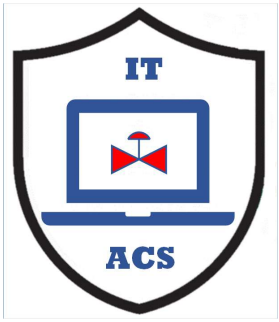
Principal Roles in Automation and Control System (ACS) Cybersecurity

MLM-001-A

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



Turn on your audio and click start to begin video

START

This module defines the "Principal Roles" involved in defining and maintaining the Cybersecurity of Industrial Automation and Control Systems (ACS)

Its intended audience is anyone with an interest in ACS Cybersecurity

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

What is a "Principal Role"

In ISA 62443-1-1 a "Principal Role" is defined as:

an organizational entity such as Owner, Operator, Maintainer, Integrator, Commissioner, or Supplier.

- Each Principal Role has different responsibilities.
- Swimlane diagrams may be used to show the exchange of Deliverables between Principal Roles.
- This MLM describes Principal Roles and their "Deliverables" during each Enterprise Phase.

In ISA 62443-1-1, a "Principal Role" is defined as "an organizational entity that includes the facility Owner, Operator, Maintainer, Integrator, Commissioner, or Supplier".

Each Principal Role has different responsibilities during the Enterprise Lifecycle, such as an Owner/Operator or a Product Supplier.

Swimlane diagrams may be used to show the exchange of Deliverables between Principal Roles. These Deliverables are often exchanged at the beginning or end of Enterprise Phases.

Enterprise Phase boundaries are also a useful "break point" because Principal Roles often begin or end their involvement at these points. ("Divide and conquer", but "Don't cut where it is thickest")

This MLM describes Principal Roles, their responsibilities, and deliverables during each Enterprise Phase.

Principal Roles vs. Professional Roles

From ISA 62443

| requirement Principal Role
| Professional Roles
| Organization Chart Positions

- Swimlane diagrams show deliverables exchanged between Principal Roles
- Workflow diagrams show deliverables exchanged between Professional Roles

3

Principal Roles contain Professional Roles, and these Professional Roles are assigned to organization chart positions that are, in turn, assigned to employees or third-party contractors.

Principal Role
| Professional Roles
| Org. Chart Positions

The 62443 standard includes only the first two items in this hierarchy. Professional Roles are assigned to organization chart positions when establishing the company's cybersecurity program.

Requirements, as defined by ISA/IEC 62443, may be assigned to both Principal Roles and Professional Roles.

Swimlane diagrams may be used to show the exchange of deliverables between Principal Roles.

- Workflow diagrams may be used to show the exchange of deliverables between Professional Roles.

These relationships are described in *MLM-001-B Professional Roles in Cybersecurity*.

Principal Roles

The following (green) Principal Roles are described in *IEC/ISA 62443-1-1 ACS Cybersecurity. Blue items were added or modified by PERA:*

- Owner / Operator
- Integrator (Engineer, Procure, Constructor)
- Vendor (Product Supplier)
- Service Provider (including Maintainer)
- Regulator (e.g., Government)
- Approvers (e.g., Insurers, Financers)
- Additional Principal Roles may be involved.

Interfaces between these Principal Roles are typically shown as "Swim Lane Diagrams".

4

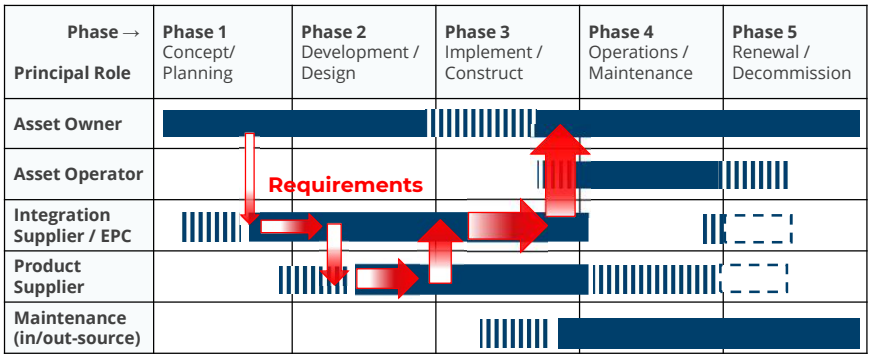
The following Principal Roles are described in MLM-001-B Interfaces between Principal Roles

Owner / Operator
Integrator EPC
Vendor / Product Supplier
Asset Maintainer
Regulators (e.g., Government)
Approvers (e.g., Insurers / Financiers)
Additional Principal Roles may be involved.

Interfaces between these Principal Roles are typically shown as "Swim Lane Diagrams".

Principal Roles' Engagement Changes Across Phases

Each Principal Role is engaged to a different degree as the ACS lifecycle progresses.



5

This is a simplified example of a horizontal swimlane type diagram. Each row represents a different principal role, and time progresses left to right. As you can see, the degree of involvement of different principal roles varies during different phases of the enterprise lifecycle. Solid bars indicate phases where each principal role has a high degree of involvement; stripes indicate some involvement. Dashed boxes indicate a potential for limited involvement, such as troubleshooting. In phases without any color, that principal role has no involvement.

The interface between different principal roles can be summarized by the information they are exchanging. An asset owner hands off their cybersecurity requirements to the integrator or EPC, who perform their 62443 requirements and hand off the necessary information to suppliers so they can complete their requirements, etc. At the end of the cycle, the integrator sends all of the information to the owner. The arrows become wider and darker, indicating that more work is being done and information is being generated at each step. Each group has requirements under 62443 to perform, which ultimately begin and end with the asset owner.

Many other cycles like this take place throughout the life of a facility. Some will be loops between maintenance, the asset owner, and product suppliers, and almost any combination of principal roles you can think of.

Note the slashes between the phase names. This shows that different principal roles will refer to these phases by different names. For example, what an asset owner calls the development phase, an EPC will call design phase. Sometimes, an owner will see an activity as a single phase while the integrator might see it as two or even three phases because of the nature of their work. As long as the deliverables to be exchanged between principal roles have been agreed upon, the phase divisions being different are not problematic.

Anatomy of an ISA-62443 Requirement

For each requirement, the 62443 standard establishes a set of inputs and deliverables.

Example requirements (during design phase, by Owner/Operator):

- "Define the risk tolerance for the ACS in operation, based on a business impact analysis."
  - Inputs - potential impact of misuse of the ACS on the business of the asset owner
  - Deliverables - consequence matrix, risk tolerance

6

For each Requirement, the 62443 standard establishes a set of Inputs and Deliverables.

For example, during the Design Phase, the Owner/Operator must

"Define the risk tolerance for the ACS in operation, based on a business impact analysis".

To do this, the Owner/Operator must define Inputs and Outputs for each Deliverable.

- Inputs – might include the potential impact of misuse of the ACS on the business of the asset owner (such as finances, HSE, reputation, legal obligations)
- Deliverables - might include a consequence matrix and a risk tolerance statement.

Owner/Operator Deliverables During Design and Fabrication Phase

Example owner/operator cybersecurity requirements:

Design Phase

- Defines the risk tolerance for ACS Cybersecurity
- Develops requirements of ACS Cybersecurity
- Verifies that the integrator maintains adequate maturity level

Fabrication/Construction Phase

- Supports the Commissioner with information for deployment of ACS cybersecurity
- Approves the cybersecurity solution deployed by the constructor
- Accepts the residual risk

7

As an example, let's look at cybersecurity Requirements for the Owner/ Operator during the Design and Fabrication Phases.

During the Design Phase, by the Owner

- Defines the risk tolerance for ACS Cybersecurity
- They also develop requirements of ACS Cybersecurity, and
- Verify that the Integrator achieves and maintains an adequate cybersecurity maturity level.

During the Fabrication/Construction Phase, by the Owner

- Supports the Commissioner with information for the deployment of ACS cybersecurity,
- Approves the cybersecurity solution deployed by Constructor, and
- Accepts the residual risk when organizational measures are implemented with the required maturity level.

Owner/Operator Deliverables During the Operations Phase

Operations/Maintenance Phase

OWNER

- Verifies that the asset operator achieves and maintains the required maturity level
- Verifies that the maintainer achieves and maintains an adequate maturity level
- Triggers a re-evaluation of the protection concept and the achieved PL-A
- Supports the Maintainer with information for maintenance of the ACS
- Approves the new protection concept
- Approves the achieved protection levels (PL-A) of the new protection concept
- Accepts the residual risk of the new protection concept.

OPERATOR

- Set organizational measures for operation
- Establish any compensating organizational measures for the ACS Solution
- Operate the ACS according to the organizational measures:
- Ensure that operating personnel act according to procedures
- Ensure that operating personnel achieve an adequate maturity level
- Get approval of the asset owner for achieved protection levels (PL-A)

8

Similarly, owner/operator Requirements are listed for each subsequent phase. These are provided so that you may examine them before proceeding to the next slide; however, they will not be discussed in this MLM.
Click next when you are ready to proceed.

Owner/Operator Deliverables (Continued)

MAINTAINER

- Maintain, and if necessary, update the protection concept for the ACS
- Actively purge classified data in assets that are put out of service
- Ensure that maintenance personnel act according to procedures
- Ensure that maintenance personnel achieve an adequate maturity level

Renewal / Decommissioning Phase

RENEWAL / UPGRADE

- For Turnarounds and other renewals without upgrade, see MAINTAINER
- For Upgrades, see Design and Construction Phase Roles

DECOMMISSIONING

- Verifies that the purging of classified data has been realized when decommissioning of the Automation Solution

Now review these Requirements for the Maintainer of the Owner's facility, and for the Renewal or Decommissioning Phase.
Click "NEXT" when you are ready to proceed to the next slide.

Additional Principal Roles

Only Owner/Operator Deliverables are listed in the previous few slides. However, Deliverables for each Principal Role are defined in more detail in *MLM-022-A Swim Lane Interfaces between Principal Roles.*

The Principal Roles defined in MLM-022-A include:

- Owner/Operator
- Integrator/EPC
- Product Supplier
- Asset Operator
- Asset Maintainer

Discussed in MLM "Swimlane Interfaces between Principal Roles"

- Regulators
- Approvers
- Contractors

Potential additional Principal Roles for an ACS program

10

Only Owner/Operator Deliverables are listed in the previous few slides. However,

Deliverables for each Principal Role are defined in more detail in *MLM-022-A Swim Lane Interfaces between Principal Roles*.

The Principal Roles defined here include:

The Owner/Operator,
The Integrator/EPC,
Product Supplier,
Asset Operator, and
Asset Maintainer.

In addition to these, other Principal Roles may be required by a given Enterprise's ACS Cybersecurity Program.
These extra Principal Roles may include:

Regulators (e.g. government bodies)
Approvers (e.g. insurers, or financers)
Contractors (e.g., Commissioning, Auditors)
and perhaps others)

See Use Case MLMs for specific examples of these Principal Roles

Key Messages in this MLM

- Principal Roles are performed by organizations such as Owner/Operator or Vendor.
- Interfaces between Principal Roles may be shown with “Swim Lane Diagrams”.
- Each Principal Role has multiple Professional Roles that are assigned to individuals or positions
- Requirements established by ISA 62443 are assigned to Professional Roles (within Principal Roles).
- Requirements are addressed as “Deliverables” provided by one Professional Role to another Professional Role.
- Exchange of Deliverables between Professional Roles may be shown in Workflow Diagrams

11

The following are the key messages in this MLM:

Principal Roles are performed by organizations

Interfaces between Principal Roles may be shown with “Swim Lane Diagrams”.

Each Principal Role has multiple Professional Roles that are assigned to individuals or positions

Requirements established by ISA 62443 are accomplished by Professional Roles within Principal Roles.

Requirements may be addressed in Deliverables.

More Reading

- **Related MLMs**
  - MLM-001-B Professional Roles in Cybersecurity
  - MLM-022-A Swim Lane Interfaces between Principal Roles
- To learn more about this MLM user interface, click here.
- Please give us your feedback on this learning module here.

For more information on cybersecurity Roles, view MLM-001-B Professional Roles in Cybersecurity.
Please give us your feedback on this MLM by clicking here.

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.

13

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,