
4. Quality Laboratory Management
5. Process Engineers
6. Maintenance Management

Context and Objectives of this Learning Map

PERA emphasizes the importance of addressing human and organizational aspects (People) in each phase of the enterprise.



This Learning Map is focused on work processes performed by:

- Control engineers and maintenance technicians who maintain and operate Industrial Control Systems (shown in yellow in the above diagram).
- IT specialists in maintaining and operating IT systems (shown in blue)
- Control Engineers and IT specialists working together to maintain OT systems that require both ICS and IT expertise (shown in green)

To facilitate workflow automation, and ultimately the use of AI agents, we have chosen to implement these Learning Maps as "Intelligent" XML Diagrams.

Objectives of this Learning Map

This Learning Map was originally intended to address Cybersecurity and Patch Management associated with Plant Control and Information Systems. However, as MLMs were assembled, it became clear that Cybersecurity was just one parameter associated with reliability (MTBF) of these systems.

When operations staff experience an unexpected "Event" it is much more likely to be the result of an equipment, software, or operations failure than from a cyber-attack. Thus, the benefit from improved detection and response is more likely to result in improved MTBF (Mean Time Between Failure) than from preventing or responding to a cyber-attack.

Furthermore, it became clear that it was impractical to estimate the probability of:

- A cyber-attack (whether by a nation state or a script kiddie),
- Successful penetration, into a sensitive or critical system
- Significant losses that might result from a successful attack.

Without credible, quantifiable impacts, it is impossible to do "consequence-based" design that can be compared to other expenditures to reduce risk for the enterprise.

Initial assessment (see MLM-038-A) has also indicated that if cybersecurity detection were improved, most benefits would be associated with reducing downtime and equipment damage.

It was therefore decided that it was more useful to combine security and reliability risks as a single Mean Time Before Failure (MTBF) value. This has the added benefit that costs and benefits may then be compared on a common basis to other risks for the enterprise.