Regional Training Program on Cybersecurity

South Asia Regional Energy Partnership (SAREP)

Session Cyber Security Standards
Speaker Shiv Kataria
Siemens

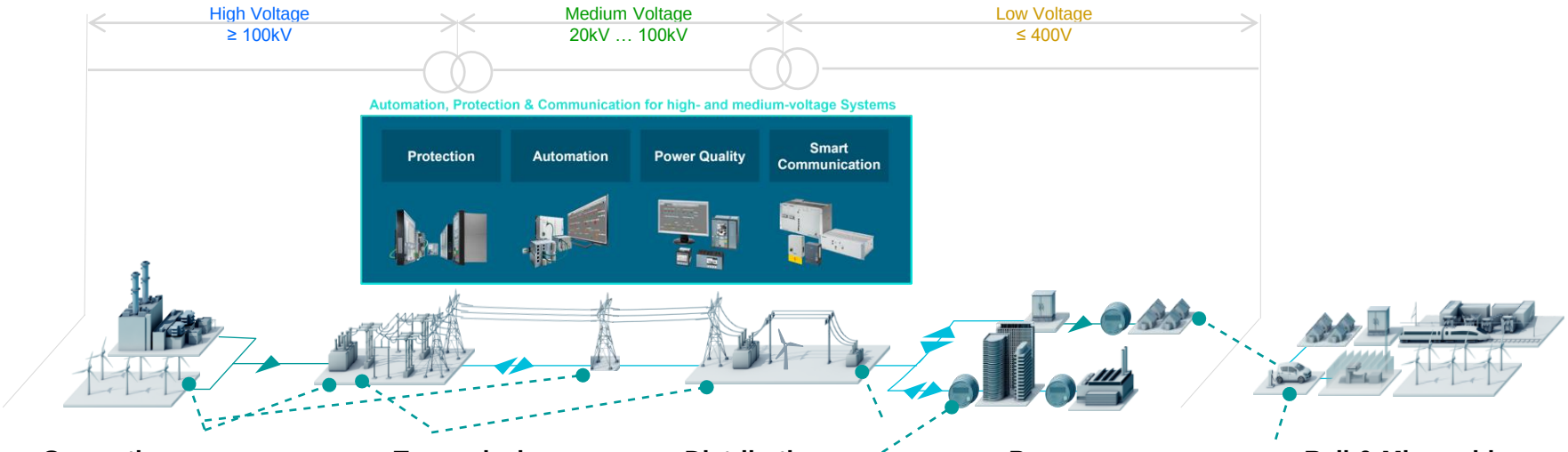
What we learn today?

- ISO 2700X
- Detailed IEC62443 Journey
- IEC 62443-4-1 Security Standard for secure development of IACS
- NIST Guidelines for OT

Why do we need a Standard or Guideline?

- **Enhanced Security Posture**: Implementing standards reduces the risk of breaches and prepares businesses with effective incident response and business continuity plans.
- **Reputation and Trust**: Compliance demonstrates to clients, stakeholders, and partners that a business prioritizes cybersecurity and data protection, fostering trust.
- **Business Opportunities**: Meeting these standards often opens up new business opportunities and qualifies businesses for certain contracts that require strict compliance.
- **Insurance Benefits**: Compliance can lower cyber insurance premiums by evidencing proactive cybersecurity efforts.
- **Structured Cybersecurity Strategy**: Standards provide a structured approach to cybersecurity, helping businesses organize and prioritize their security measures effectively.
- **Cost Efficiency**: Standards help identify specific security needs, reducing wasted expenditure on unnecessary or irrelevant cybersecurity solutions.
- **Investment Justification**: Adhering to a recognized framework ensures that any investments in cybersecurity are likely to deliver measurable and beneficial outcomes.

Value chain in Power Grid and Automation Use cases



Generation

- Power Quality Monitoring
- Network Optimization

Transmission

- Substation Automation
- Inter Control Center Communication
- Remote Maintenance and Service

Distribution

- DER Integration (Metering & Control)
- Remote Services

Prosumer
Consumer / Producer

- Connecting Electric Vehicles to the Charging Infrastructure

Rail & Microgrids

Standards and Regulations

Regulative/Guidelines

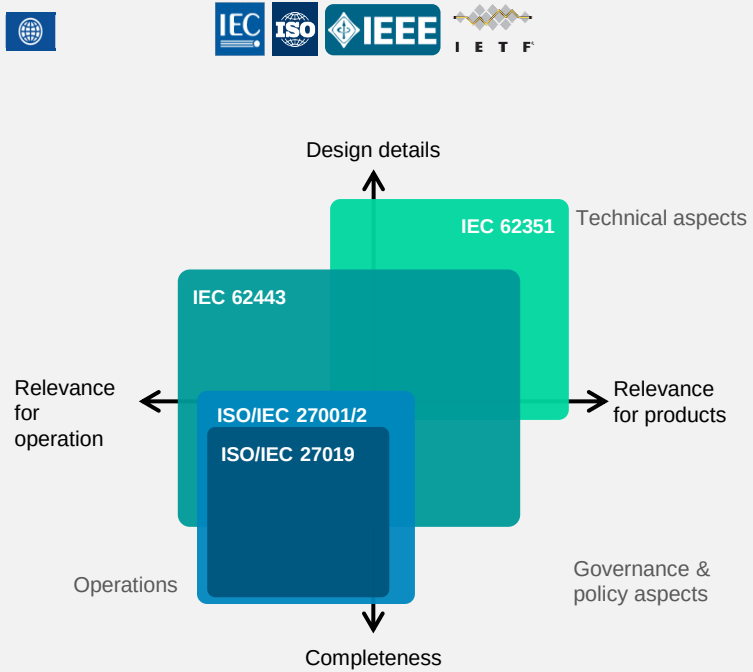
- Critical Infrastructure Protection (NERC CIP)
- Executive Order 13636: Improving Critical Infrastructure Cybersecurity
- Executive Order 14028: Improving Nation's Cyber Security
- NIST 800-82
- NIST 1800-32

- IT Security Act
- B3S Standards for dedicated critical infrastructure domain
- BNetzA Security Catalogue
- German Energy Act

- Cyber Security Act (EU-CSA)
- Network Information Security Directive (NIS2)
- RED Delegated Act
- Cyber Resilience Act (EU-CRA)

- NCIIPC Guidelines
- CEA Guidelines
- QCI/NCIIPC framework
- Sectoral CERTs

International Standards



ISO 270XX

ISO/IEC 27OXX Series

ISMS Family of standards

Vocabulary standard	**27000** Overview and vocabulary	
Requirement standards	**27001** **ISMS – Requirements** 	**27006** Requirements for bodies providing audit and certification of ISMS
Guideline standards	**27002** Code of practice for information security controls	**27005** Information security risk management
	27003 ISMS – Implementation guidance	**27007** Guideline for ISMS auditing
	27004 ISMS – Measurement	
Sector-specific guideline Standard (exmples)	**27017** Code of practice for information security controls based on ISO/IEC 27002 for cloud services	**27019** ISMS – Guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

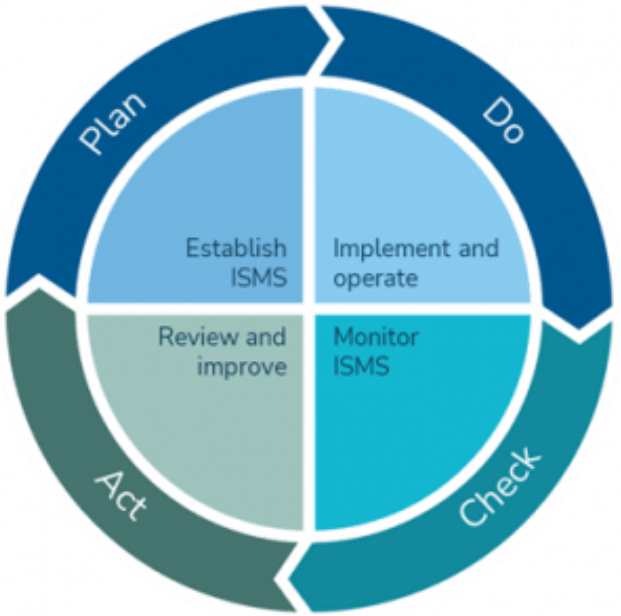
Addresses specifically

- Security Policies
- Organization and info. security
- Human Resource Security
- Asset Management
- Access Control
- Cryptography
- Physical and Environ. Security
- Operations Security
- Communications Security
- System and Application
- Supplier Relationship
- Incident Management
- Business Continuity
- Compliance

Domain specific standards augment ISO 27002 according to the target environment

ISO 270XX

Dealing specifically in information security, the ISO-27001 standard enables organizations to address and prioritize their confidentiality, integrity, and availability requirements. At its heart is a plan-do-check-act cycle, normally referred to as the PDCA cycle, which traces its roots from quality assurance in production environments.



ISO/IEC 27019 Series

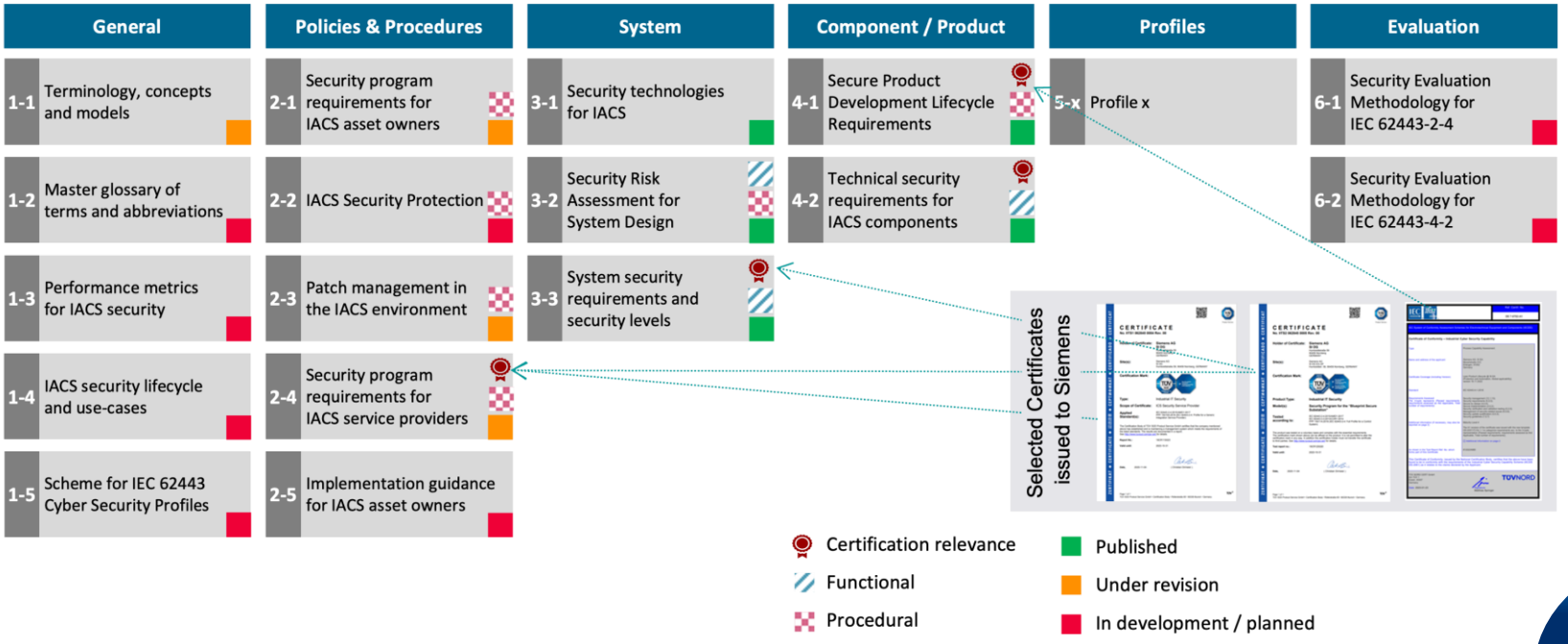
Application of ISO/IEC 27002:2013 to process control systems used by the energy utility industry for controlling and monitoring the production or generation, transmission, storage and distribution of electric power, gas, oil and heat, and for the control of associated supporting processes. This includes in particular the following:

- Central and distributed process control, monitoring and automation technology as well as information systems used for their operation, such as programming and parameterization devices;
- Digital controllers and automation components such as control and field devices or Programmable Logic Controllers (PLCs), including digital sensor and actuator elements;
- all further supporting information systems used in the process control domain, e.g. for supplementary data visualization tasks and for controlling, monitoring, data archiving, historian logging, reporting and documentation purposes;
- communication technology used in the process control domain, e.g. networks, telemetry, telecontrol applications and remote control technology;
- Advanced Metering Infrastructure (AMI) components, e.g. smart meters;
- measurement devices, e.g. for emission values;
- digital protection and safety systems, e.g. protection relays, safety PLCs, emergency governor mechanisms;
- energy management systems, e.g. of Distributed Energy Resources (DER), electric charging infrastructures, in private households, residential buildings or industrial customer installations;
- distributed components of smart grid environments, e.g. in energy grids, in private households, residential buildings or industrial customer installations;
- all software, firmware and applications installed on above-mentioned systems, e.g. DMS (Distribution Management System) applications or OMS (Outage Management System);
- any premises housing the above-mentioned equipment and systems;
- remote maintenance systems for above-mentioned systems.

IEC/ISA 62443

IEC 62443 – Security for Industrial Automation and Control Systems

Targets operator, integrator, and product supplier in terms of processes and security capabilities and allows for certification



How to make a Cybersecurity Management System (CSMS)IEC 62443 based security Approach

3-dimensional approach

People

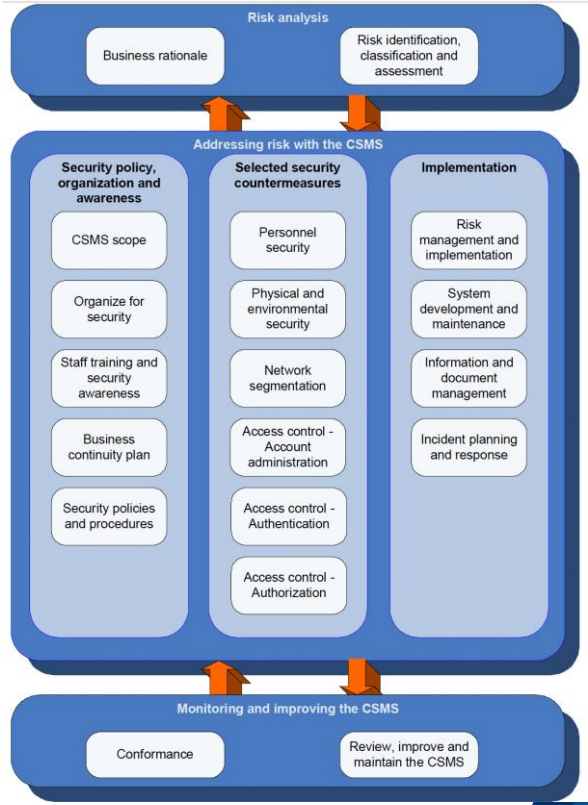
Evaluate the awareness and cybersecurity understanding of your people involved in production

Process

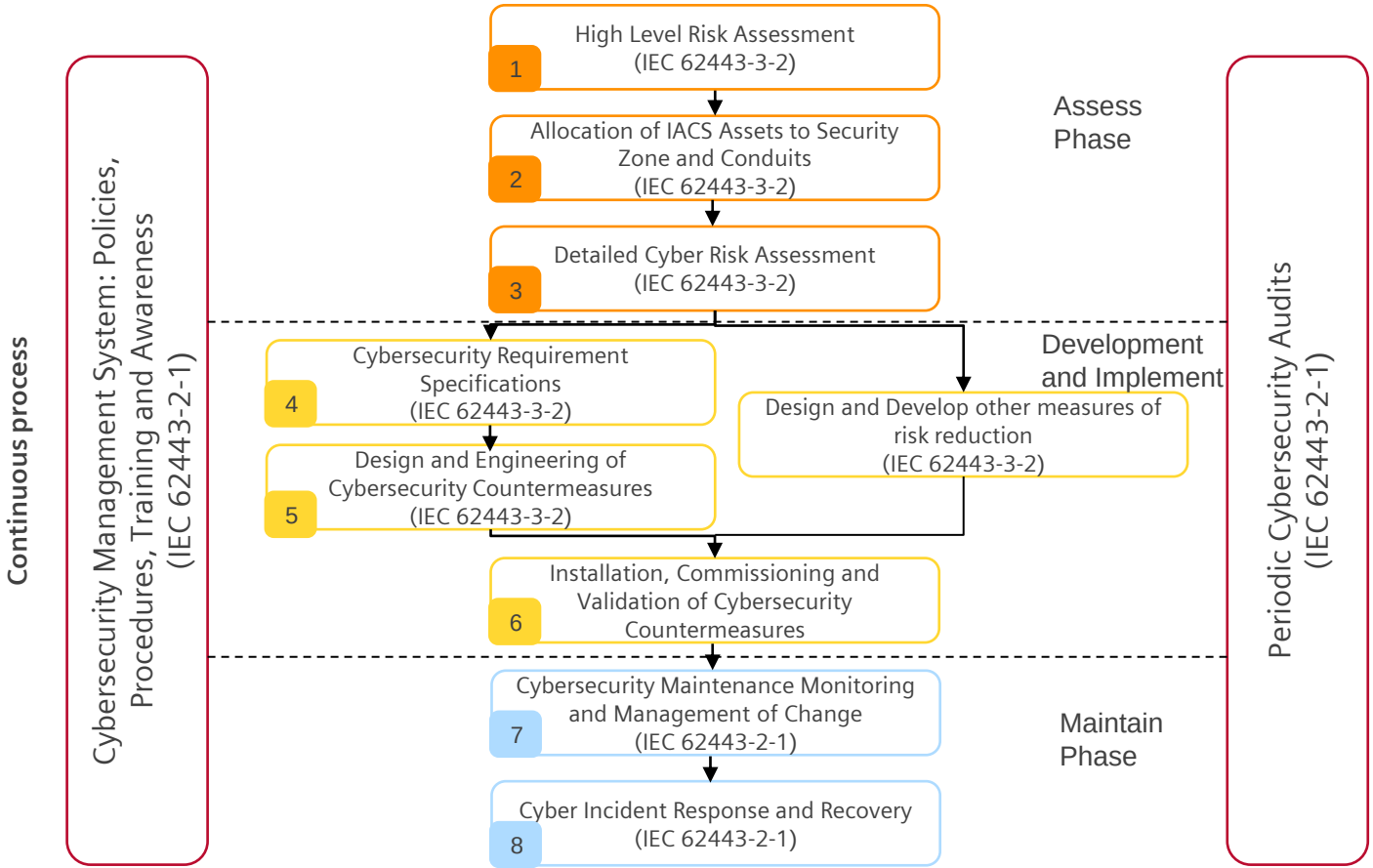
Assess the maturity of organizational processes and work instructions towards Cybersecurity Risk Mitigation

Technology

Evaluate your installed base and System Architecture to find gaps against IEC 62443 Standard



IACS Cybersecurity Lifecycle



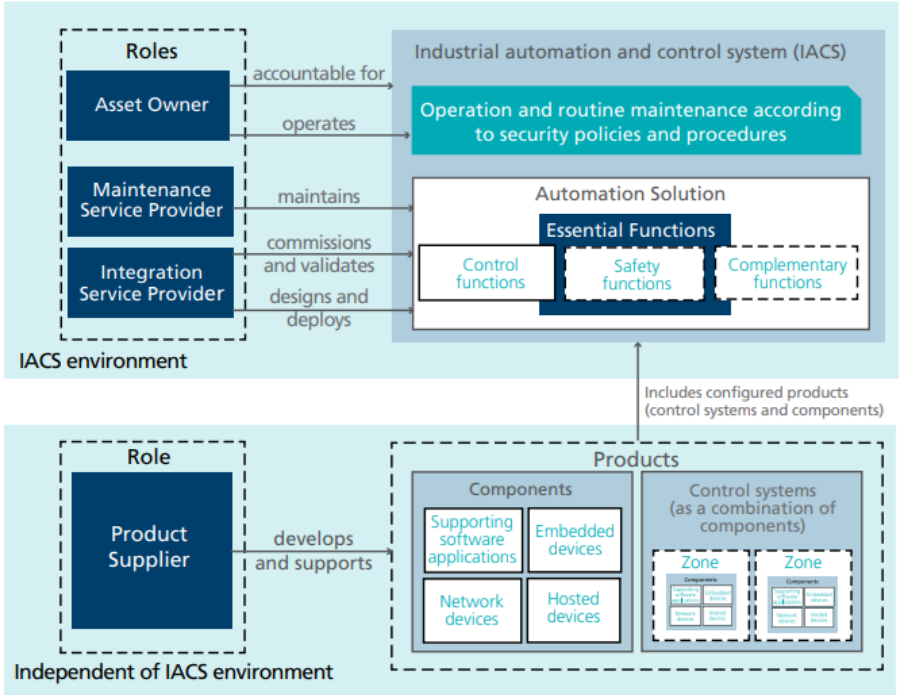
Roles, Products, Automation Solution and IACS

1. Asset Owner:
Establishes security objectives and policies, and bears the primary responsibility for securing IACS.

2. Maintenance Providers:
Ensures system resilience and integrity through regular upkeep and prompt incident responses.

3. Automation Solution Providers:
Designs and implements secure automation solutions, integrating security considerations throughout system development.

4. Original Equipment Manufacturers (OEMs):
Focuses on manufacturing equipment that aligns with specified security standards and resilient designs.



Security Levels | IEC62443

Security Levels		
4	Protection against intentional violation using sophisticated means with extended resources, system specific skills and high motivation	Groups/Nation-states, governmental organization members ..
3	Protection against intentional violation using sophisticated means with moderate resources, system specific skills and moderate motivation	Cybercrime player, Terrorists, hacktivists, professional thieves, Cyber-criminals, Competitors
2	Protection against intentional violation using simple means with low resources, generic skills and low motivation	Insider or Intruder (Thrill-seeking, hobbyists, malicious organization..)
1	Protection against casual or coincidental violation	Insider (Careless employees/contractors)

Maturity Levels | IEC62443

Security Levels are a measure of the strength of technical requirements, **Maturity Levels** are a measure of processes (people, policies, and procedures).

Parts 2-1, 2-2, 2-4, and 4-1 use Maturity Levels to measure how thoroughly requirements are met.

Maturity Model is based on the Capability Maturity Model Integration (CMMI), with Levels 4&5 combined into Level 4.

Level	CMMI	62443	Description
1	Initial	Initial	• Product development typically ad-hoc and often undocumented • Consistency and repeatability may not be possible
2	Managed	Managed	• Product development managed using written policies • Personnel have expertise and are trained to follow procedures • Processes are defined but some may not be in practice
3	Defined	Defined (Practiced)	• All processes are repeatable across the organization • All processes are in practice with documented evidence
4	Quantitively Managed	Improving	• CMMI Levels 4 and 5 are combined • Process metrics are used control effectiveness and performance
5	Optimizing		• Continuous improvement

Risk equation and basics

Risk = (Threat x Vulnerability) x Consequence.

Likelihood

Scenario: Power plant's control system software has a known vulnerability that hasn't been patched yet. An adversary group known for targeting energy infrastructures (the threat) has just released a new form of malware that can exploit this exact vulnerability.

Risk Components:

Threat: The adversary group with its new malware (High threat)

Vulnerability: The unpatched software in the control system (High)

Consequence: A successful attack could disrupt the power supply to a large area causing significant impact on homes, businesses, and critical infrastructures like hospitals (High).

Likelihood: The likelihood of an attack is also high due to the known active threat combined with the unpatched vulnerability.

Risk (Likelihood x Consequence) is high due to the high likelihood and severe consequences.

Foundational Requirements:

FR-1	Identification and Authentication Control	A requirement for identifying and authenticating users to prevent unauthorized access.
FR-2	Use Control	A requirement for controlling the use of system capabilities once a user has been authenticated.
FR-3	System Integrity	A requirement for maintaining the integrity of IACS data and functions.
FR-4	Data Confidentiality	A requirement for protecting the confidentiality of sensitive IACS data.
FR-5	Restricted Data Flow	A requirement for controlling the flow of data through the IACS, including into, out of, and within the system.
FR-6	Timely Response to Events	A requirement for detecting, reporting, and responding to security events in a timely manner.
FR-7	Resource Availability	A requirement for ensuring the availability of IACS resources, including functions, data, and equipment.

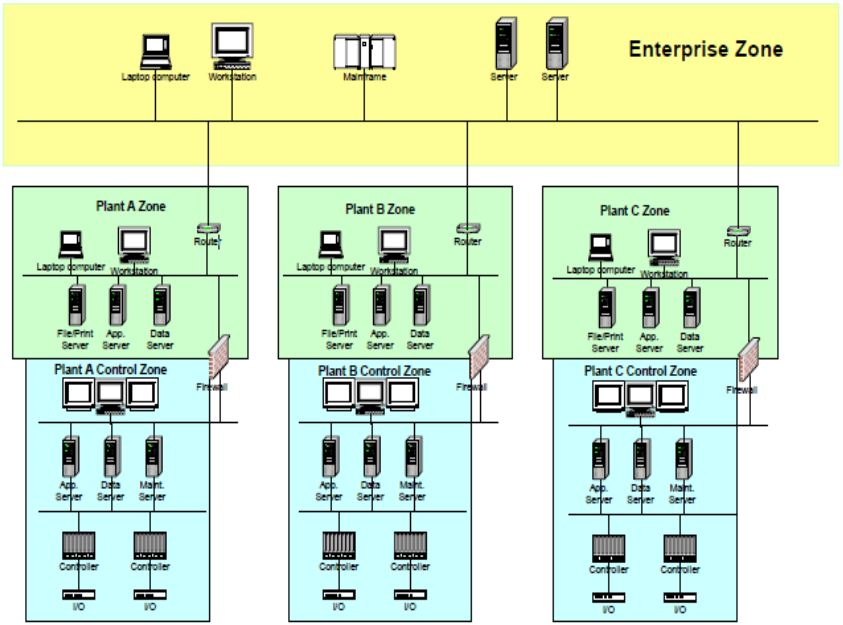
Security Zone and Conduits

- Zone is a logical grouping of physical, informational, and application assets sharing common security requirements.
- Zones represent logical divisions within an ICS network, typically based on functionality, purpose, or security requirements.
- Zones are created to facilitate network segmentation and enforce security policies specific to each zone.
- Each zone typically represents a distinct area or level of trust within the ICS environment.
- Examples of common zones in ICS environments include the manufacturing zone, control zone, enterprise zone, and DMZ (Demilitarized Zone).
- Zones help to segregate critical systems from less critical systems, limit access to sensitive information, and prevent the lateral movement of threats within the network.

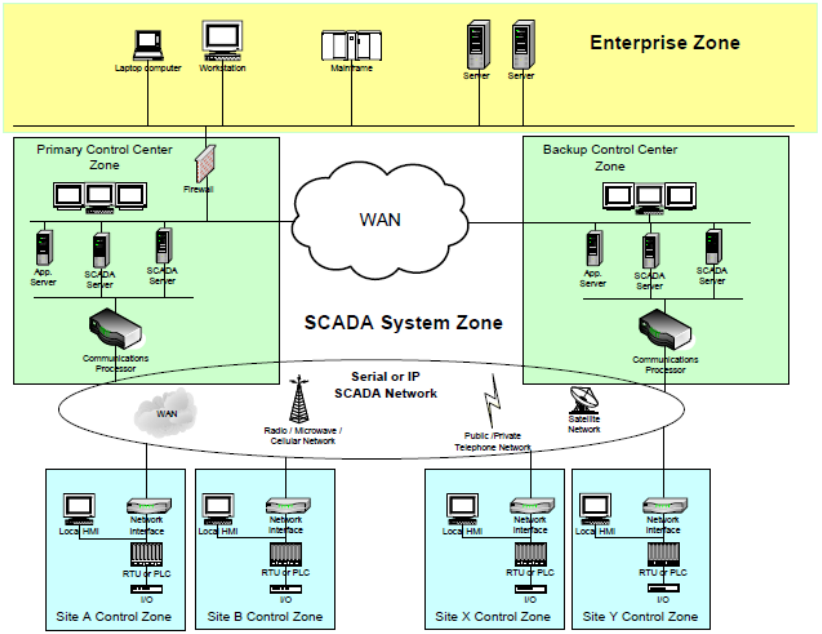
Conduits

- Conduit is a logical grouping of communication assets that protects the security of the channels it contains.
- Conduits serve as controlled paths or connections between different zones, enabling communication while maintaining security boundaries.
- Conduits can be thought of as “pipes” that connect zones or that are used for communication within a zone.
- Conduit is the wiring, routers, switches, and network management devices that make up the communications under study.
- Conduits are used to analyze the communication threats and vulnerabilities that can exist in the communications within and between zones.

Zones and Conduit Models

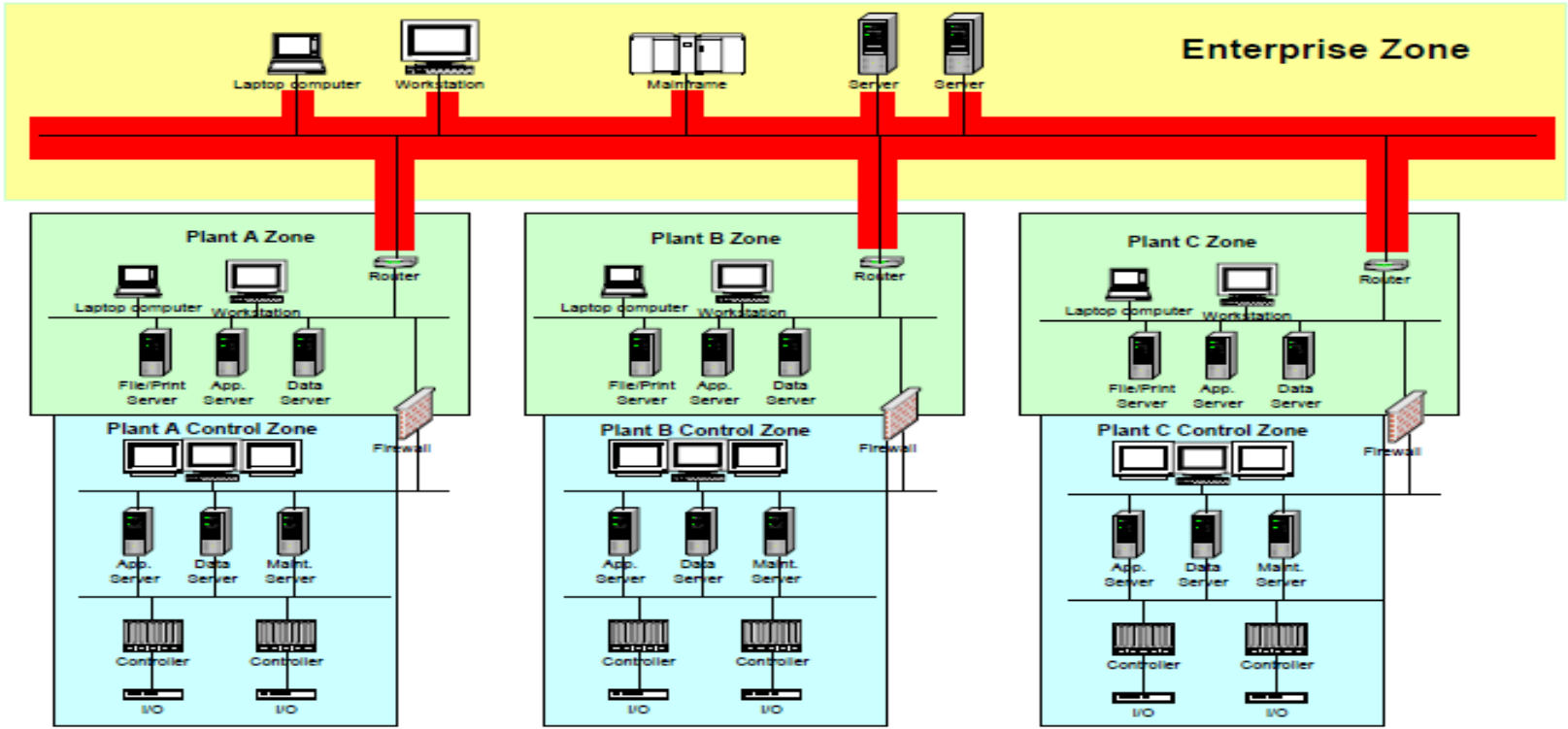


Separate Zones Example

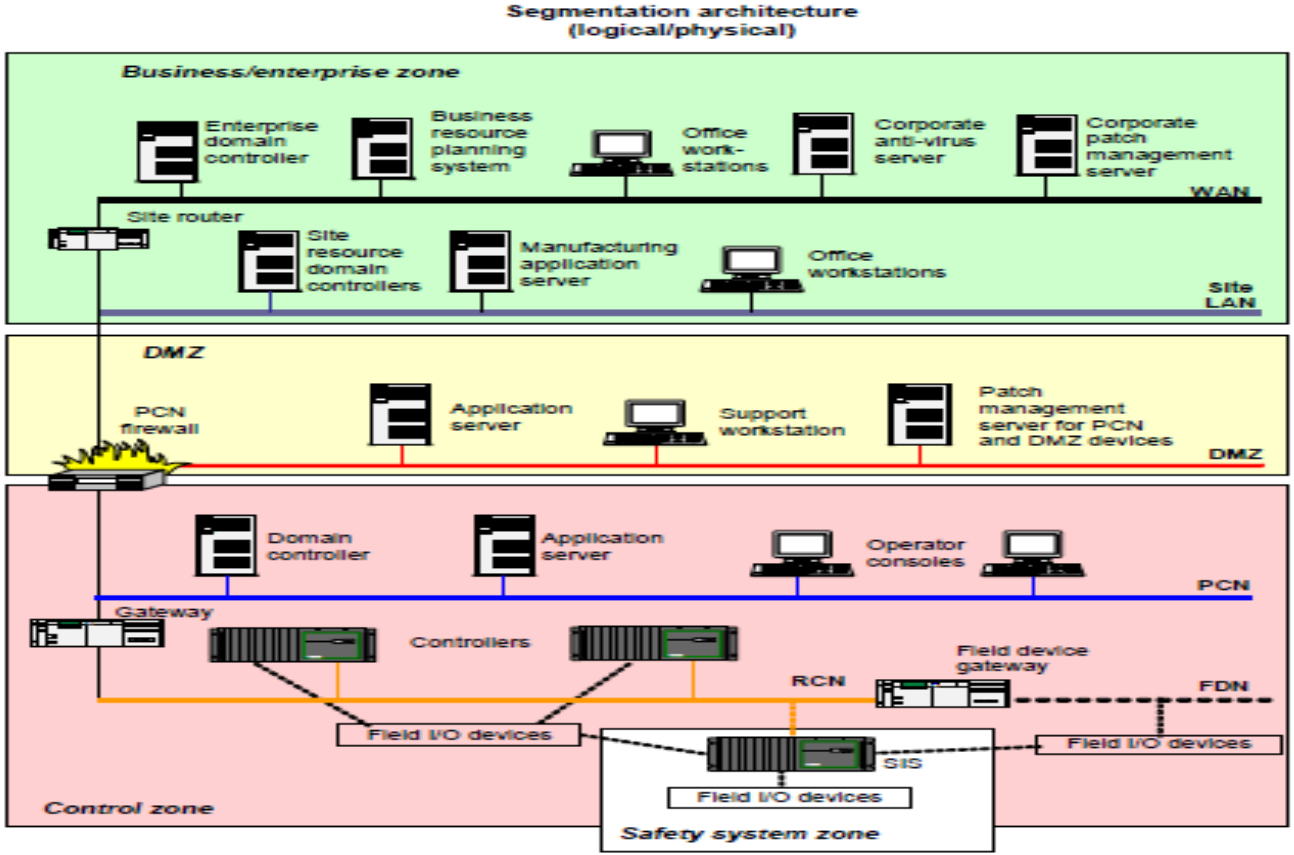


SCADA Separate Zones Example

Enterprises Models



Enterprises Models



- Control Zone
- DMZ
- Safety System Zone
- Enterprise Zone

IEC 62443-2-3: Patch Management

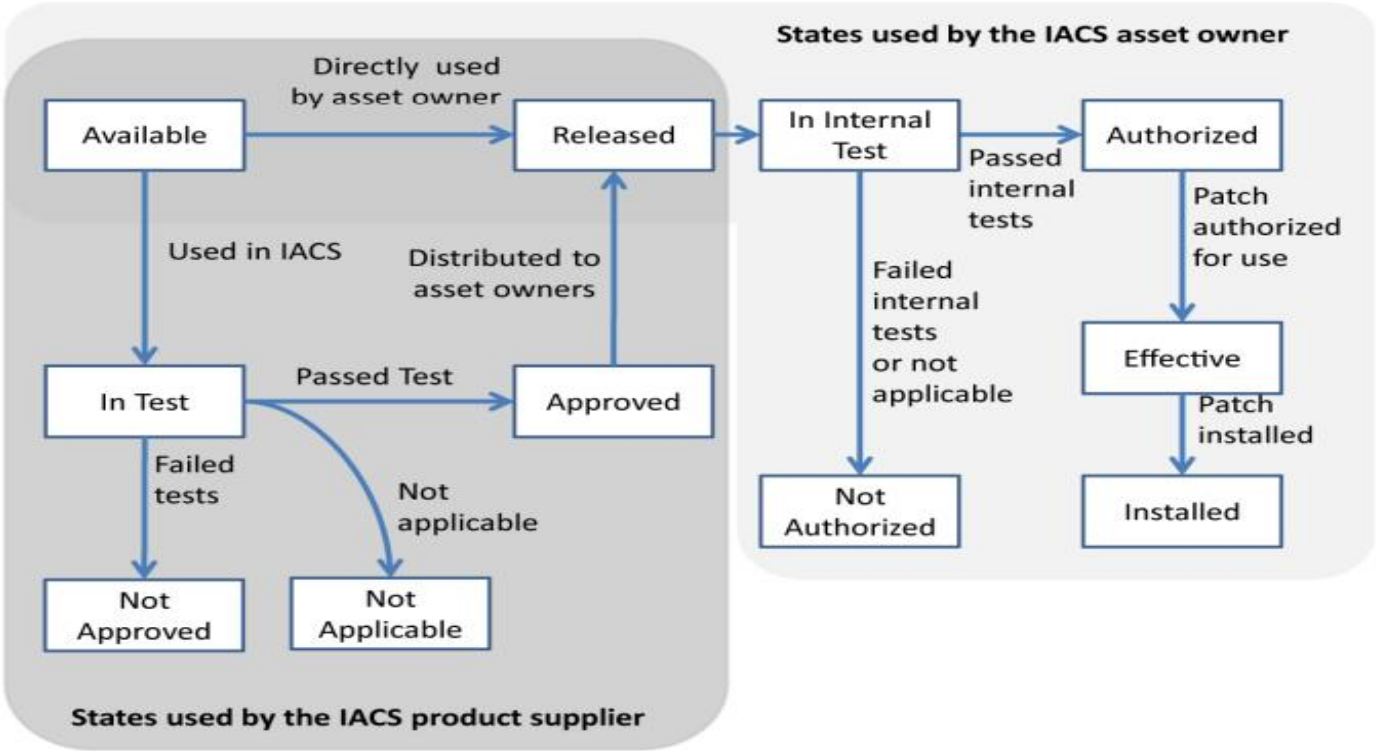
Patch - incremental software change in order to address a security vulnerability, a bug, reliability or operability issue (update) or add a new feature (upgrade).

Patches also called as:

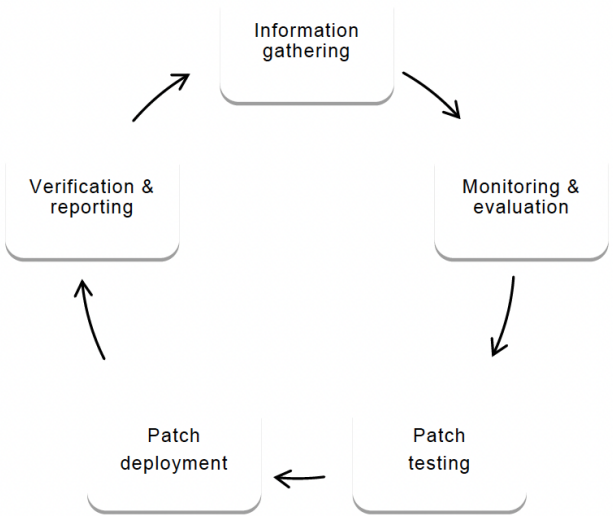
- Software updates
- Software upgrades
- Firmware upgrades
- Service packs, hotfixes, basic input output system (BIOS) updates
- Security advisories and other digital electronic program updates

Patch Management is set of processes for monitoring patch releases, determining their installation on systems, testing necessity, installation timing, and tracking successful setup.

IACS Patch Management



Patch Management Workflow and RACI



Patch Management workflow

Process Control Network Security Management Activity or Responsibility / Subject Area	VP, Generation	Generation Support	Generation Support (team)	Vendor Relations	John Doe	Managing Directors	Site Security Leads	Engineering Support (per Site)	I&C Supervisor	Generation Compliance Office	Central Testing Group	Company Compliance Office	Hardware/ Software Vendors	Contract Technical Labor	New Hire, Administrative Labor	IT Support Manager	IT Security, Manager	Corporate Security	
	PE	PE	PE	PE	PE	PE	PE	PE	PE	PE	PE					IT	IT	IT	I
CIP-007 - R3 (Security Patch Management) and CIP-007 - R4 (Malicious Software Prevention)																			
Security Patch Management																			
IT Security Alert Monitoring (Microsoft, CERT, NERC)		I														A	R		
Existing Monitoring Activities (Hydro, Trans, IT… looking at Emerson, ABB…)		I														R			
Ongoing monitoring of patch websites (all vendors)		A	R	R						I			C			S			
Downloading and Organizing Patch Files		A	R										C						
Establishing SLAs/Contracts for Vendors	A	R				R							S						
Patch Evaluation: Part A (general)		A	R				I										C	S	
Patch Evaluation: Part B (site-specific)		I	S			A	R	R	S	V		I	C						
Provision Equipment for Testing (Central)	A	R	S	S	S								C						
Patch Acceptance Testing (Central)		A	R										C			S			
Patch Acceptance Testing (Site)				S	S	A	R	R	S				C						
Provision Equipment for Testing (Site)		I	S	S	S	A		R	S				C						
Patch Deployment and Verification		I	S	S	S	A	I	R	R				C						
Detailed Inventory Tracking (CCA Lists, Firmware, OS, Versions, Patches etc.)'		I	S			A	R	S	S	V			S				I		
Generate Deployment Reports		I				A	R	S	S	V		I							

IEC

Responsibility Chart Sample

Some recommendations

- ✓ Maintain an inventory of all 'updatable' electronic devices linked with the IACS
- ✓ Keep accurate records of each device's 'installed' version.
- ✓ Regularly check available 'latest' upgrades and updates for each device
- ✓ Determine 'released versions' of updates compatible with their standards on a set schedule
- ✓ Test IACS patch installations in a production-like environment to authorize them
- ✓ Schedule installation of 'authorized' patches considering system design and operational needs
- ✓ Regularly update records (at least quarterly) about different versions for each updatable device

Risk Assessment

Risk Assessment is the process of identifying, analyzing, and evaluating the risks associated with potential threats and vulnerabilities in the OT ICS environment.

ISA/IEC62443 definition:
Risk Assessment is a process that systematically identifies potential vulnerabilities to valuable system resources and threats to those resources, quantifies loss exposures and consequences based on probability of occurrence, and (optionally) recommends how to allocate resources to countermeasures to minimize total exposure.

Risk assessments are often combined with vulnerability assessments to identify vulnerabilities and quantify the associated risk. They are carried out initially and periodically to reflect changes in the organization's risk tolerance, vulnerabilities, procedures, personnel and technological changes.

Risk Assessment | IEC 62443

Purpose of Cyber Risk Assessment:

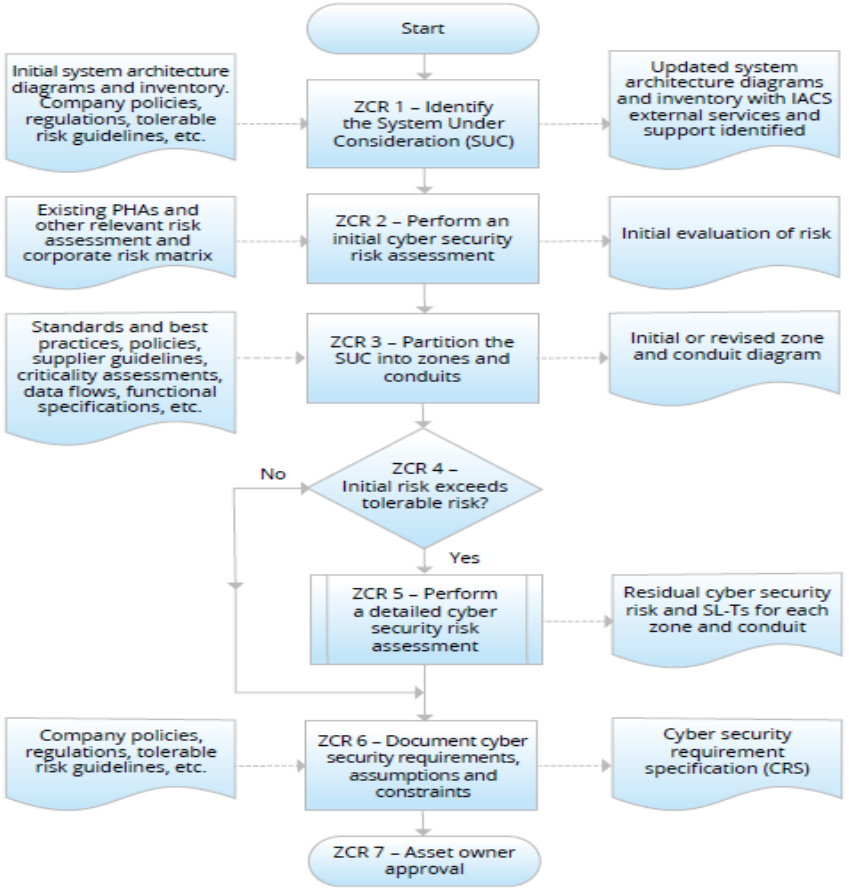
- Evaluate the likelihood and consequences
- Prioritize the risk.
- Determine necessary measures to reduce risks
- Align with tolerable risk levels set by the asset owner.

It provides general requirements and is not prescriptive, meaning it defines what to do, but not how to do it.

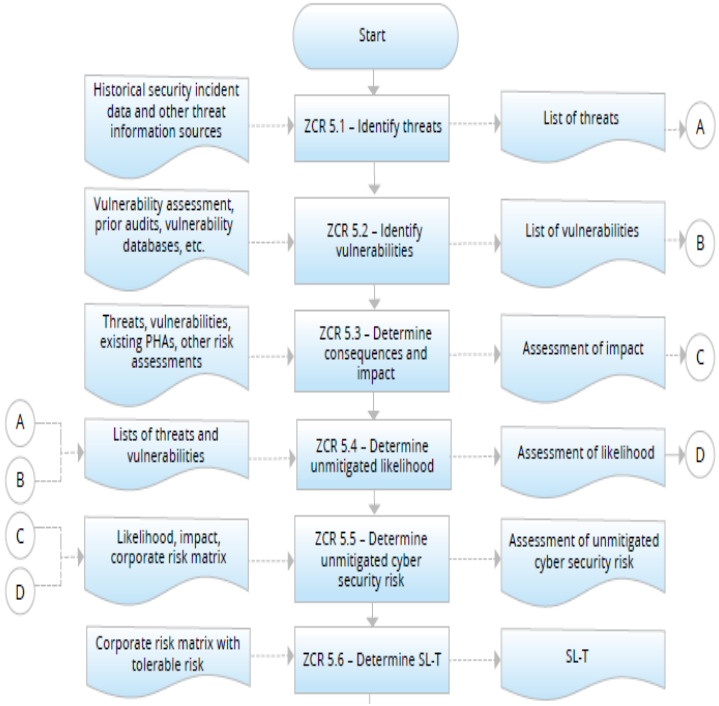
ZCR – Zone and Conduit Requirement

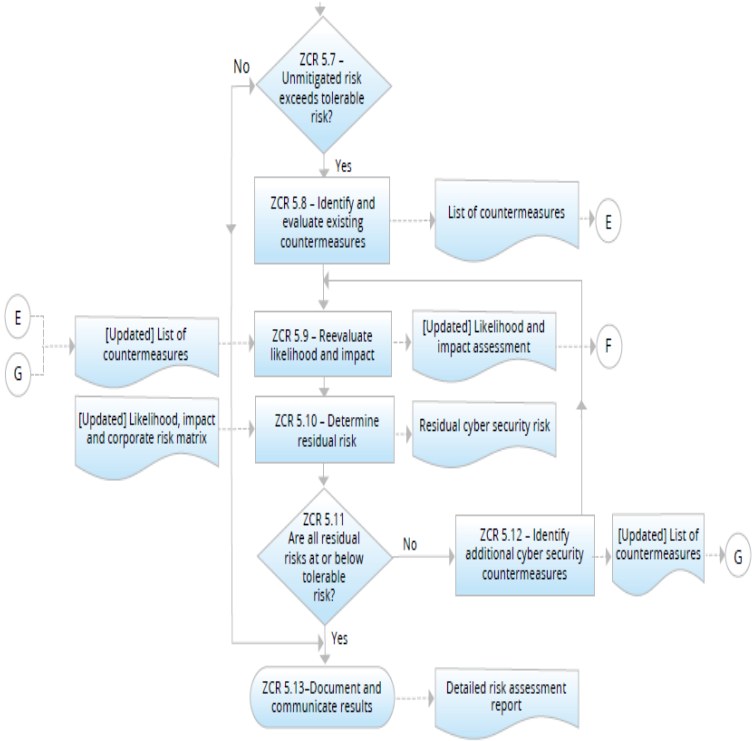
Left Column – Inputs

Right Column – Outputs



Detailed Risk Assessment | IEC 62443





Security Level- Target

- SL-T is a **Desired level of security** for a particular system.

What influences it ?

- Network architecture with defined zone boundaries and conduits
- SL(Target) of the zones with which the zone under consideration will communicate
- SL(Target) of conduit, if assigned, used for communication by the zone
- Physical access to devices and systems within the zone

CRRF: Cyber Risk Reduction Factor

CRRF = Unmitigated Risk / Tolerable Risk.

Unmitigated Risk - risk before any security controls are implemented.

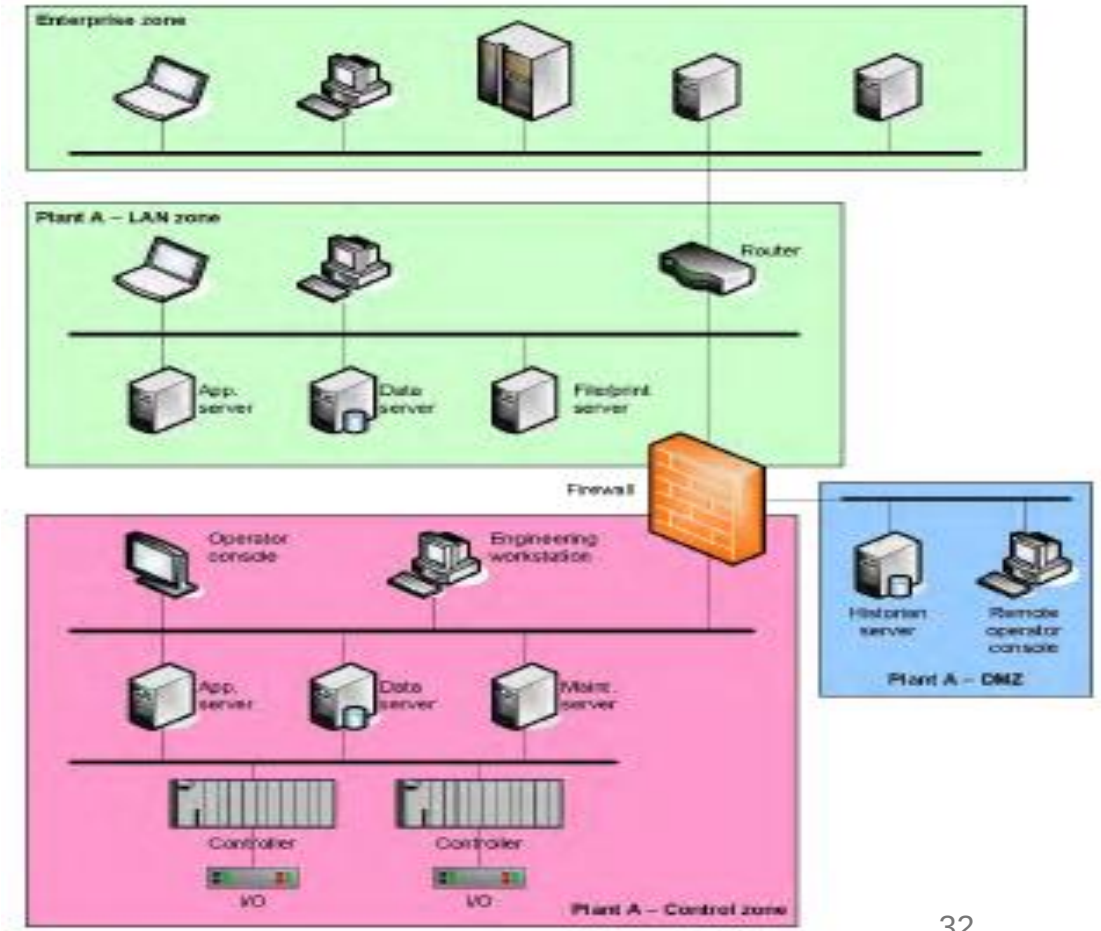
Tolerable Risk - maximum amount of risk that an organization is willing to accept.

Higher the number more the work.

SL-T based upon the organization's risk matrix and risk tolerance.

SL-T Example

Zone	Target Security Level SL(Target)
Plant A control zone	High
Plant A DMZ	Medium
Plant A LAN zone	Medium
Enterprise zone	Low



Treating Risk

Risk treatment plans are reactive measures that specify how to respond and recover from risks after they occur.

Risk Response	Description
Risk Avoidance	Eliminating the risk by discontinuing the operation or activity that's associated with the risk. Example: shutting down a specific process, removing certain devices, or avoiding the use of certain technologies that have been assessed as too risky.
Risk Reduction	Reduce the impact or likelihood of a risk. For example, implementing new security measures such as encryption, firewalls, and intrusion detection systems, or improving physical security.
Risk Transfer	Shifting the risk to another entity. For instance, buying insurance to cover potential losses, or entering into contracts with vendors that include indemnification clauses for certain risks.
Risk Acceptance	Accepting the risk without taking any specific action. often used for low-impact and low-likelihood risks.
Risk Sharing	Distributing risk among several entities, for instance, business partners or within different parts of the organization.

IEC 62443-3-3/4-2 Security Requirements

Foundational Requirements → System Requirements → Requirement enhancements

FRs SRs REs

Example: FR 1 – Identification and authentication control

Purpose and SL-C(IAC) descriptions: Identify and authenticate all users (humans, software processes and devices) before allowing them to access to the control system.

SR 1.1 – Human user identification and authentication:

The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.

Requirement enhancements:

Unique identification and authentication
Multifactor authentication for untrusted networks
Multifactor authentication for all networks

Mapping of SRs with Security Levels

SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control (IAC)				
SR 1.1 – Human user identification and authentication	✓	✓	✓	✓
RE (1) Unique identification and authentication		✓	✓	✓
RE (2) Multifactor authentication for untrusted networks			✓	✓
RE (3) Multifactor authentication for all networks				✓
SR 1.2 – Software process and device identification and authentication		✓	✓	✓
RE (1) Unique identification and authentication			✓	✓
SR 1.3 – Account management	✓	✓	✓	✓
RE (1) Unified account management			✓	✓
SR 1.4 – Identifier management	✓	✓	✓	✓
SR 1.5 – Authenticator management	✓	✓	✓	✓
RE (1) Hardware security for software process identity credentials			✓	✓
SR 1.6 – Wireless access management	✓	✓	✓	✓
RE (1) Unique identification and authentication		✓	✓	✓

SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 2 – Use control (UC)				
SR 2.1 – Authorization enforcement	✓	✓	✓	✓
RE (1) Authorization enforcement for all users		✓	✓	✓
RE (2) Permission mapping to roles		✓	✓	✓
RE (3) Supervisor override			✓	✓
RE (4) Dual approval				✓
SR 2.2 – Wireless use control	✓	✓	✓	✓
RE (1) Identify and report unauthorized wireless devices			✓	✓
SR 2.3 – Use control for portable and mobile devices	✓	✓	✓	✓
RE (1) Enforcement of security status of portable and mobile devices			✓	✓
SR 2.4 – Mobile code	✓	✓	✓	✓
RE (1) Mobile code integrity check			✓	✓

ISA/IEC 62443-4-2: CRs and Types of Components

Component Requirements (CRs):

- Derived from the system requirements (SRs) in ISA-62443-3-3.
- SRs in turn are derived from foundational requirements (FRs) in ISA-62443-1-1.
- CRs can include a set of requirement enhancements (REs). Combined CRs and REs determine a component's target security level.
- Majority of requirements are consistent across all four component types and are termed CR.
- Unique component-specific requirements are mentioned as such and can be found in the component-specific sections of the standard.

Types of Components:

- Software application (SAR)
- Embedded device (EDR)
- Host device (HDR)
- Network device (NDR)

Mapping of CRs and REs to FR SLs 1 to 4

SRs and Res	SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control (IAC)				
CR 1.1 – Human user identification and authentication	✓	✓	✓	✓
RE (1) Unique identification and authentication:		✓	✓	✓
RE (2) Multifactor authentication for all interfaces			✓	✓
CR 1.2 – Software process and device identification and authentication		✓	✓	✓
RE (1) Unique identification and authentication			✓	✓
CR 1.3 – Account management	✓	✓	✓	✓
CR 1.4 – Identifier management	✓	✓	✓	✓
CR 1.5 – Authenticator management	✓	✓	✓	✓
RE (1) Hardware security for authenticators			✓	✓
NDR 1.6 – Wireless access management	✓	✓	✓	✓
RE (1) Unique identification and authentication		✓	✓	✓

IEC 62443-4-1 Secure Development

Defines process (practices) to be used when developing products securely throughout the entire development lifecycle:

- Practice 1 - Security Management
- Practice 2 - Specification of Security Requirements
- Practice 3 - Secure by Design
- Practice 4 - Secure Implementation
- Practice 5 - Security Verification and Validation Testing
- Practice 6 - Management of security related issues
- Practice 7 - Security Update Management
- Practice 8 - Security Guidelines

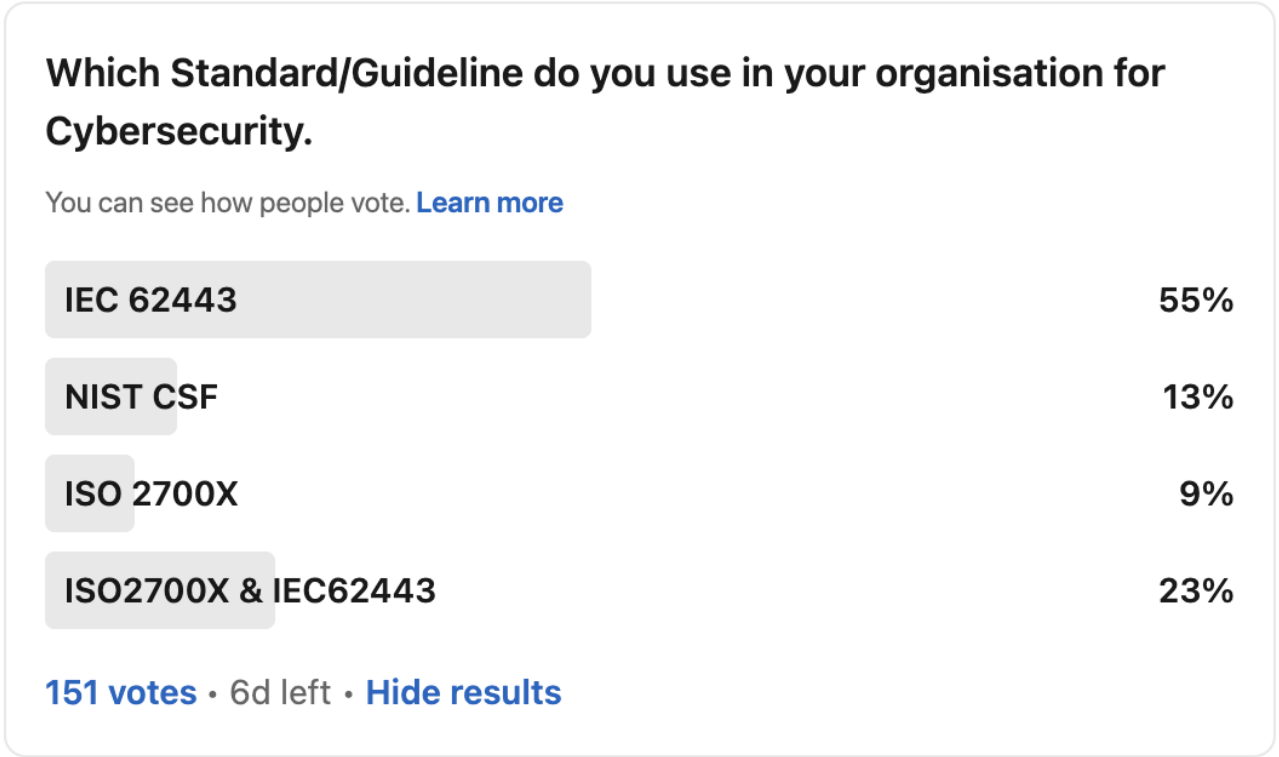
Follows industry-best SDL practices

SDL is interchangeable with:

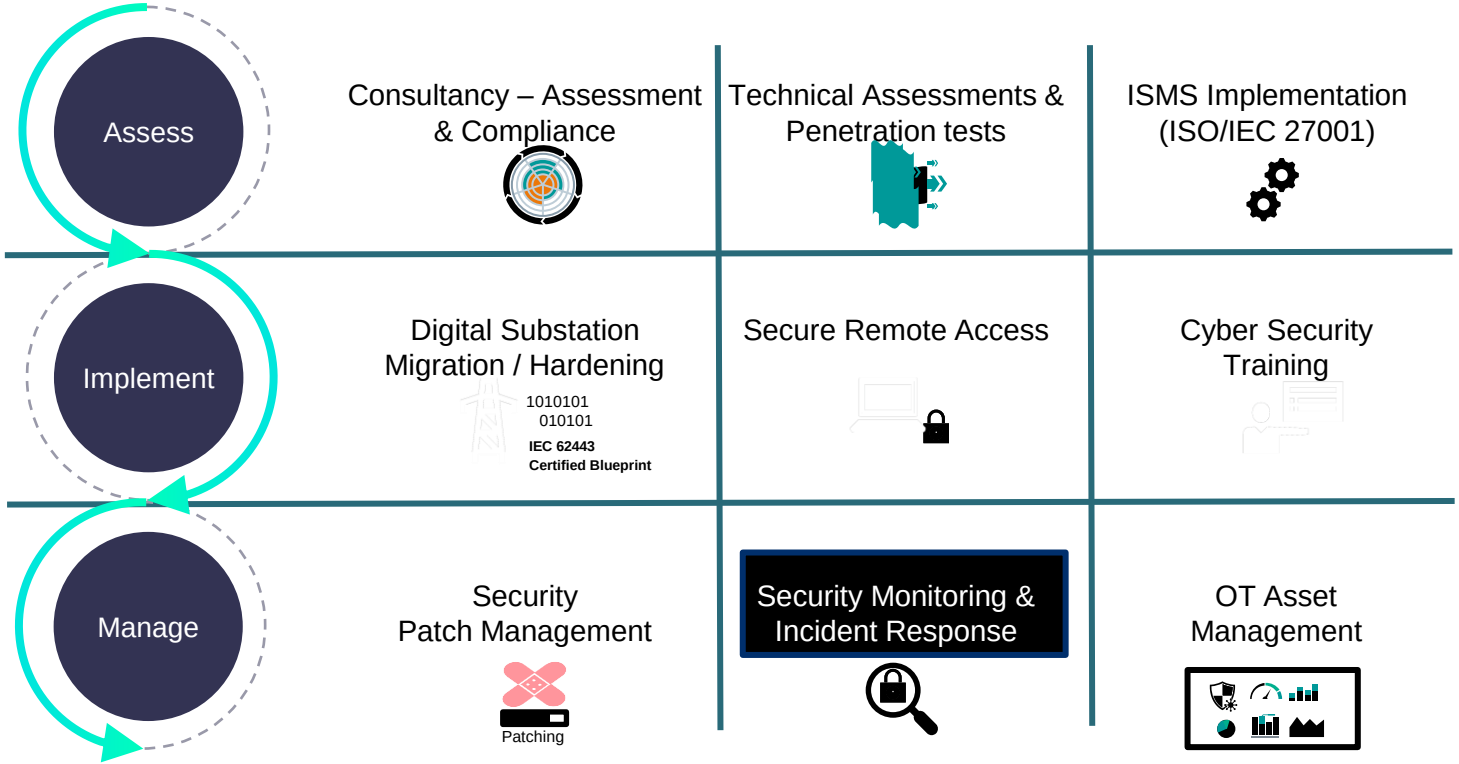
- SDLC (Secure Development Life Cycle)
- Security Development Lifecycle
- Secure Development Lifecycle

SDL introduces security considerations throughout all phases of the development process, helping developers build highly secure products and systems, address security compliance requirements, and reducing development and sustaining costs.
*A key focus of SDL is **building security in** up front.*
SDL was initially focused on software but applies to hardware products and systems such as IACS (Industrial Automation And Control Systems), DCS (Distributed Control System) and electrical utility systems

How much is the adoption of IEC 62443?



The Pragmatic approach for Implementing Security



Benefits

- Comprehensive coverage from a trusted partner
- Reduced downtime in the face of cyber threats
- Operational security with certified solutions
- Swift and secure incident response and recovery
- Premium service with proven competence

NIST 800 82

NIST 800 82 Rev3 Guide to Operational Technology (OT) Security

What is it?

- A set of guidelines published by the National Institute of Standards and Technology (NIST) to help organizations secure their Industrial Control Systems (ICS).
- Offers a risk-based approach to securing critical infrastructure.

Key Points (Bullet Points):

- **Focuses on Risk Management**
  - Identifies, assesses, and prioritizes cybersecurity risks specific to ICS environments.
- **Provides Security Controls:**
  - Recommends a variety of security controls categorized into different families (e.g., access control, incident response) to address identified risks.
  - Emphasizes tailoring controls to the specific needs of each ICS.
- **Highlights Best Practices:**
  - Promotes secure system development practices, secure configuration of devices, and ongoing monitoring for vulnerabilities.
- **Importance of Supply Chain Security:**
  - Emphasizes the need to manage risks associated with vendors and suppliers of ICS components.
- **Cybersecurity Workforce Training:**
  - Stresses the importance of training personnel on cybersecurity best practices to protect ICS.
- **Incident Response Framework:**
  - Provides a framework for handling cybersecurity incidents effectively, minimizing damage and downtime.

NIST Cybersecurity Framework

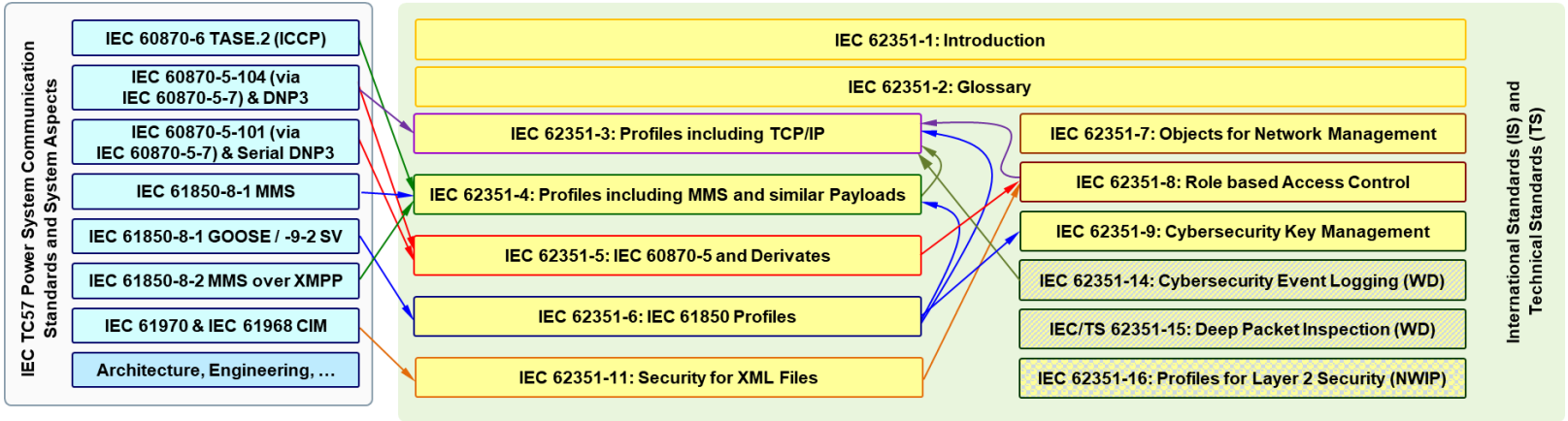
The CSF Functions guide the following actions:

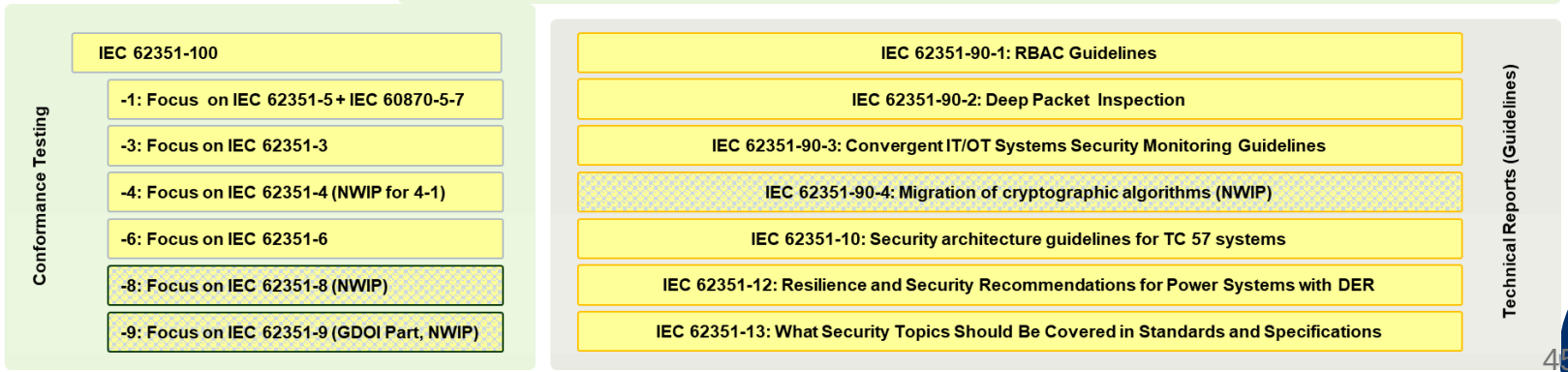
- **Identify (ID)** – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- **Protect (PR)** – Develop and implement appropriate safeguards to ensure delivery of critical services.
- **Detect (DE)** – Develop and implement appropriate activities to identify the occurrence of the cybersecurity event.
- **Respond (RS)** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- **Recover (RC)** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

NIST Cybersecurity Framework

Function	Category	Category Identifier
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

IEC 62351 : Cybersecurity for Digital Grid



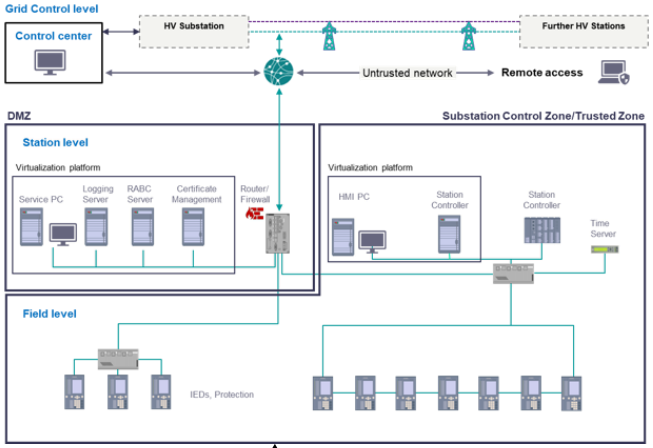


Example of a Compliant System

Cyber Security regulations are provided for instance by
- European NIS/NIS2 Directive and derived country specific laws
- US FERC for North America

ISO/IEC 27001

Asset Owner Operator	IT Infrastructure	ISO/IEC 27001	
		ISO/IEC 27019	IEC 62351
Integrator	IT Infrastructure	IEC 62443-2-4	
		IEC 62443-3-3	IEC 62351
Product Supplier	IT Infrastructure	IEC 62443-3-3	IEC 62443-4-2	IEC 62443-4-1
		IEC 62351	



OT - Infrastructure

Procedural: e.g.: ISMS for operator, or requirements for the development process for integrators and manufacturers

Functional: e.g., security levels, strength of security measures

Technical: e.g., security measures implementation, support interoperability

ISO 27019 vs IEC62443 vs NIST Framework

Feature	ISO 27019	IEC 62443	NIST CSF
Focus	Security for process control systems in the energy sector.	Security for industrial control systems.	General cybersecurity framework applicable across sectors.
Industry Application	Specifically tailored to the energy sector.	Focuses on industrial automation and control systems.	Broad and flexible for all sectors.
Framework Structure	Based on ISO/IEC 27002 but adjusted for energy utility ICS.	Series of standards and technical reports for ICS security.	Consists of five core functions: Identify, Protect, Detect, Respond, Recover.
Purpose	Enhance the security of process control systems and automation.	Improve the safety, availability, integrity, and confidentiality of components or systems.	Provide a policy framework of computer security guidance for how organizations can assess and improve their ability to prevent, detect, and respond to cyber attacks.

ISO 27019 vs IEC62443 vs NIST Framework

Feature	ISO 27019	IEC 62443	NIST CSF
Regulatory Aspect	Often used as a compliance benchmark in the energy sector.	Increasingly referenced for regulatory compliance in industries using control systems.	Used as a voluntary framework, often referenced in regulatory and policy contexts.
International Recognition	Widely recognized in countries with significant energy sectors, like Germany.	Global recognition, particularly in manufacturing and critical infrastructure.	Highly recognized and used worldwide across various industries.
Implementation Detail	Provides detailed controls specific to energy sector needs.	Detailed security levels and risk assessment methodologies specific to ICS.	Provides high-level strategic guidance that can be detailed through sector-specific profiles.

Thank You