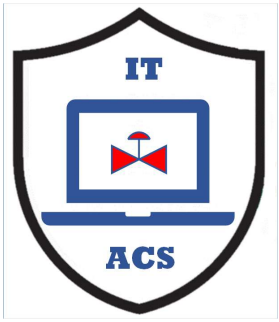
What is a Corporate Cybersecurity Program

MLM-013-A

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

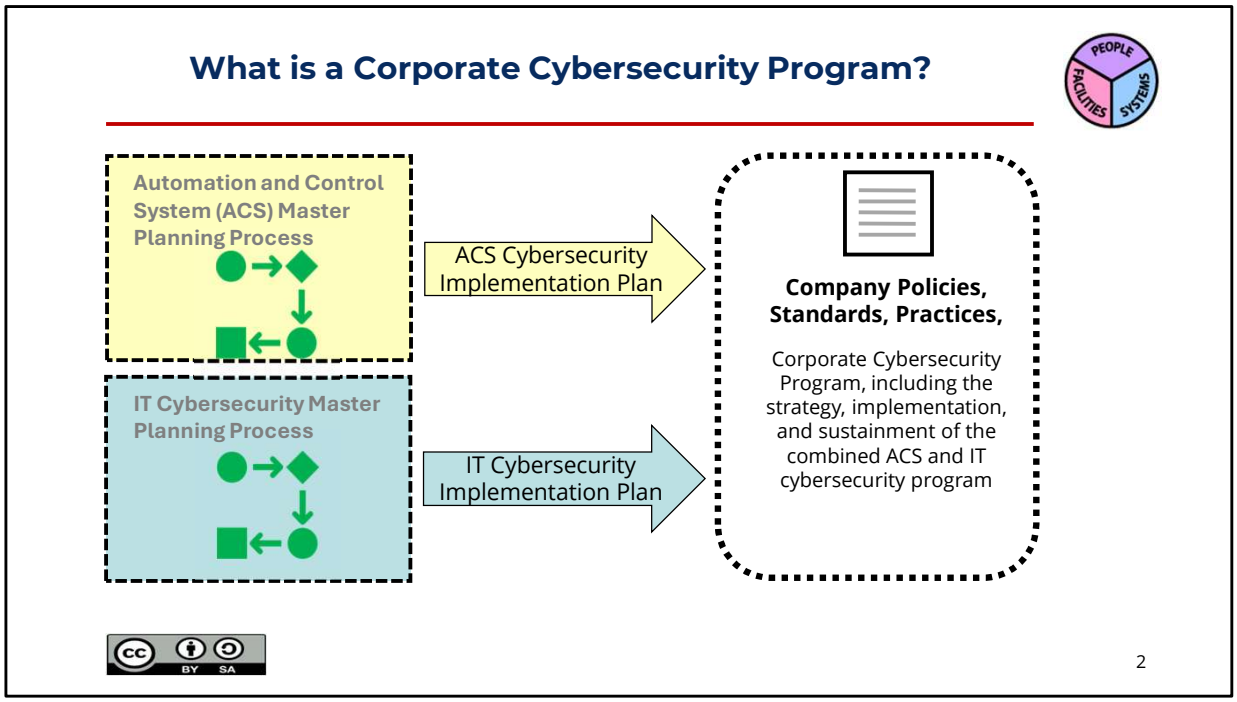


Turn on your audio and click start to begin video

START

This MLM describes the standards involved and the process involved in the creation of Cybersecurity Programs for Automation and Control Systems, and Information Technology (IT).

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

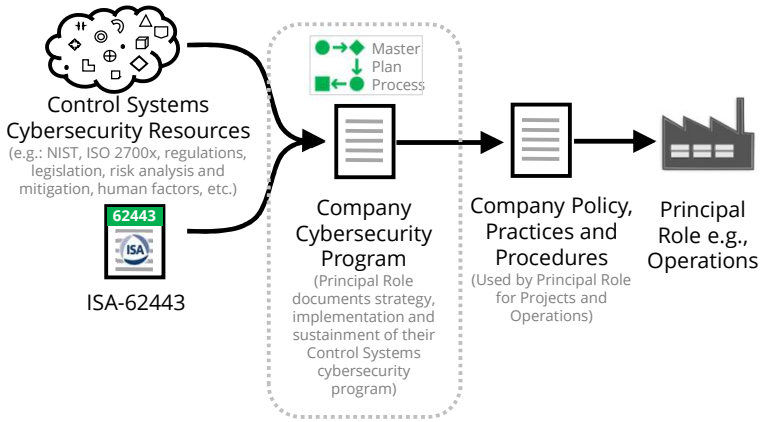


The ACS and IT Programs are combined to produce a Corporate Cybersecurity Program, and the policies and practices established therein are then applied to company projects and Operations.

An IACS Cybersecurity Program is a document that defines the company's policies, practices, and procedures associated with the operation of facilities and the design of projects.

It is developed by a "Principal Role" (e.g., an Owner Operator of a gas pipeline company). A formal PERA planning process is recommended to efficiently develop this IACS Cybersecurity Program.

How is an ACS Cybersecurity Program Used in your Enterprise



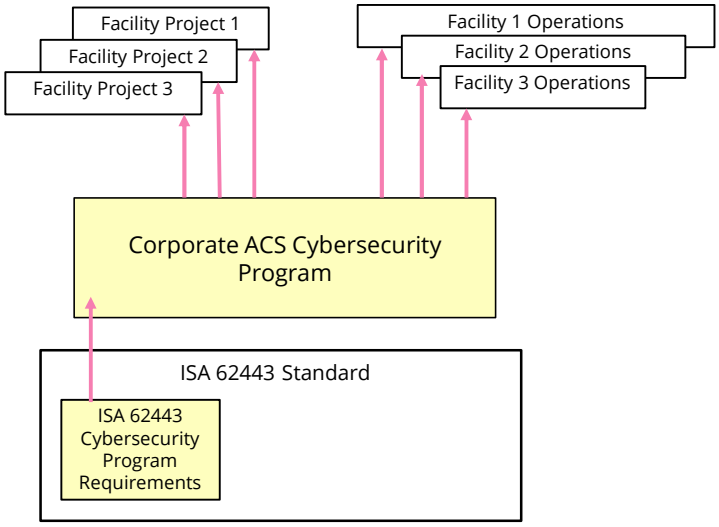
3

ISA 62443 is a "horizontal standard" designed to address a wide range of industries across all enterprise phases. As a result, any specific industry is likely to find that some "normative requirements" that are appropriate, for example, at an interstate pipeline, are not relevant for a pharmaceutical plant.
There are also obvious differences between a large-scale corporation with numerous sites and thousands of employees, and a small plant with a few dozen staff members.
Ultimately, each company must strike its own balance to effectively manage cybersecurity risks within its unique IT (Information Technology) environment, as well as OT (Operations Technology) measures and procedures, and other relevant organizational factors.

As a result, it is recommended that each company prepare its own ACS Cybersecurity Program, which retains requirements appropriate for them and may even expand some requirements specific to their industry. MLM-013-B "Preparing an ACS Cybersecurity Program" explains this process in more detail.

Once the ACS Cybersecurity Program is submitted and approved, the company's policies, practices, and procedures can be modified to address the requirements defined in the Cybersecurity Program. It may even be appropriate to define somewhat different procedures at different company facilities to address special requirements at that site.

Enterprise Owner's ACS Cybersecurity Program is Based on ISA/IEC 62443 Program Requirements



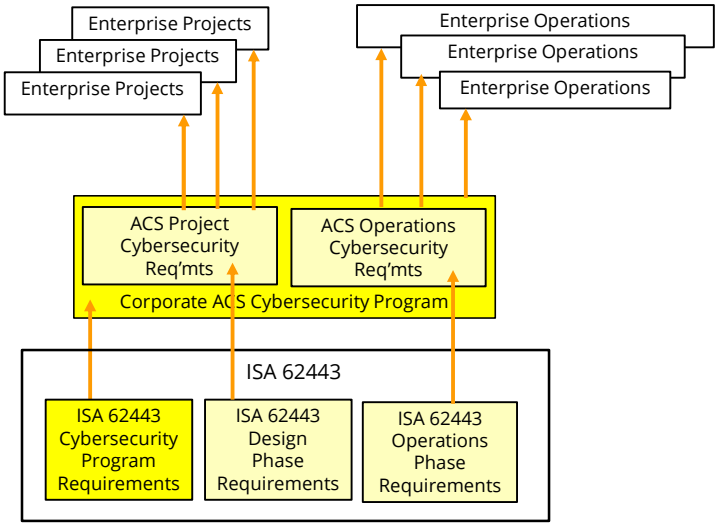
4

The *Corporate ACS Cybersecurity Program* defines *Requirements* for company projects that involve ACS, as well as Requirements for ACS in existing Facilities Operations.

The Corporate ACS Cybersecurity Program, in turn, receives its requirements from the ISA/IEC 62443 standard and other ACS standards discussed below.

The requirements in these standards may not be applicable or may even contradict each other; therefore, they must be reviewed, edited, and approved before being included in the Corporate ACS Cybersecurity Program.

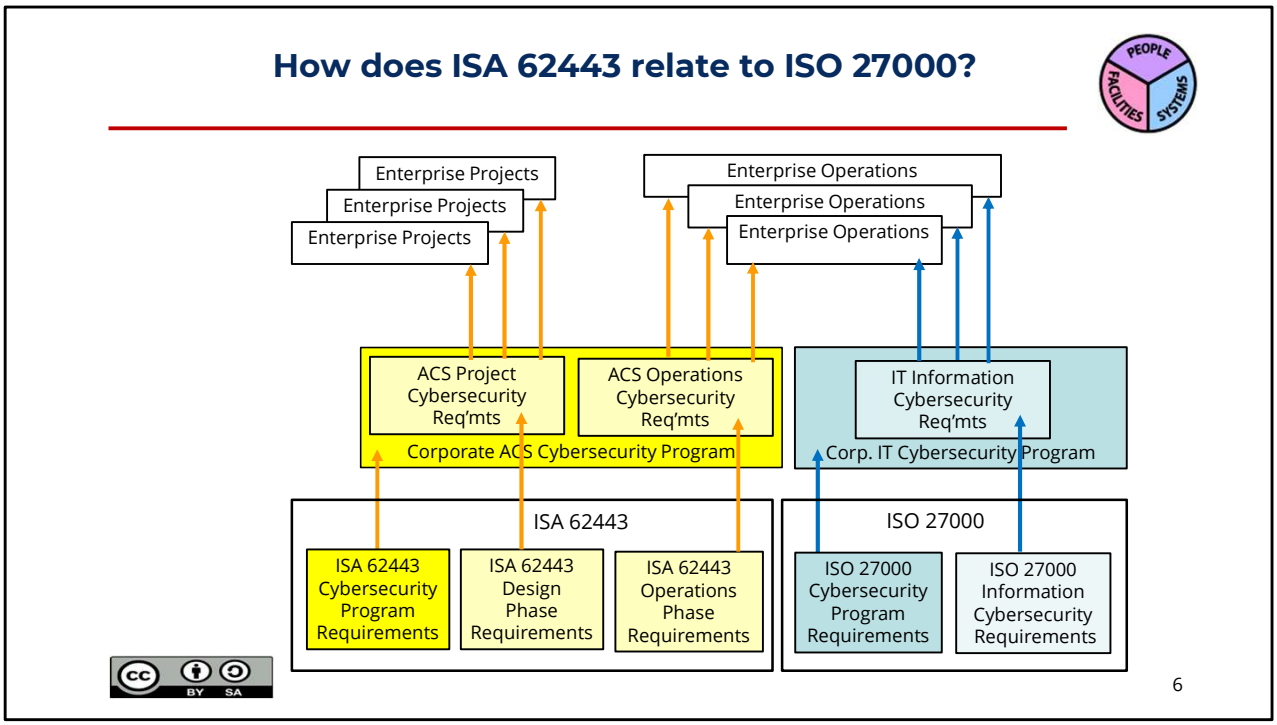
ACS Cybersecurity Program has General, Project, and Operations Requirements



5

The ACS Cybersecurity Program of a Corporation will contain "Program Requirements" for all Enterprise Phases of Corporate Facilities, including the Project Design Phase and Operations Phase. These may include procedural requirements, deliverables such as design documentation and drawings, and required measurements, including KPIs and incident reports.

These Requirements are similarly divided by Enterprise Phase in the 62443 standard.



ISA/IEC 62443 and ISO 27000 are in effect "parallel standards" as shown in this diagram. ISO 27000 addresses IT information security, while ISA/IEC 62443 addresses the cybersecurity of ACS.

However, ISA-62443 addresses parts of the enterprise where ISO 27000 cannot generally be applied, including:

- production areas with interlocks and regulatory control,
- Industrial equipment monitoring,
- safety systems in hazardous areas,
- sophisticated analyzers, and
- special purpose industrial networks.

The distinction between areas where ISA/IEC 62443 and ISO 27000 may be applied is indicated in the following "architecture diagram".

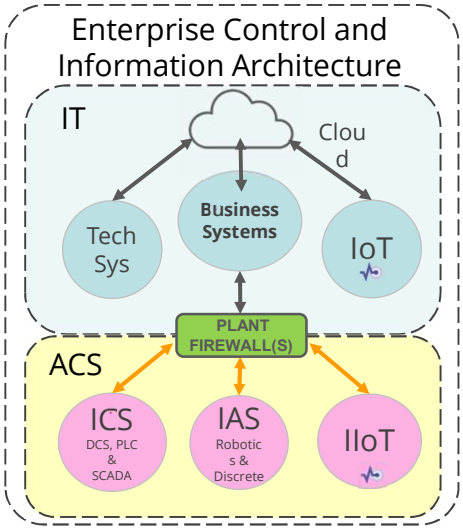
Example Enterprise Logical Architecture

Enterprise Control and Information Architectures may include:

Cloud Computing (Internal & Internet)
Business & Technical Systems

IoT (Internet of Things)

ICS (Industrial Control Systems)
IAS (Industrial Automation Systems)
IIoT (Industrial Internet of Things)



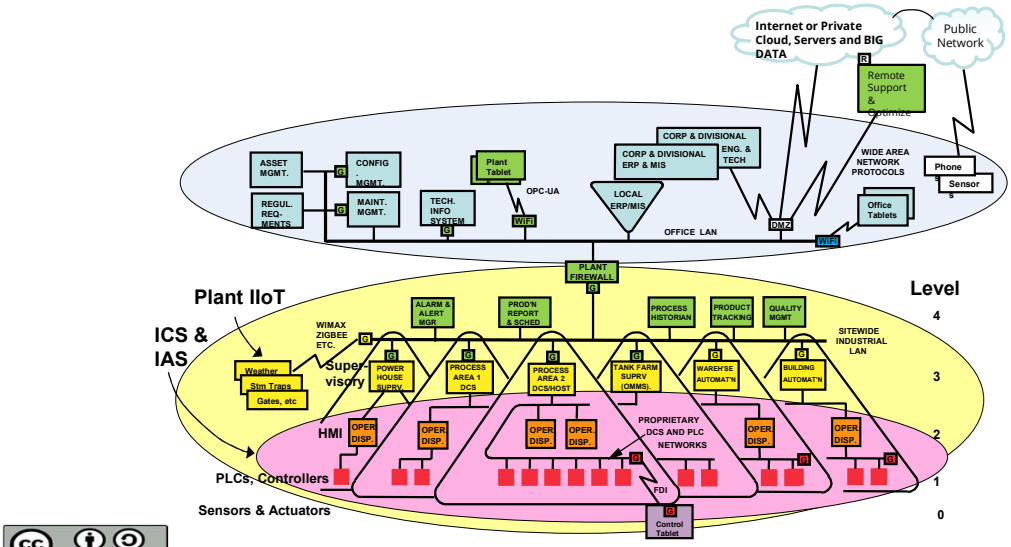
7

Enterprise Control & Information Systems typically consist of "IT systems" and "ACS"
IT Systems (blue area) consist of
- **Cloud Computing** and Internet – including internal and outsourced applications.
- **Business & Technical Systems** such as commercial, H/R, engineering, etc., including both IT and OT applications.
- **IoT** - Internet of Things Devices and Networks in **non-industrial** environments

ACS (yellow area) consisting of:
- **Industrial Control Systems** (ICS), including continuous and batch **DCS, PLC and SCADA** Control,
- **Industrial Automation Systems** (IAS), including **discrete manufacturing and robotics,** and,
- **Industrial Internet of Things (IIoT) Devices and Networks in industrial environments.**

The purpose of this set of Micro Learning Modules is to lay a foundation for understanding ACS Architectures. These MLMs will therefore focus on ACS, and leave IT systems and their Architectures to others.

Example
Process Plant Physical Systems Architecture

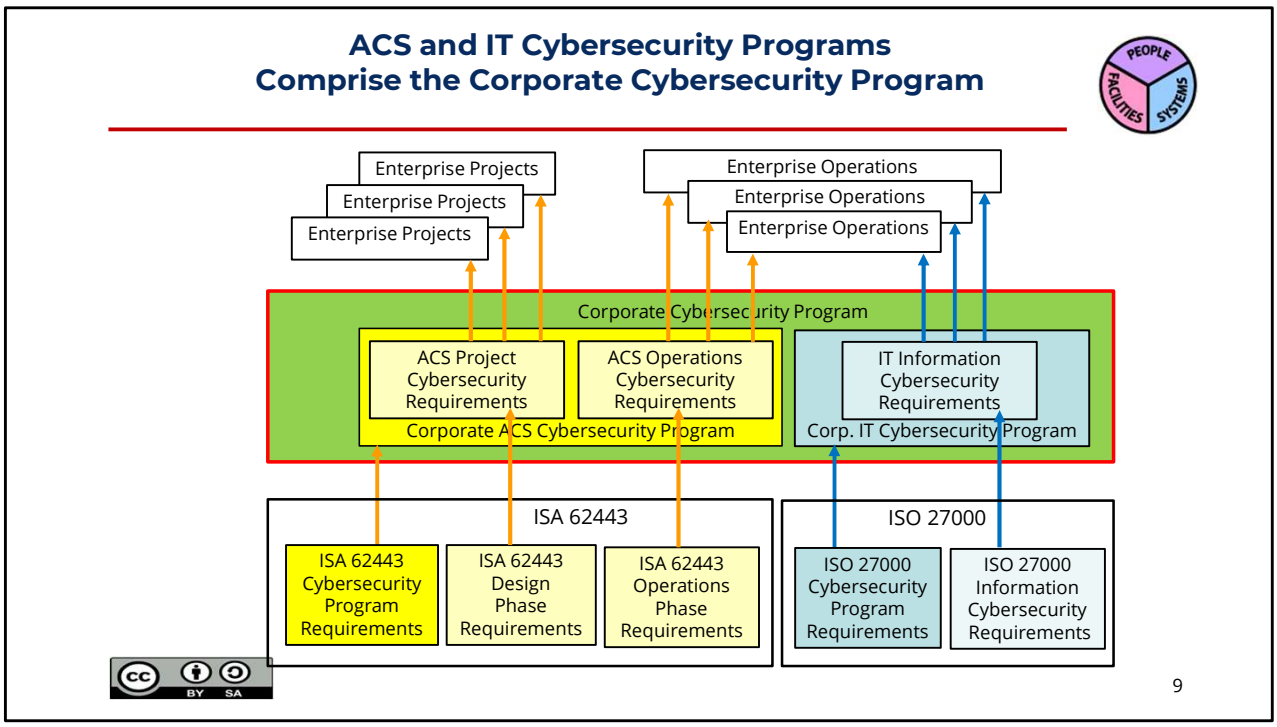


8

This Example demonstrates the application of concepts using the same "area" color coding as our earlier diagrams.

- Pink indicates Industrial Control (ICS) & Industrial Automation Systems (IAS) in Hazardous Areas
- Yellow indicates Supervisory & IIoT Systems in general-purpose industrial Environments. E.g., process & energy optimizers, Warehouse Automation, gates, cameras, etc.
- Green has been used to designate Manufacturing Execution Systems (MES) that "span" the Office Business LAN and the Site-wide Industrial LAN. Green was chosen as yellow + blue = green.
- Blue shows secured Ethernet and Wi-Fi Business Applications and LANs in Office Environments, and finally
- White indicates IoT devices and public networks, including Sensors, Tablets, Phones, GPS, etc.

The Architectural Levels shown in this diagram are described in more detail in a separate Micro Learning Module on "ACS Architectural Levels".
The ACS Architecture Levels (ranging from 1 to 4) in this "Process Plant Physical Architecture" are related to, but distinct from, Cybersecurity Zones. For more discussion of Cyber Security Zones, see MLM-006 "Cyber Security Levels and SPRs".

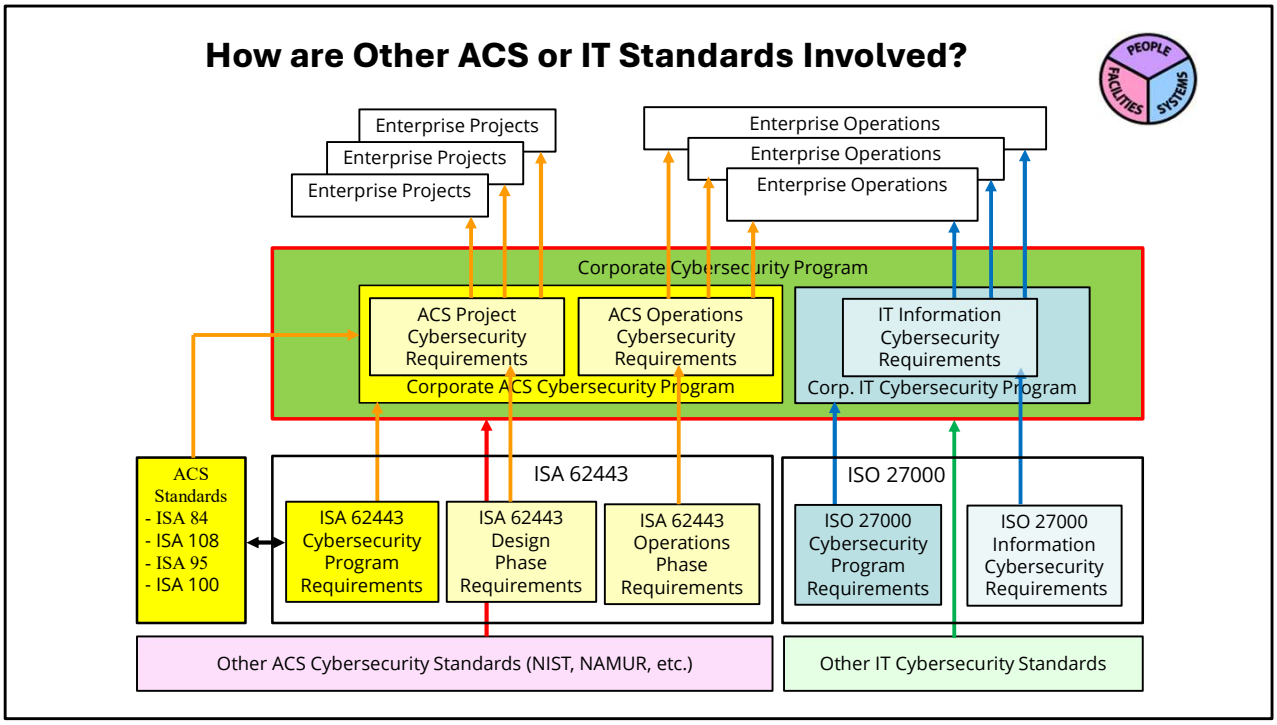


ISA/IEC 62443 and ISO 27000 are considered "parallel standards," as illustrated in the diagram. ISO 27000 addresses IT information security, while ISA/IEC 62443 addresses the cybersecurity of ACS.

However, ISA-62443 addresses parts of the enterprise where ISO 27000 cannot generally be applied, including:

- production areas with interlocks and regulatory control,
- Industrial equipment monitoring,
- safety systems in hazardous areas,
- sophisticated analyzers, and
- Special-purpose industrial networks.

The distinction between areas where ISA/IEC 62443 and ISO 27000 may be applied is indicated in the following "architecture diagram".



Although IEC/ISA 62443 and ISO 27000 are the two most important cybersecurity standards, other standards may also influence the Corporate Cybersecurity Program. These include other ACS Standards such as:

ISA84 - Safety Instrumented Systems to reduce risks such as fire and explosions

ISA108 – Intelligent Device Management for plant equipment, such as software-configured instrumentation

ISA95 – Enterprise Integration, including transfer of information between plant instrumentation and corporate information systems.

ISA100 – Industrial Local Area Network design, configuration, and operation.

These standards are coordinated within ISA to improve the cybersecurity of ACS devices and networks

Other Standards may have an influence on ACS cybersecurity, such as

- NIST
- NAMUR

However, if they are required, the integration of these standards must be coordinated with the requirements of IEC/ISA 62443.

Similarly, other IT Cybersecurity Standards may influence the Corporate IT Cybersecurity Program. However, most companies already have a Corporate IT Cybersecurity Program, so development of this will not be examined further in this MLM.

Key "Take-away" Messages

- The Corporate ACS Cybersecurity program and the Corporate IT Cybersecurity Program are complementary parts of the overall Corporate Cybersecurity Program.
- The ACS Cybersecurity Program selects which standards and requirements are to be used in company facilities and projects, and reconciles conflicts between them.
- Once standards are selected and reconciled, the versions of these standards that were used are specified, but no further reference to these standards is required.
- The ACS Cybersecurity Master Plan should be reviewed on a planned schedule (e.g. each 5 years) when new or updated standards may be added.

11

The Corporate ACS Cybersecurity program and the Corporate IT Cybersecurity Program are complementary parts of the overall Corporate Cybersecurity Program.

The ACS Cybersecurity Program selects the standards and requirements to be used in company facilities and projects and reconciles any conflicts between them.

Once standards are selected and reconciled, the versions used are specified, but no further reference to these standards is required.

The ACS Cybersecurity Master Plan should be reviewed on a planned schedule (e.g., every 5 years) to incorporate new or updated standards.

Key “Take-away” Messages

- The IEC/ISA 62443 standard provides input to
  - Corporate ACS Cybersecurity policies, standards, and practices.
    - which in turn, provides input to
      - Project or Facility ACS Cybersecurity practices.
- IEC/ISA 62443 is coordinated with other ISA control and network standards which avoids conflicts with existing project or facility operations.
- An ACS Cybersecurity Program typically begins with an “As-Is” Audit and a “To-Be” Master Plan.

12

The IEC/ISA 62443 standard provides input to
- Corporate ACS Cybersecurity policies, standards, and practices.
  - which in turn, provides input to
    - Project or Facility ACS Cybersecurity practices.

IEC/ISA 62443 is coordinated with other ISA control and network standards which avoids conflicts with existing project or facility operations.

An ACS Cybersecurity Program typically begins with an “As-Is” Audit and a “To-Be” Master Plan.

More Reading

Related MLMs:

- MLM-003-A Enterprise Lifecycles and Phases.
- MLM-013-B Cybersecurity Program Implementation.
- MLM-013-C Sustaining a Cybersecurity Program

References

- ISA Global Cybersecurity Alliance White Paper
  "Applying ISO/IEC 27001, ISO/IEC 27002 and the ISA/IEC 62443 Series for Operational Technology Environments"

:

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.