SIEMENS
Ingenuity for life

Industrial Security

Getting Started…

siemens.com/industrial-security

The

Threat Landscape

The Global Risks Report 2019 14th Edition
The Global Risks Landscape

SIEMENS
Ingenuity for life

WORLD ECONOMIC FORUM

Top 10 risks in terms of **Likelihood**

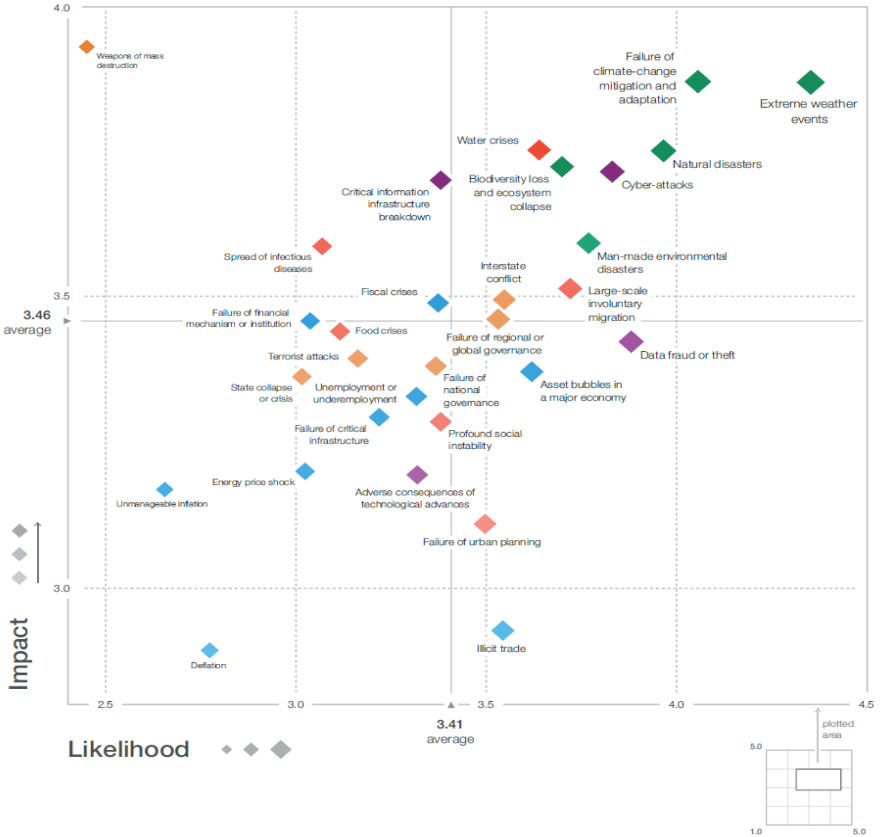
1. Extreme weather events
2. Failure of climate-change mitigation and adaptation
3. Natural disasters
4. Data fraud or theft
5. Cyber-attacks
6. Man-made environmental disasters
7. Large-scale involuntary migration
8. Biodiversity loss and ecosystem collapse
9. Water crises
10. Asset bubbles in a major economy

Top 10 risks in terms of **Impact**

1. Weapons of mass destruction
2. Failure of climate-change mitigation and adaptation
3. Extreme weather events
4. Water crises
5. Natural disasters
6. Biodiversity loss and ecosystem collapse
7. Cyber-attacks
8. Critical information infrastructure breakdown
9. Man-made environmental disasters
10. Spread of infectious diseases

Categories

- Economic
- Environmental
- Geopolitical
- Societal
- Technological



Source: https://www.weforum.org/reports/the-glc

Motivation
More than productivity

SIEMENS
Ingenuity for life

Shareholders

Insurance

Regulatory requirements and Legislation

Who are we?

What do we do?

Our reality

"Security is a top priority for Siemens as the world's leading automation provider with **30 million automated systems**, **75 million contracted smart meters** and **one million Cloud connected products** in the field"

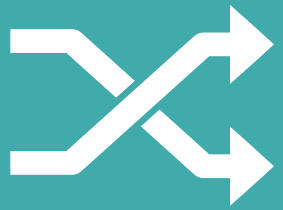
Digitalization and… IIoT

Unlocks enormous opportunities and potentials in all industries

SIEMENS
Ingenuity for life

Speed

Flexibility



Quality

Efficiency

Security

Pushing Industrial Security
Charter of Trust

SIEMENS
Ingenuity for life

More info: www.charter-of-trust.com

Cyberwar and cyberattacks

NATO Cooperative Cyber Defense Centre of Excellence

SIEMENS
Ingenuity for life

LOCKED SHIELDS

Tallinn, Estonia (April 23rd to 27th 2018)

More info: ccdcoe.org/nato...ields-2018.html

So…

how do we start?

Caught between regulation, requirements, and standards

SIEMENS
Ingenuity for life

The all encompassing Industrial Security Standard

Provides greater clarity by clearly defining the roles and responsibilities

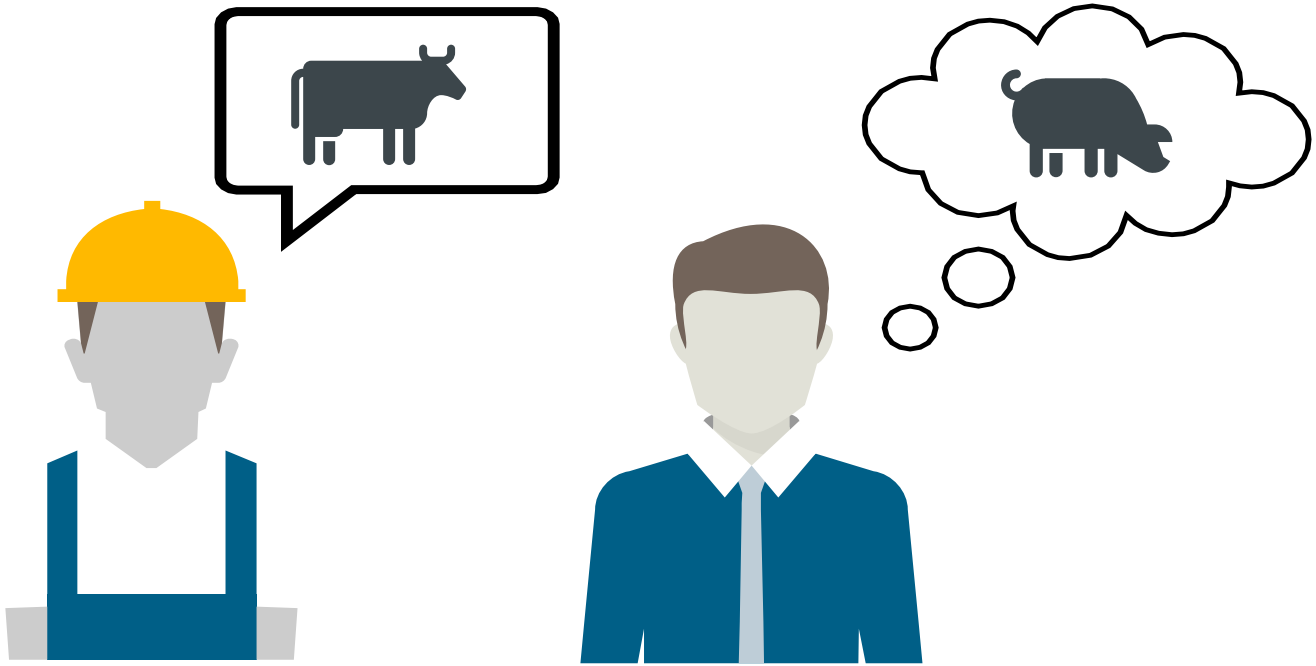
SIEMENS
Ingenuity for life

IEC 62443

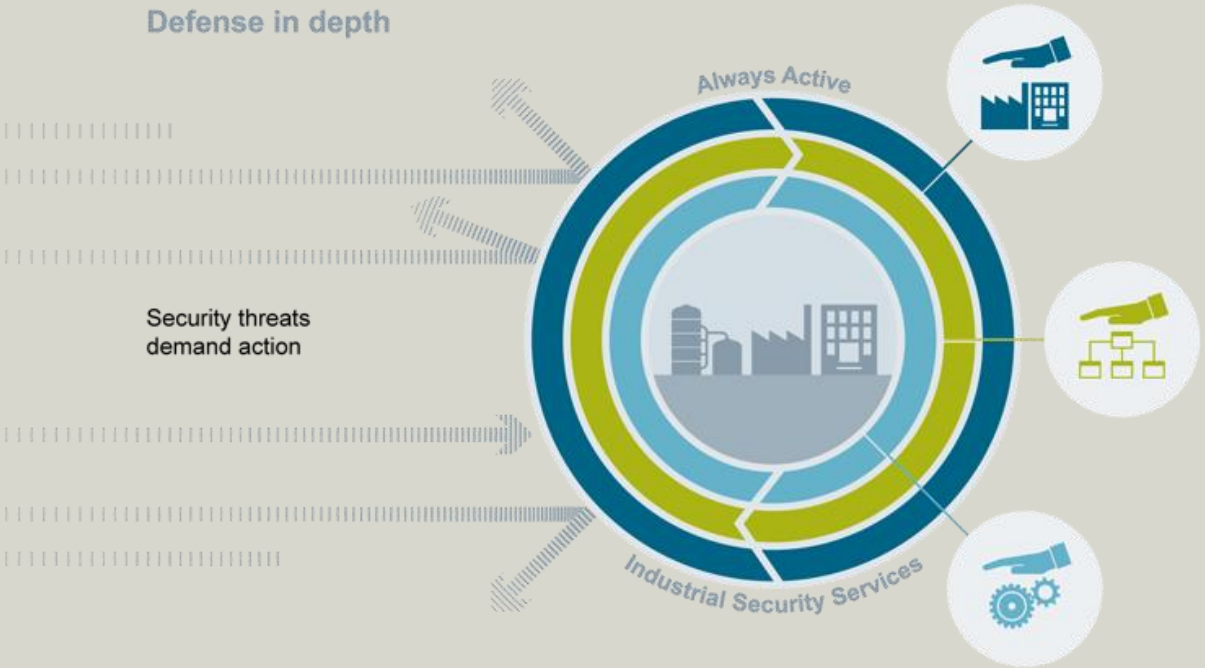
From IEC62443

IEC 62443 gives us the ability to communicate
In an unambiguous way

SIEMENS
Ingenuity for life



IEC 62443 addresses the Defense in Depth concept



Plant Security

- Physical access protection
- Processes and guidelines
- Security service protecting production plants

Network Security

- Cell protection, DMZ and remote maintenance
- Firewall and VPN
- Segmentation
- Asset and Network Management

System integrity

- System hardening
- Authentication and user administration
- Patch management
- Logging and Monitoring
- Detection of attacks

IEC 62443 focus on the interfaces between all stakeholders

SIEMENS
Ingenuity for life

Operator, **Integrator**, and **Manufacturer**

IEC 62443 from machines to corporates

SIEMENS
Ingenuity for life

It is **scalable**

IEC 62443 provides a complete Cyber Security Management System

SIEMENS
Ingenuity for life

Risk based approach

That covers the setup of:

Risk analysis

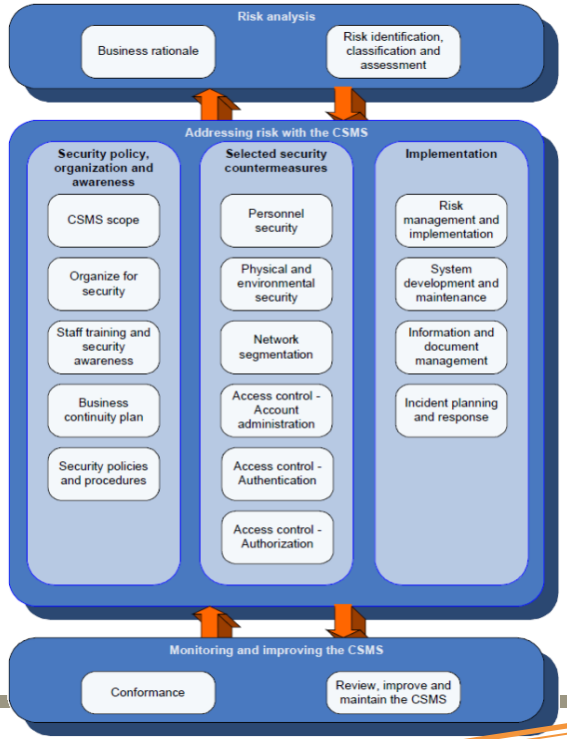
Addressing risk

security organization and **security processes**

security countermeasures

and **Implementation**

Monitoring and improving



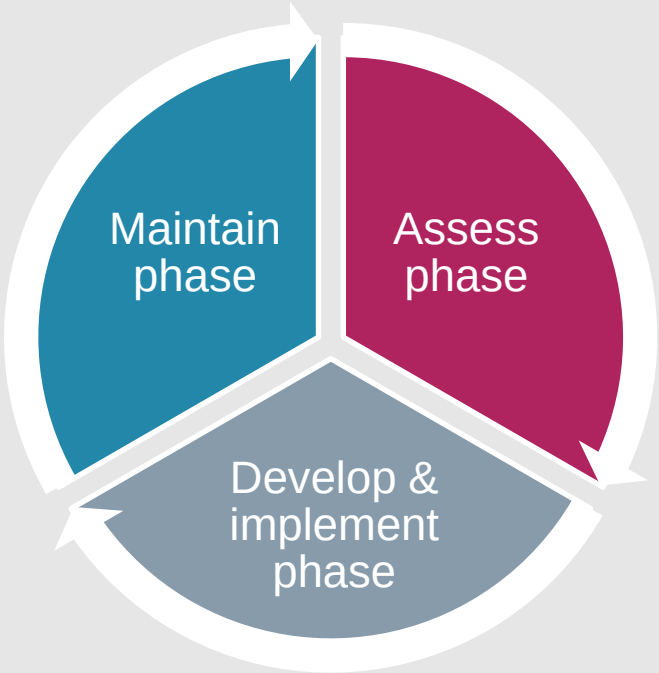
From IEC62443-3-2

IEC 62443 from the beginning to the end

SIEMENS
Ingenuity for life

It addresses the entire **life cycle**

Cybersecurity Life Cycle



From IEC62443-3-2

Cybersecurity Life Cycle
Getting started

SIEMENS
Ingenuity for life

Assess phase

High-level Cyber Risk Assessment

Allocation of IACS Assets to Zones or Conduits

Detailed Cyber Risk Assessment

Develop & implement phase

Cybersecurity Requirements Specification

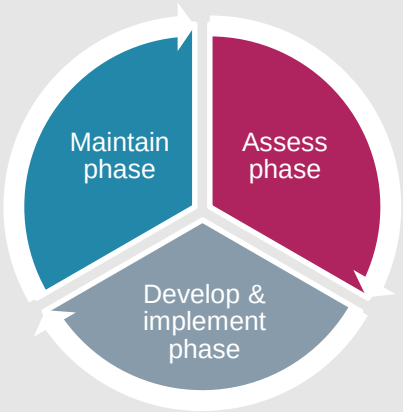
Design and Engineering of countermeasures or other means of risk reduction

Installation, commissioning and validation of countermeasures

Maintain phase

Maintenance, Monitoring and Management of change

Incident Response and Recovery



From IEC62443-3-2

SIEMENS
Ingenuity for life

Risk = Likelihood x Consequence

Where: Likelihood = Threat x Vulnerability

From IEC62443-3-2

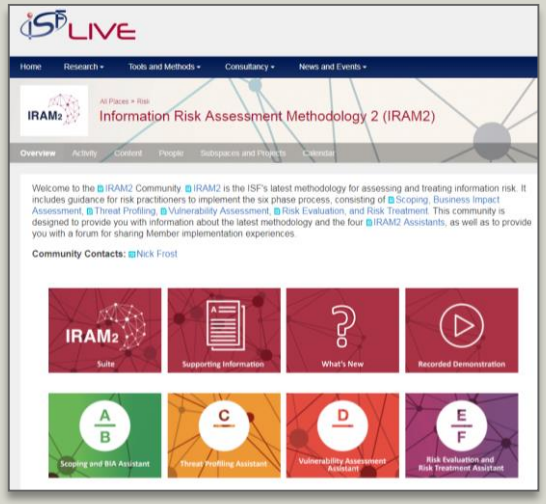
Assess phase
Risk methods and frameworks

SIEMENS
Ingenuity for life

National Cyber Security Centre
a part of GCHQ

A good overview

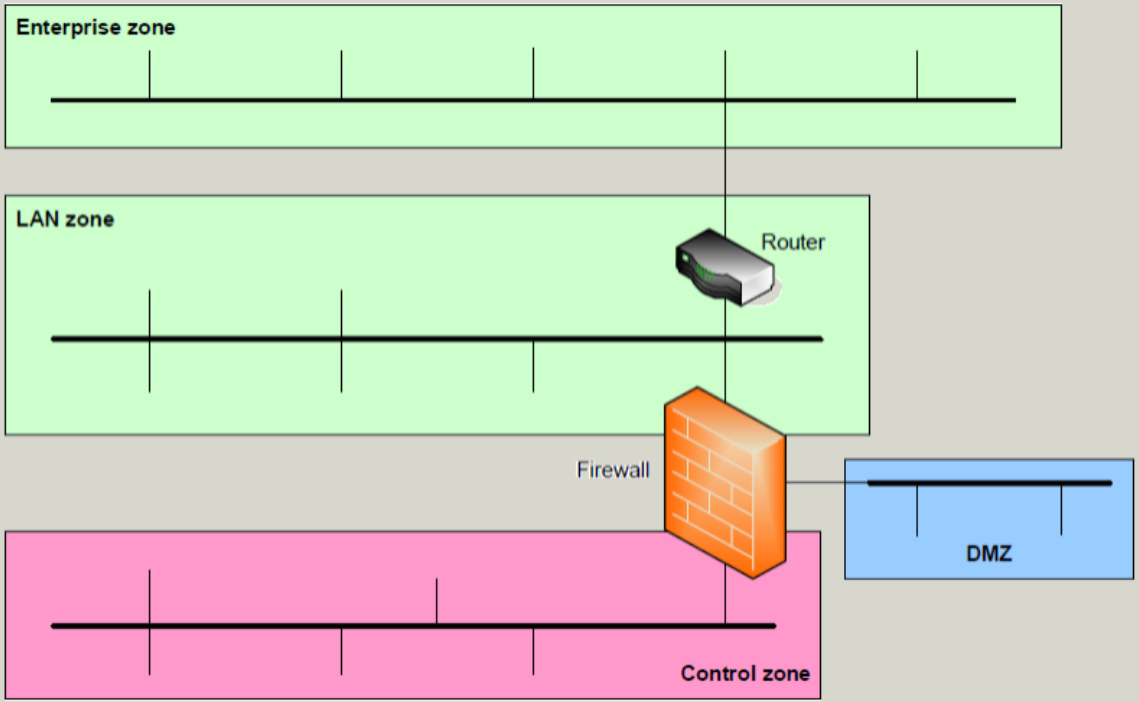
The Information Security Forum (ISF)



National Institute of Standards and Technology (NIST) and…

More info: https://www.ncsc.gov.uk/guidance/summary-risk-methods-and-frameworks

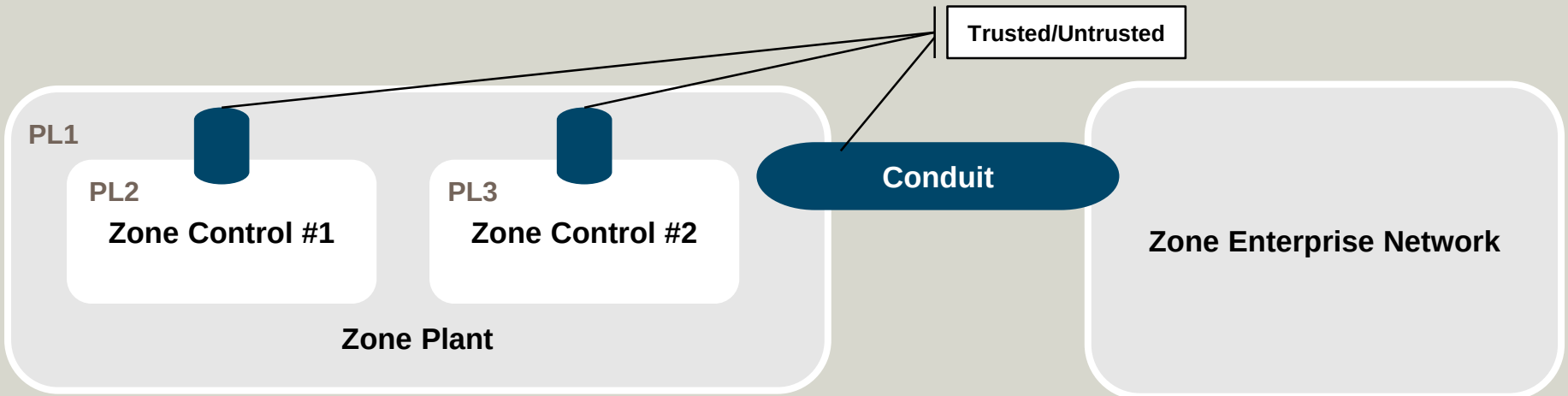
Assess phase
Segmentation of TI and OT



From IEC62443-3-2

Assess phase
Zones and Conduits

SIEMENS
Ingenuity for life

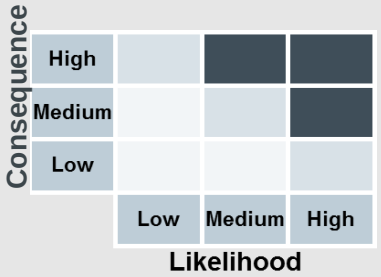


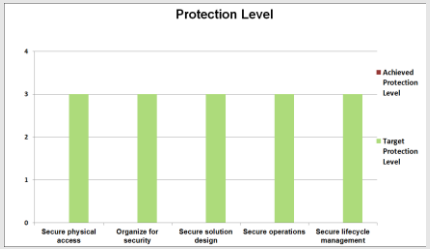
From IEC62443-3-2

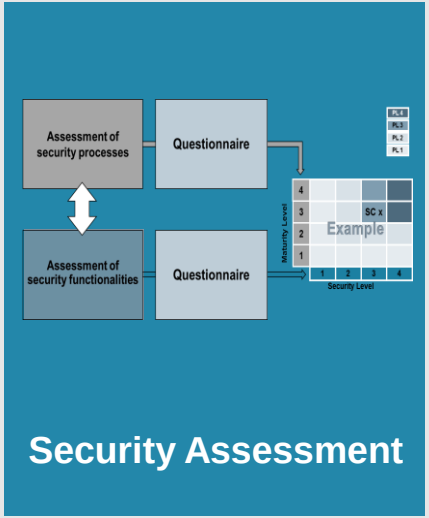
Assess phase
Risk based development of security levels

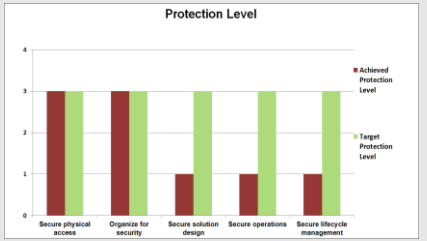
SIEMENS
Ingenuity for life

Evaluate Business Risk to determine Criticality → **Assign Target Protection Levels** → **Evaluate Protection Levels** → **Achieved Protection Levels**









But…

how **specific**

is the **IEC 62443?**

What is the structure of IEC 62443?

SIEMENS
Ingenuity for life

1-1 General
Terminology, concepts and models

1-2 General
Master glossary of terms and abbreviations

1-3 General
System security compliance metrics

1-4 General
IACS sec. life cycle and use case

1-5 General
IACS protection levels

2-1 Policies and procedures
Establishing an IACS security program

2-2 Policies and procedures
Operating an IACS security program

2-3 Policies and procedures
Patch management in the IACS environment

2-4 Policies and procedures
Certification of IACS supplier security policies

3-1 System
Security technologies for IACS

3-2 System
Security assurance levels for zones and conduits

3-3 System
System sec. requirements and security assurance levels

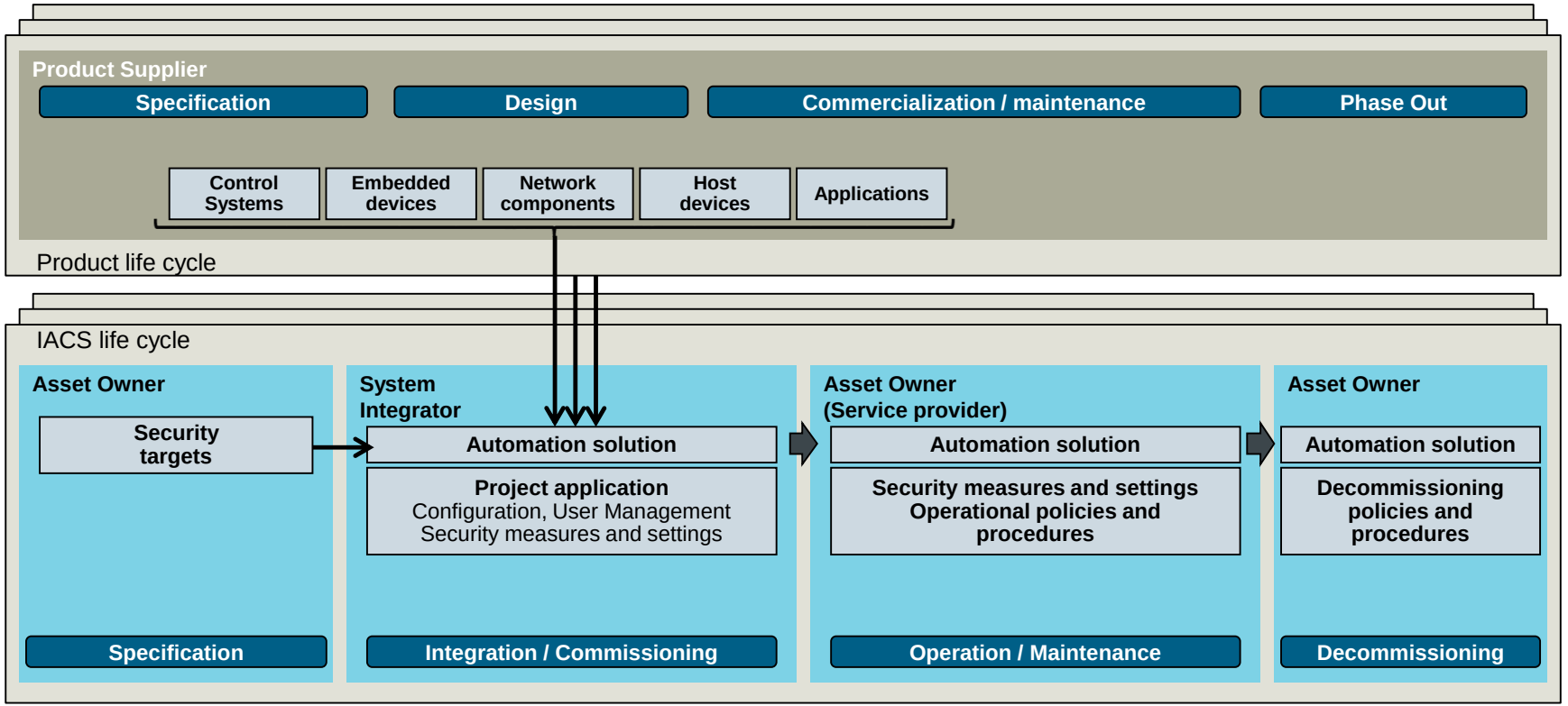
4-1 Component
Product development requirements

4-2 Component
Technical sec. requirements for IACS products

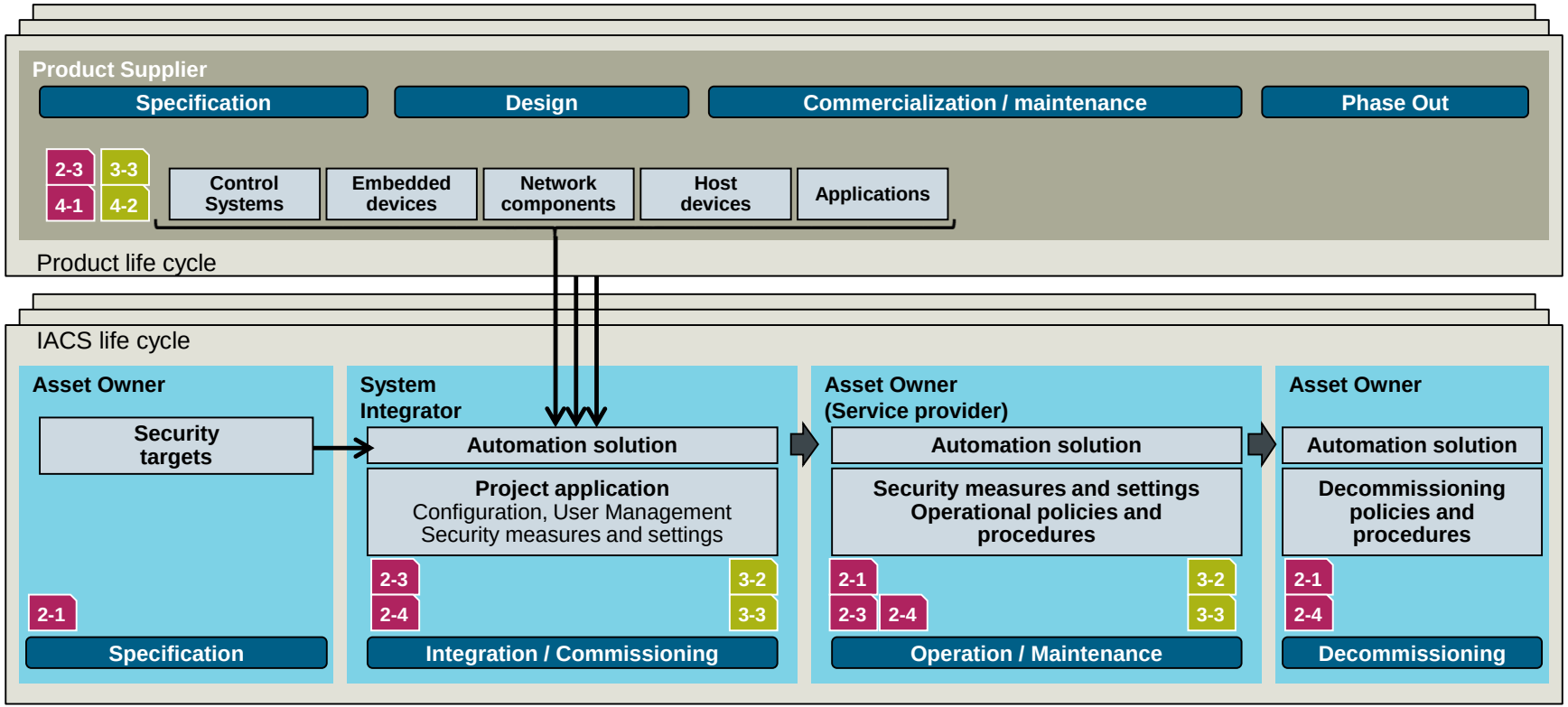
Definition and metrics
Processes / procedures
Functional requirements

From IEC62443

Phases in product and IACS life cycles



Phases in product and IACS life cycles



Protection Levels
Cover security functionalities and processes

SIEMENS
Ingenuity for life

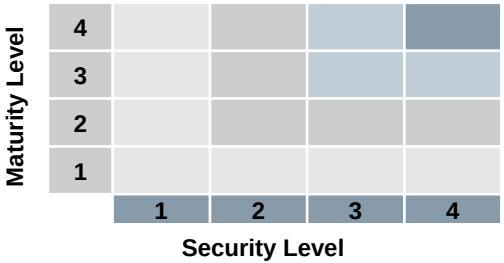
Security functionalities

SL 1	Capability to protect against casual or coincidental violation
SL 2	Capability to protect against intentional violation using simple means with low resources, generic skills and low motivation
SL 3	Capability to protect against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
SL 4	Capability to protect against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

Security processes

ML 1	**Initial** - Process unpredictable, poorly controlled and reactive.
ML 2	**Managed** - Process characterized , reactive
ML 3	**Defined** - Process characterized, proactive deployment
ML 4	**Optimized** - Process measured, controlled and continuously improved

Protection Levels



PL 1	Protection against casual or coincidental violation
PL 2	Protection against intentional violation using simple means with low resources, generic skills and low motivation
PL 3	Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
PL 4	Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

From IEC62443

IEC 62443 Security measures
It is unambiguous …

SIEMENS
Ingenuity for life

	Secure Physical Access	Organize Security	Secure Solution Design	Secure Operations	Secure Lifecycle management
PL 4	Revolving doors with card reader and PIN; Video Surveillance and/or IRIS Scanner at door	Dual approval for critical actions	Firewalls with Fail Close(e.g. Next Generation Firewall)	Monitoring of all device activities	Online security functionality verification …
+ PL 3	Revolving doors with card reader	No Email, No WWW, etc. in Secure Cell …	2 PCs (Secure Cell/outside) …	Monitoring of all human interactions …	Automated backup / recovery Remote access with cRSP or equivalent
+ PL 2	Doors with card reader	Persons responsible for security within own organization Mandatory security education	Physical network segmentation or equivalent (e.g. SCALANCE S)	Continuous monitoring (e.g. SIEM) …	Backup verification Remote access restriction (e.g. need to connect principle)
+ PL 1	Locked building/doors with keys	Awareness training (e.g. Operator Aware. training) Mandatory rules on USB sticks (e.g. Whitelisting)	Network segmentation (e.g. VLAN)	Security logging on all systems …	Backup / recovery system

Protection Levels
Cover security functionalities and processes

SIEMENS
Ingenuity for life

PL 1	Protection against casual or coincidental violation
PL 2	Protection against intentional violation using simple means with low resources, generic skills and low motivation
PL 3	Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
PL 4	Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

IEC 62443-3-3

Defines security requirements for industrial control systems

SIEMENS
Ingenuity for life

7 Foundational Requirements

FR 1 – Identification and authentication control

FR 2 – Use control

FR 3 – System integrity

FR 4 – Data confidentiality

FR 5 – Restricted data flow

FR 6 – Timely response to events

FR 7 – Resource availability

From IEC62443-3-3

FR 1 – Identification and authentication control
System Requirement Overview (Part 1)

SIEMENS
Ingenuity for life

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

From IEC62443-3-3

SIEMENS
Ingenuity for life

5.3 SR 1.1 – Human user identification and authentication

5.3.1 Requirement

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.

5.3.2 Rationale and supplemental guidance

All human users need to be identified and authenticated for all access to the control system. Authentication of the identity of these users should be accomplished by using methods such as passwords, tokens, biometrics or, in the case of multifactor authentication, some combination thereof. The geographic location of human users can also be used as part of the authentication process…….

From IEC62443-3-3

FR 1 – Identification and authentication control
System Requirement Overview (Part 2)

SIEMENS
Ingenuity for life

SRs und REs	SL 1	SL 2	SL 3	SL 4
SR 1.7 – **Strength of password-based authentication**	✔	✔	✔	✔
SR 1.7 RE 1 – Password generation and lifetime restrictions for human users			✔	✔
SR 1.7 RE 2 – Password lifetime restrictions for all users				✔
SR 1.8 – **Public key infrastructure certificates**		✔	✔	✔
SR 1.9 – **Strength of public key authentication**		✔	✔	✔
SR 1.9 RE 1 – Hardware security for public key authentication			✔	✔
SR 1.10 – **Authenticator feedback**	✔	✔	✔	✔
SR 1.11 – **Unsuccessful login attempts**	✔	✔	✔	✔
SR 1.12 – **System use notification**	✔	✔	✔	✔
SR 1.13 – Access via untrusted networks	✔	✔	✔	✔
SR 1.13 RE 1 – Explicit access request approval		✔	✔	✔

From IEC62443-3-3

FR 2 – Use control
System Requirement Overview (Part 1)

SIEMENS
Ingenuity for life

SRs und REs	SL 1	SL 2	SL 3	SL 4
SR 2.1 – Authorization enforcement	✔	✔	✔	✔
SR 2.1 RE 1 – Authorization enforcement for **all users**		✔	✔	✔
SR 2.1 RE 2 – Permission mapping to roles		✔	✔	✔
SR 2.1 RE 3 – Supervisor override			✔	✔
SR 2.1 RE 4 – Dual approval				✔
SR 2.2 – **Wireless use** control	✔	✔	✔	✔
SR 2.2 RE 1 – Identify and report unauthorized wireless devices			✔	✔
SR 2.3 – Use control for **portable and mobile devices**	✔	✔	✔	✔
SR 2.3 RE 1 – Enforcement of security status of portable and mobile devices			✔	✔
SR 2.4 – Mobile code	✔	✔	✔	✔
SR 2.4 RE 1 – Mobile code integrity check			✔	✔
SR 2.5 – **Session lock**	✔	✔	✔	✔

From IEC62443-3-3

FR 2 – Use control
System Requirement Overview (Part 2)

SIEMENS
Ingenuity for life

SRs und REs	SL 1	SL 2	SL 3	SL 4
SR 2.6 – **Remote session termination**		✔	✔	✔
SR 2.7 – **Concurrent session control**			✔	✔
SR 2.8 – **Auditable events**	✔	✔	✔	✔
SR 2.8 RE 1 – Centrally managed, system-wide audit trail			✔	✔
SR 2.9 – **Audit storage capacity**	✔	✔	✔	✔
SR 2.9 RE 1 – Warn when audit record storage capacity threshold reached			✔	✔
SR 2.10 – **Response to audit processing failures**	✔	✔	✔	✔
SR 2.11 – **Timestamps**		✔	✔	✔
SR 2.11 RE 1 – Internal time synchronization			✔	✔
SR 2.11 RE 2 – Protection of time source integrity				✔
SR 2.12 – **Non-repudiation**			✔	✔
SR 2.12 RE 1 – Non-repudiation for all users				✔

From IEC62443-3-3

FR 3 – System integrity
System Requirement Overview

SIEMENS
Ingenuity for life

SRs und REs	SL 1	SL 2	SL 3	SL 4
SR 3.1 – **Communication integrity**	✔	✔	✔	✔
SR 3.1 RE 1 – Cryptographic integrity protection			✔	✔
SR 3.2 – **Malicious code protection**	✔	✔	✔	✔
SR 3.2 RE 1 – Malicious code protection on entry and exit points		✔	✔	✔
SR 3.2 RE 2 – Central management and reporting for malicious code protection			✔	✔
SR 3.3 – Security functionality verification	✔	✔	✔	✔
SR 3.3 RE 1 – Automated mechanisms for security functionality verification			✔	✔
SR 3.3 RE 2 – Security functionality verification during normal operation				✔
SR 3.4 – **Software and information integrity**		✔	✔	✔
SR 3.4 RE 1 – Automated notification about integrity violations			✔	✔
SR 3.5 – **Input validation**	✔	✔	✔	✔
SR 3.6 – Deterministic output	✔	✔	✔	✔
SR 3.7 – **Error handling**		✔	✔	✔
SR 3.8 – **Session integrity**		✔	✔	✔
SR 3.8 RE 1 – Invalidation of session IDs after session termination			✔	✔
SR 3.8 RE 2 – Unique session ID generation			✔	✔
SR 3.8 RE 3 – Randomness of session IDs				✔
SR 3.9 – **Protection of audit information**		✔	✔	✔
SR 3.9 RE 1 – Audit records on write-once media				✔

From IEC62443-3-3

FR 4 – Data confidentiality
System Requirement Overview

SIEMENS
Ingenuity for life

SRs und REs	SL 1	SL 2	SL 3	SL 4
SR 4.1 – **Information confidentiality**	✔	✔	✔	✔
SR 4.1 RE 1 – Protection of confidentiality at rest or in transit via untrusted networks		✔	✔	✔
SR 4.1 RE 2 – Protection of confidentiality across zone boundaries				✔
SR 4.2 – **Information persistence**		✔	✔	✔
SR 4.2 RE 1 – Purging of shared memory resources			✔	✔
SR 4.3 – **Use of cryptography**	✔	✔	✔	✔

From IEC62443-3-3

FR 5 – Restricted data flow
System Requirement Overview

SIEMENS
Ingenuity for life

SRs und REs	SL 1	SL 2	SL 3	SL 4
SR 5.1 – **Network segmentation**	✓	✓	✓	✓
SR 5.1 RE 1 – Physical network segmentation		✓	✓	✓
SR 5.1 RE 2 – Independence from non-control system networks			✓	✓
SR 5.1 RE 3 – Logical and physical isolation of critical networks				✓
SR 5.2 – **Zone boundary protection**	✓	✓	✓	✓
SR 5.2 RE 1 – Deny by default, allow by exception		✓	✓	✓
SR 5.2 RE 2 – Island mode			✓	✓
SR 5.2 RE 3 – Fail close			✓	✓
SR 5.3 – General purpose person-to-person communication restrictions	✓	✓	✓	✓
SR 5.3 RE 1 – Prohibit all general purpose person-to-person communications			✓	✓
SR 5.4 – **Application partitioning**	✓	✓	✓	✓

From IEC62443-3-3

FR 6 – Timely response to events
System Requirement Overview

SIEMENS
Ingenuity for life

SRs und REs	SL 1	SL 2	SL 3	SL 4
SR 6.1 – **Audit log accessibility**	✔	✔	✔	✔
SR 6.1 RE 1 – Programmatic access to audit logs			✔	✔
SR 6.2 – **Continuous monitoring**		✔	✔	✔

From IEC62443-3-3

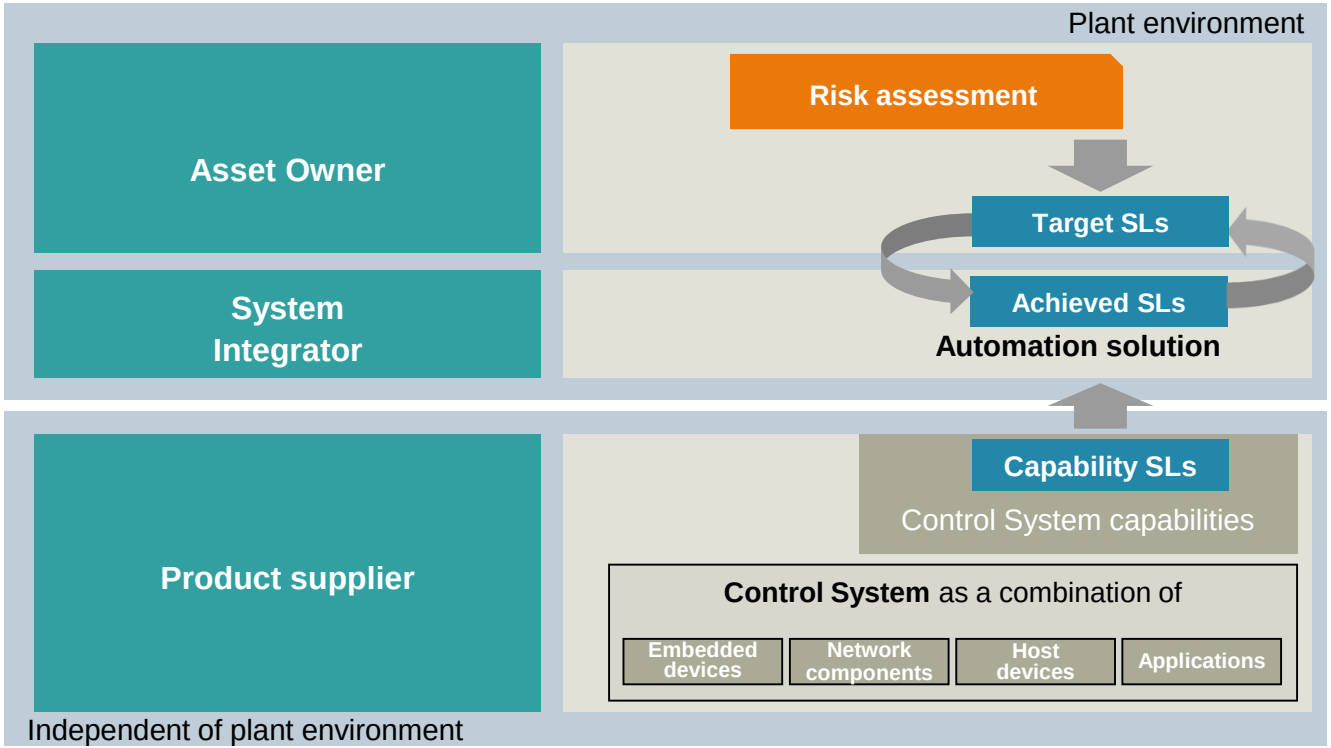
FR 7 – Resource availability
System Requirement Overview

SIEMENS
Ingenuity for life

SRs und REs	SL 1	SL 2	SL 3	SL 4
SR 7.1 – **Denial of service protection**	✔	✔	✔	✔
SR 7.1 RE 1 – Manage communication loads		✔	✔	✔
SR 7.1 RE 2 – Limit DoS effects to other systems or networks			✔	✔
SR 7.2 – Resource management	✔	✔	✔	✔
SR 7.3 – **Control system backup**	✔	✔	✔	✔
SR 7.3 RE 1 – Backup verification		✔	✔	✔
SR 7.3 RE 2 – Backup automation			✔	✔
SR 7.4 – **Control system recovery and reconstitution**	✔	✔	✔	✔
SR 7.5 – **Emergency power**	✔	✔	✔	✔
SR 7.6 – **Network and security configuration settings**	✔	✔	✔	✔
SR 7.6 RE 1 – Machine-readable reporting of current security settings			✔	✔
SR 7.7 – Least functionality	✔	✔	✔	✔
SR 7.8 – **Control system component inventory**		✔	✔	✔

From IEC62443-3-3

Recap - System Security Levels
Contributions of the stakeholders

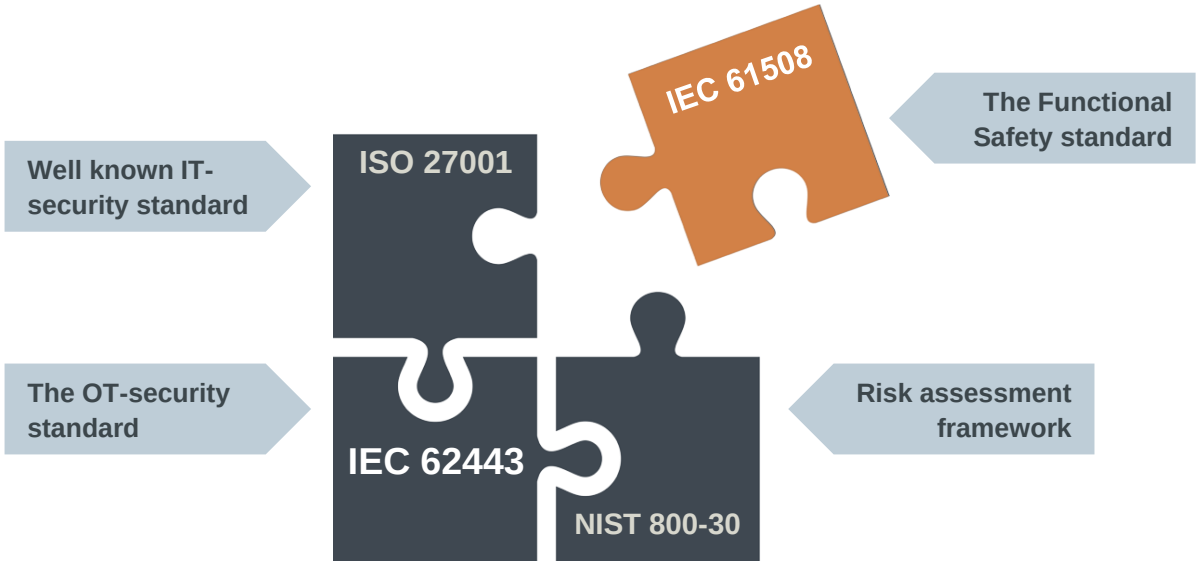


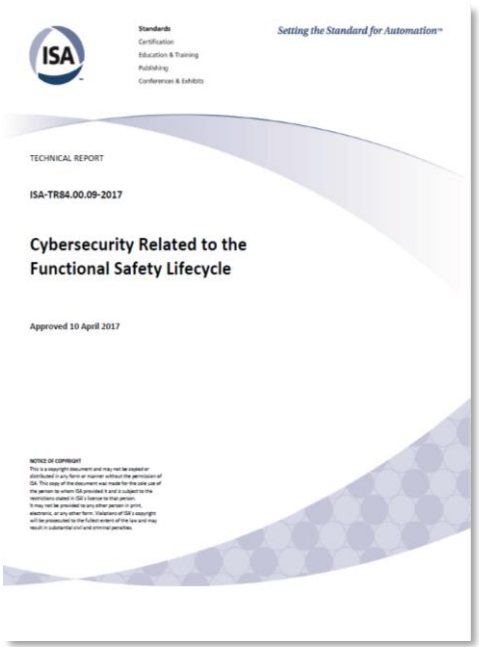
IEC 62443

- 2-1 Establishing an IACS security program
- 3-2 Security risk assessment and system design
- 2-4 Certification of IACS supplier security policies
- 3-3 System security requirements and Security levels
- 4-1 Product development requirements
- 4-2 Technical security requirements for IACS products

A piece of a bigger picture

SIEMENS
Ingenuity for life





DS DANSK STANDARD ISA IEC ISO

Recap…

Act **now**

Everyone is a **target** – also small and medium sized plants

IEC62443 is a **Risk based framework** that can help you **getting started** in a **very structured** way

Define your **Risk…**

Define your **Organization**

Define your **Protection level**

Define your **Zones** and **Conduits**

Thank You

for your attention

Contact information

Name	Phone	email
Per Krogh Christiansen	+4540426239	per.christiansen@siemens.com
Jesper Kristiansen	+45 2478 7829	jesper.kristiansen@siemens.com
Morten Kromann	+45 2037 3508	morten.kromann@siemens.com
Lars Peter Hansen	+45 2129 9650	lars-peter.hansen@siemens.com

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.
In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept.

The customer is responsible for preventing unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the Internet where necessary and with appropriate security measures (e.g., use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends applying product updates as soon as they are available, and always using the latest product version. Using versions that are obsolete or are no longer supported can increase the risk of cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at http://www.siemens.com/industrialsecurity.