SIEMENS
Ingenuity for life

Industry Information Live

Beskyt produktiviteten med Industrial Security

www.siemens.dk/di-webinarer

Dagens værter

Morten Kromann
Technology Specialist

Lars Peter Hansen
Technology Specialist Manager

Per Christiansen
Q&A

Jesper Kristiansen
Q&A

Kim Meyer Jacobsen
Moderator

Agenda

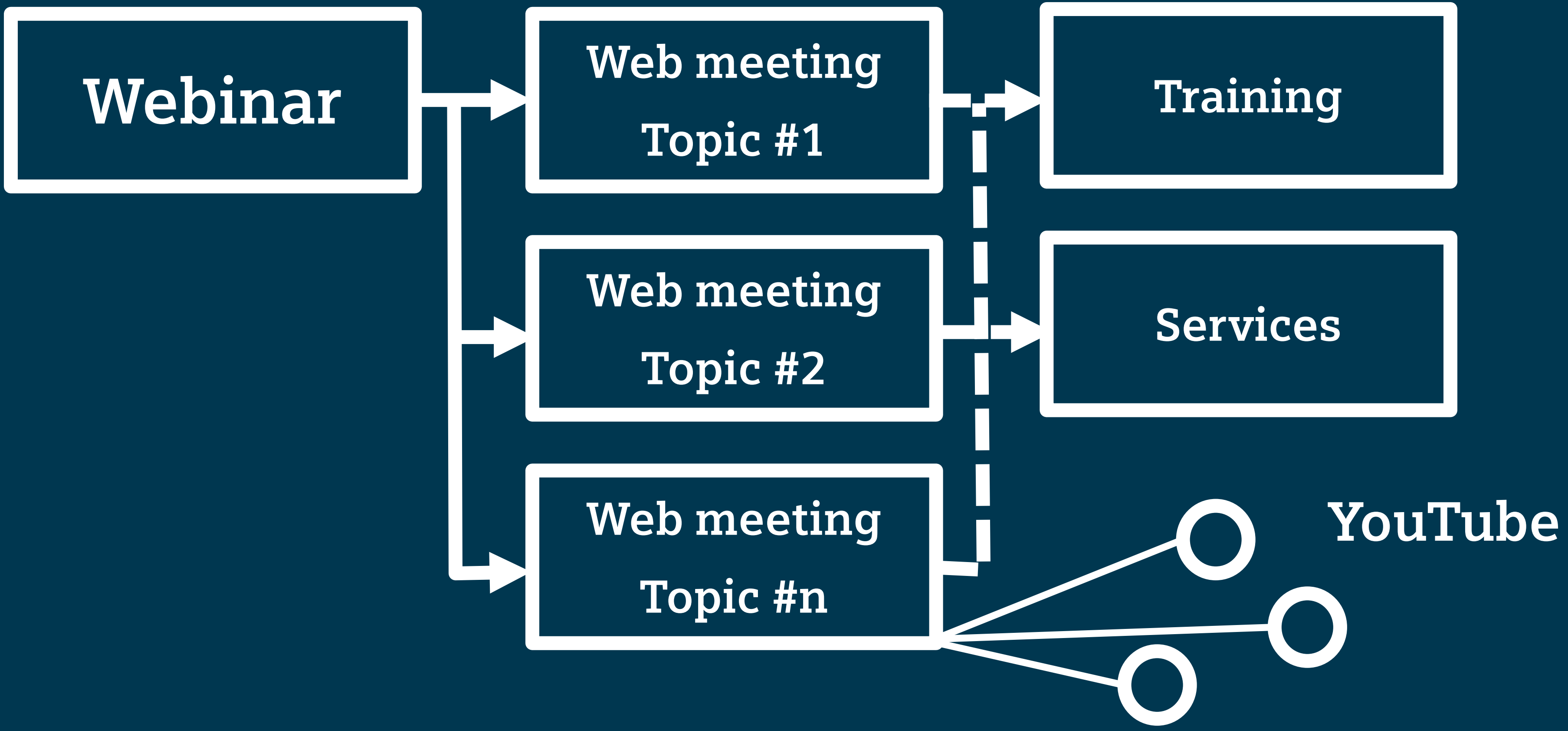
Beskyt produktiviteten med Industrial Security

- Who are we?
- How do we start?
- The standard
- Operational guidelines
- Getting specific

SIEMENS
Ingenuity for life

SIEMENS
Ingenuity for life

Way more information – **NO spam**…!



Who are we?

What do we do?

Taking cyber threats **seriously**

With **> 30 million** automated systems, > 75 million contracted smart meters and **> one million** Cloud connected products in the field”

SIEMENS
Ingenuity for life

Charter of Trust

Leading global companies and organizations working together to make the **digital world** of tomorrow **safer**

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

Charter of Trust

We sign for cybersecurity!

We sign the Charter of Trust.

SIEMENS AES AIRBUS Allianz AtoS CISCO DAIMLER DELL Technologies

enel IBM Munich Security Conference MSC Münchner Sicherheitskonferenz NXP SGS T · · TOTAL TÜV SÜD

SIEMENS
Ingenuity for life

LOCKED SHIELDS

NATO Cooperative Cyber Defense Centre of Excellence

More info: https://ccdcoe.org/exercises/locked-shields/

So…

How do we start?

SIEMENS
Ingenuity for life

Caught between **regulation**, **requirements**, and **standards**

BDSG

Bundesamt
für Sicherheit in der
Informationstechnik

NIS directive

WIB
The Process Automation Users' Association

WIB

NERC CIP

Homeland
Security

ISO 27032

ISA 99

IEC 62443

ANSSI

ANSSI
Agence nationale de
la sécurité des
systèmes
d'information

NIST

National Institute of
Standards and Technology

SIEMENS

Ingenuity for life

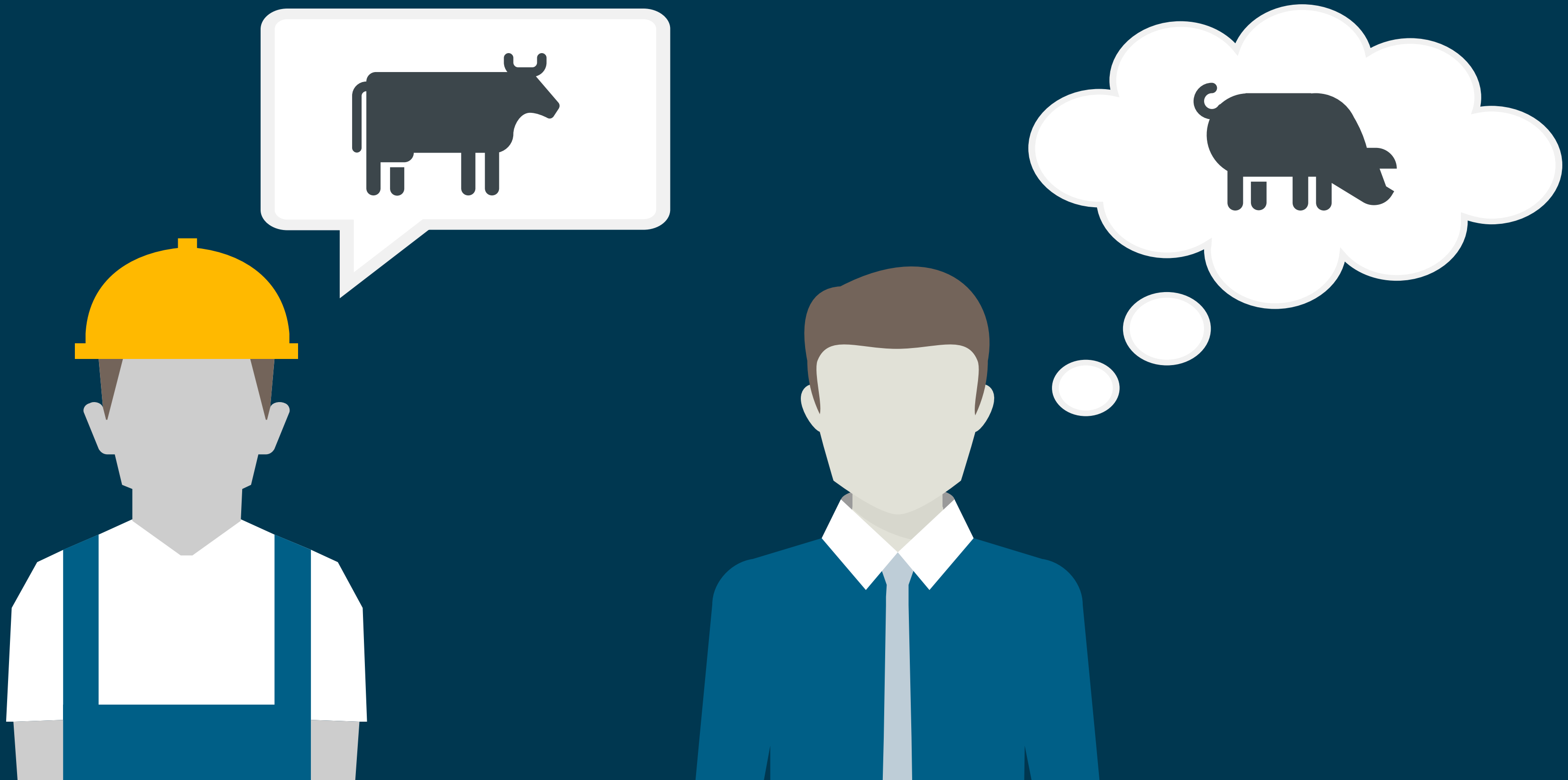
SIEMENS
Ingenuity for life

IEC 62443

From IEC62443

IEC 62443

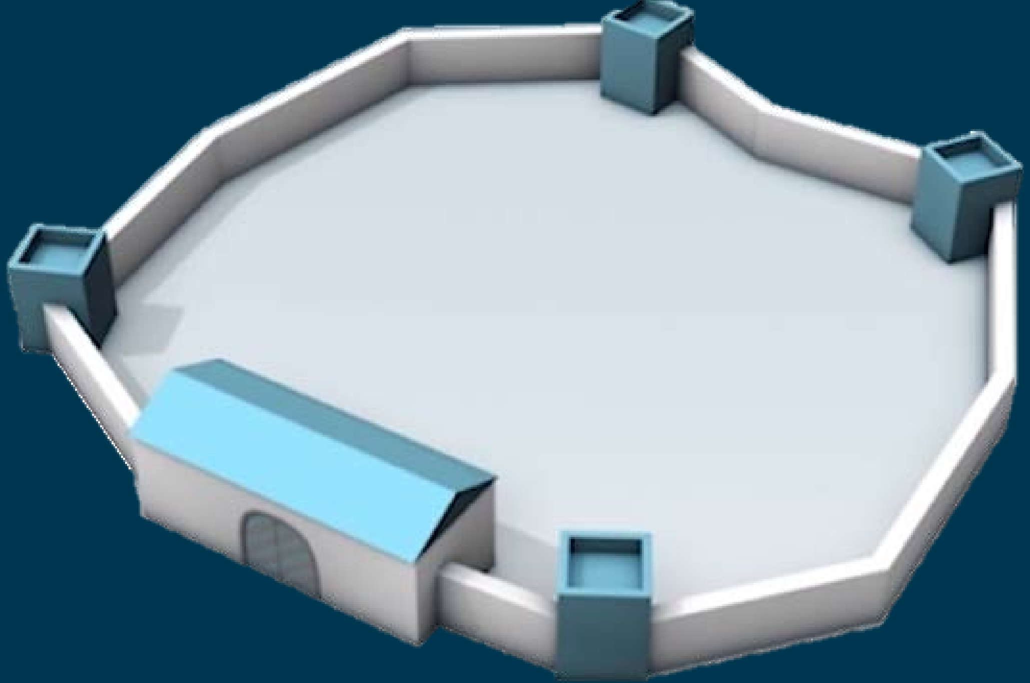
gives us the ability to **communicate** in an **unambiguous** way



SIEMENS
Ingenuity for life

IEC 62443

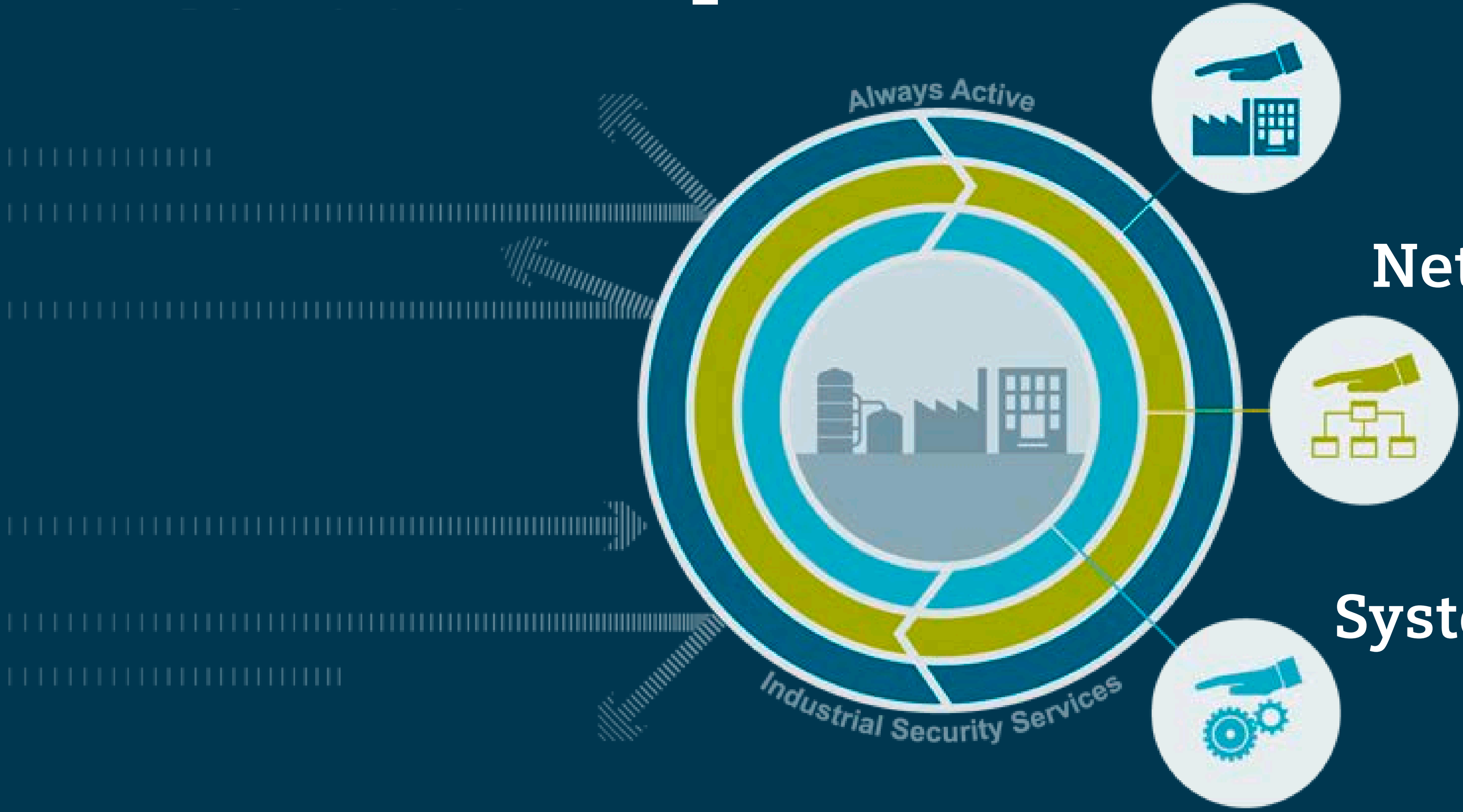
based on a **holistic** Defense in depth concept



IEC 62443

Defense in depth

SIEMENS
Ingenuity for life



Plant security

Network security

System integrity

Plant security

Plant Physical access protection

Processes and guidelines

Security service protecting production plants

Network security

Segmentation

Cell protection, DMZ and remote access

Firewall and VPN

Asset and Network Management

System integrity

System hardening

Authentication and user administration

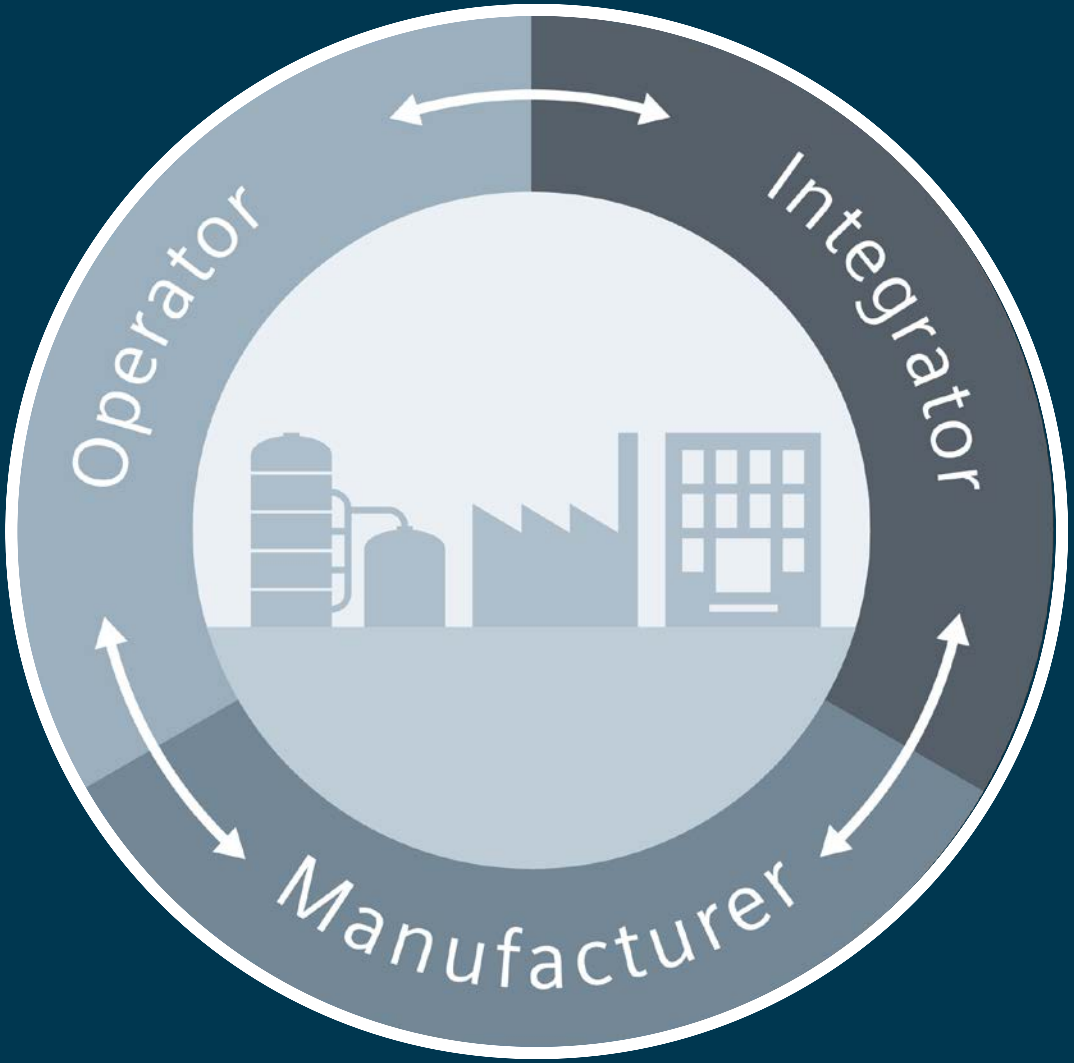
Patch management

Logging and Monitoring

Detection of attacks

IEC 62443

Focus on the **interfaces** between all stakeholders



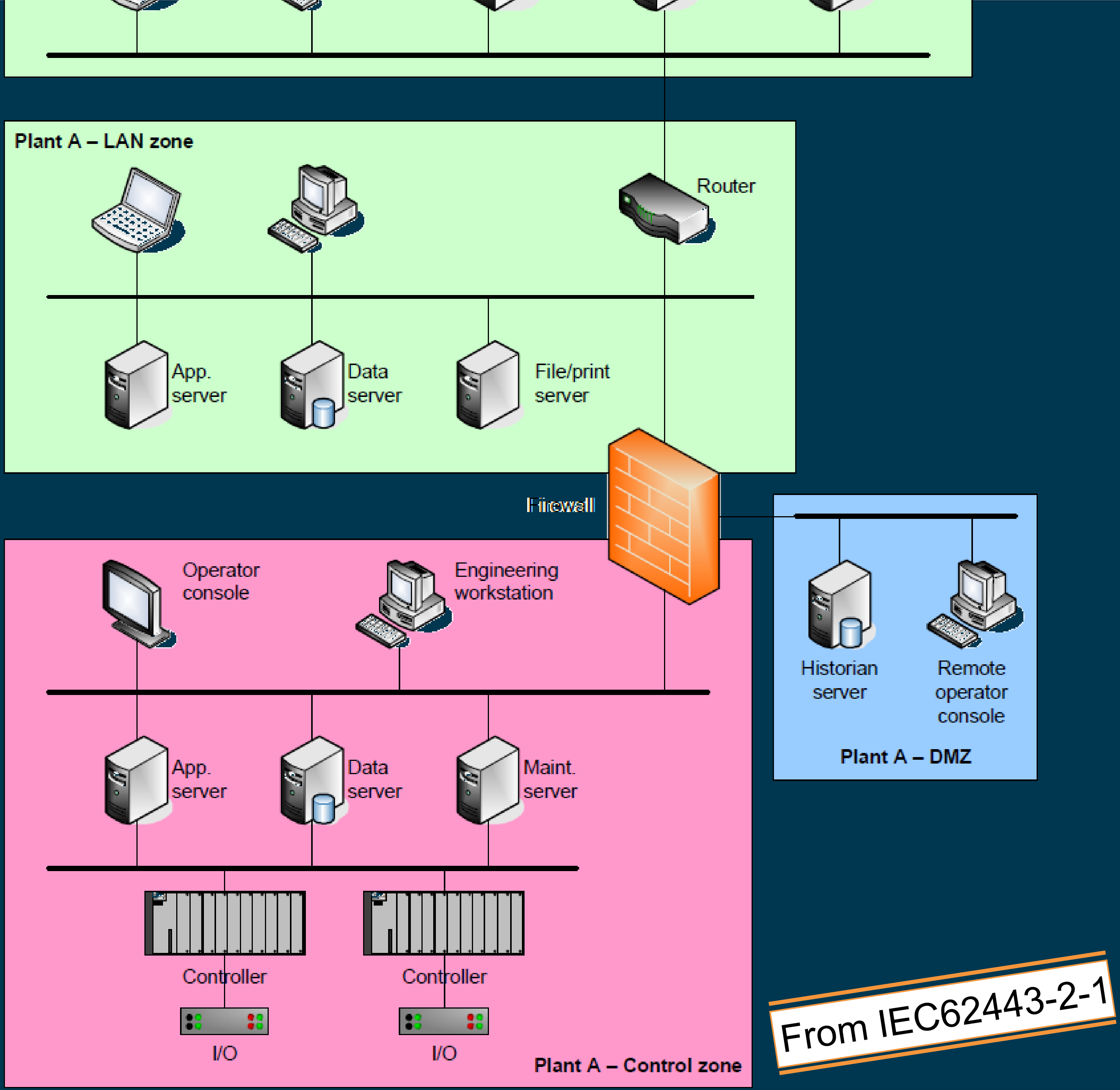
Operator, **Integrators**, and **Manufacturers**

IEC 62443

Is scalable

IEC 62443

provides system design guidelines



From IEC62443-2-1

IEC 62443

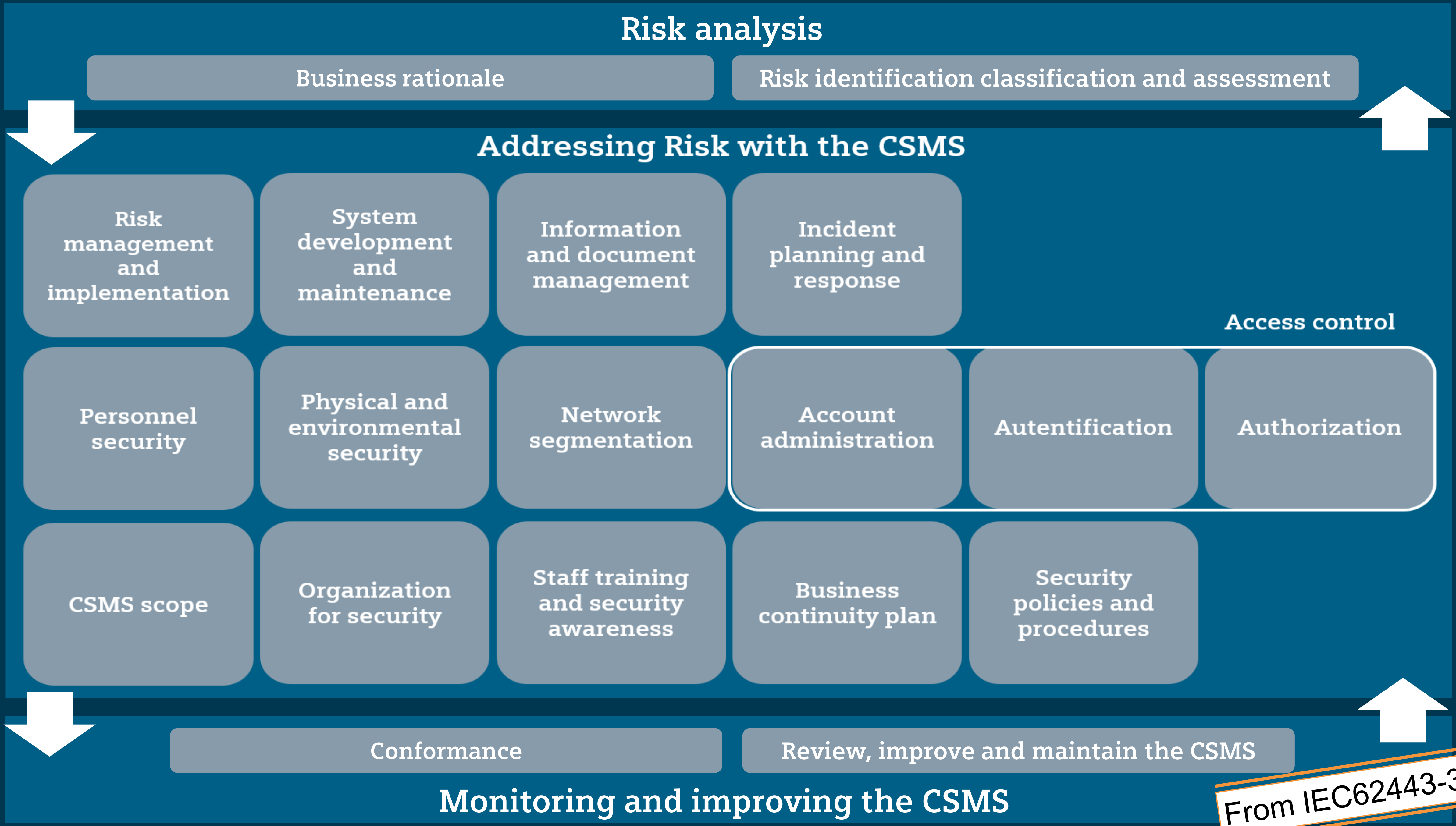
Addresses the entire **life cycle**

IEC 62443

provides a complete

Cyber Security Management System

From IEC62443-3-2



Risk analysis

Business rationale

Risk identification classification and assessment

Addressing Risk with the CSMS

Risk management and implementation

System development and maintenance

Information and document management

Incident planning and response

Access control

Personnel security

Physical and environmental security

Network segmentation

Account administration

Autentification

Authorization

CSMS scope

Organization for security

Staff training and security awareness

Business continuity plan

Security policies and procedures

Conformance

Review, improve and maintain the CSMS

Monitoring and improving the CSMS

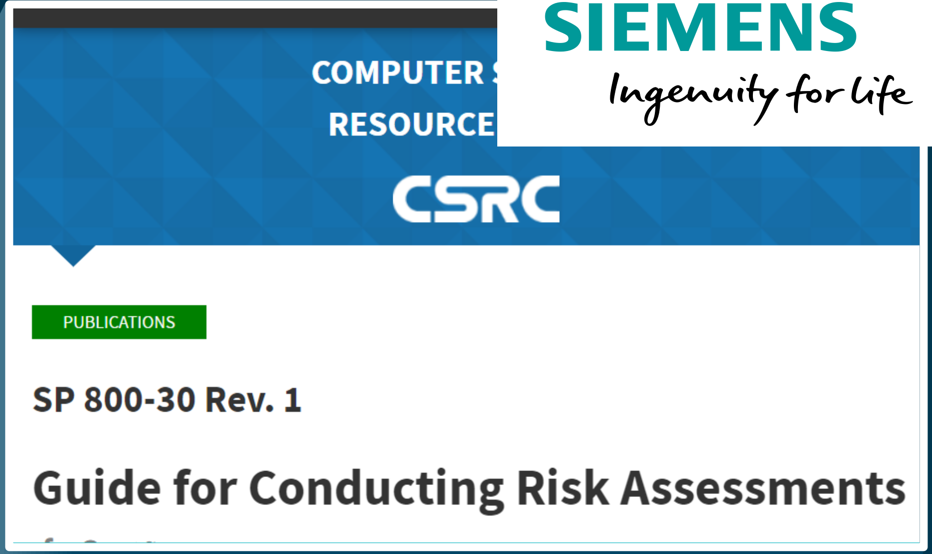
From IEC62443-3-2

SIEMENS
Ingenuity for life

Risk methods and frameworks

National Cyber Security Centre
a part of GCHQ

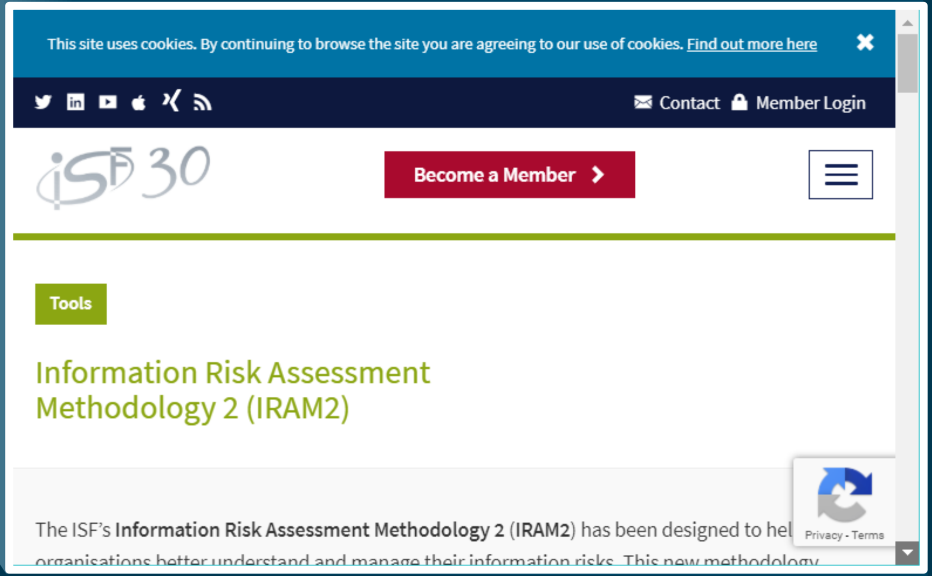
"A good overview"


COMPUTER S
RESOURCE
CSRC

PUBLICATIONS

SP 800-30 Rev. 1

Guide for Conducting Risk Assessments


This site uses cookies. By continuing to browse the site you are agreeing to our use of cookies. Find out more here ✖

Tools

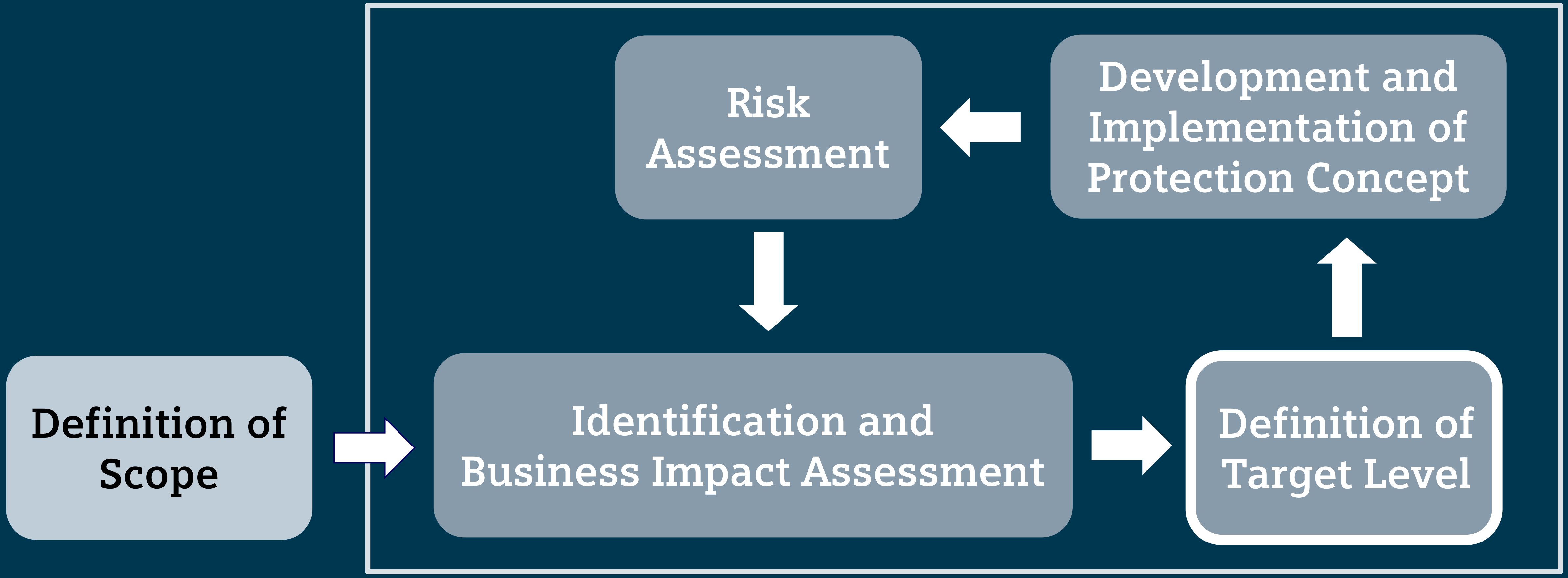
Information Risk Assessment Methodology 2 (IRAM2)

The ISF's **Information Risk Assessment Methodology 2** (IRAM2) has been designed to hel
organisations better understand and manage their information risks. This new methodology

More info: https://www.ncsc.gov.uk/collection/risk-management-collection/component-system-driven-approaches/understanding-component-driven-risk-management

Getting started

The IEC62443/ISO27001 based method



Definition of Scope

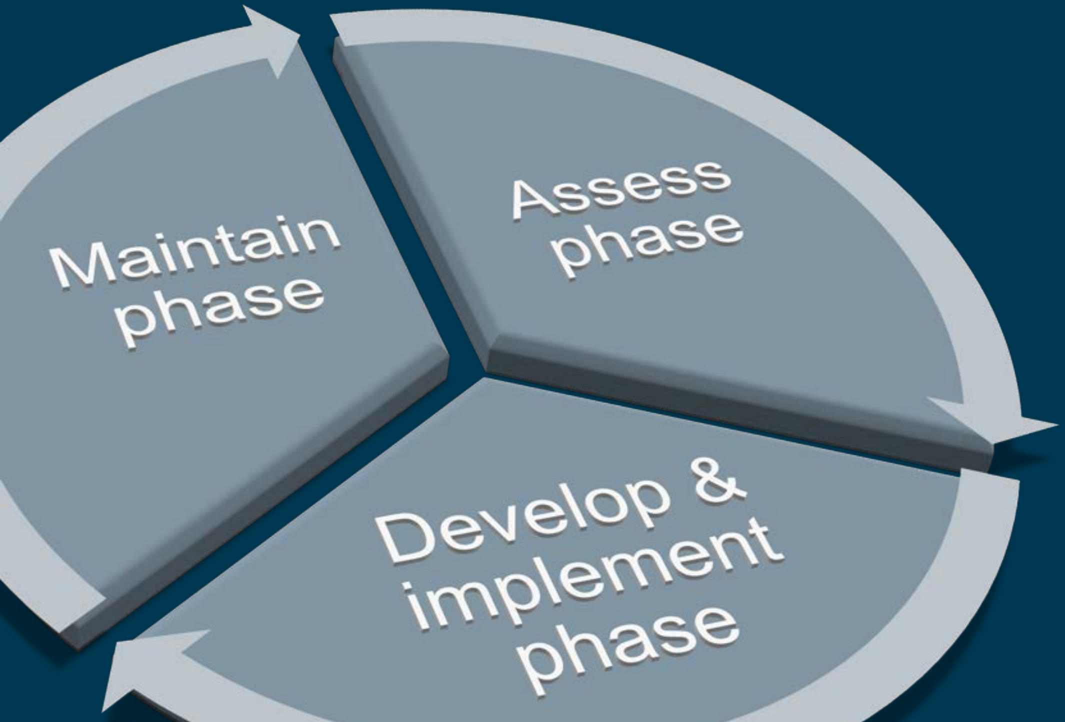
Identification and Business Impact Assessment

Definition of Target Level

Development and Implementation of Protection Concept

Risk Assessment

Cybersecurity
Life Cycle



SIEMENS
Ingenuity for life

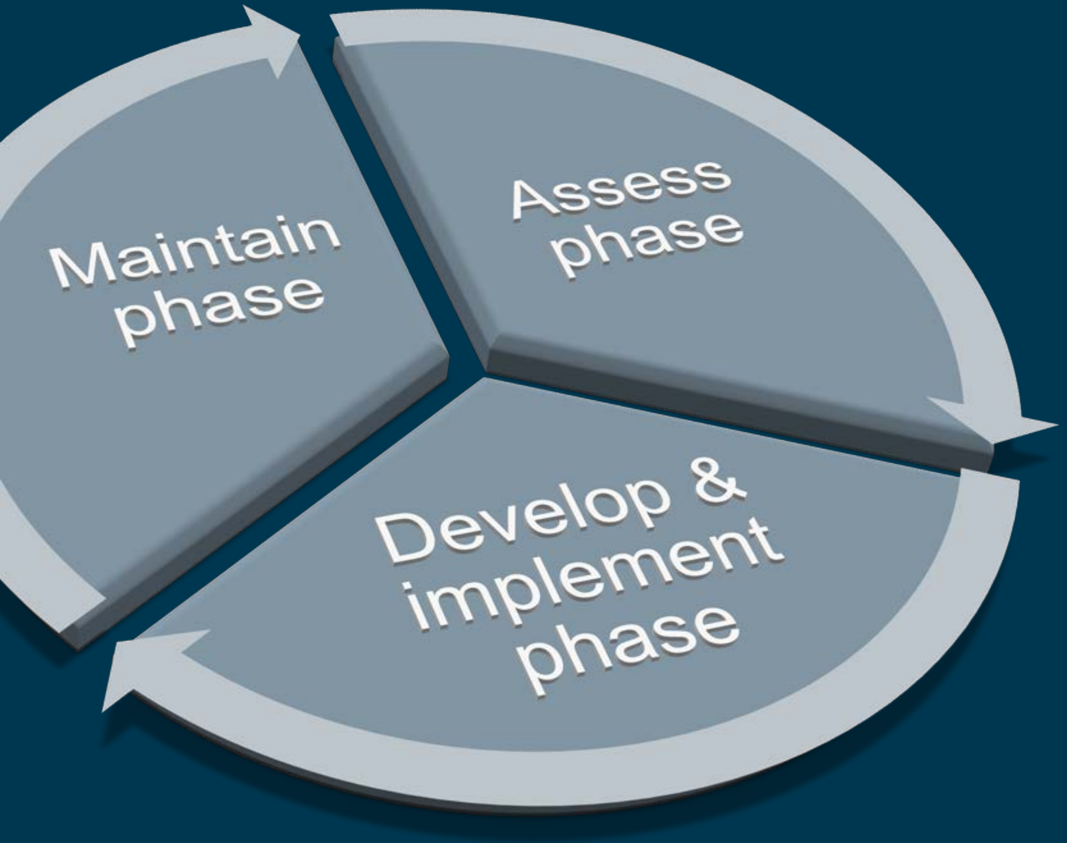
Assess phase

1. High-level Cyber Risk Assessment
2. Allocation of IACS Assets to Zones or Conduits
3. Detailed Cyber Risk Assessment

From IEC62443-3-2

Cybersecurity Life Cycle

SIEMENS
Ingenuity for life



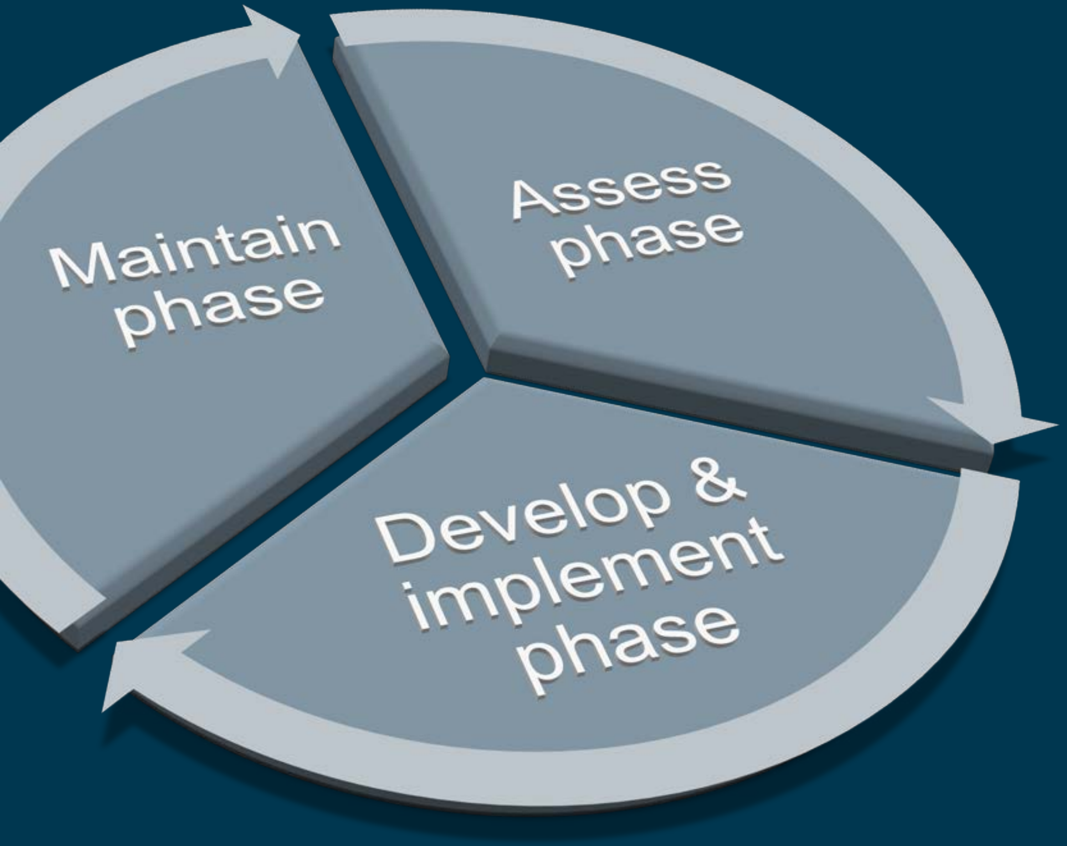
Develop & implement phase

4. Cybersecurity Requirements Specification
5. Design and Engineering of countermeasures or other means of risk reduction
6. Installation, commissioning and validation of countermeasures

From IEC62443-3-2

Cybersecurity
Life Cycle

SIEMENS
Ingenuity for life



Maintain phase

7. Maintenance, Monitoring and Management of change
8. Incident Response and Recovery

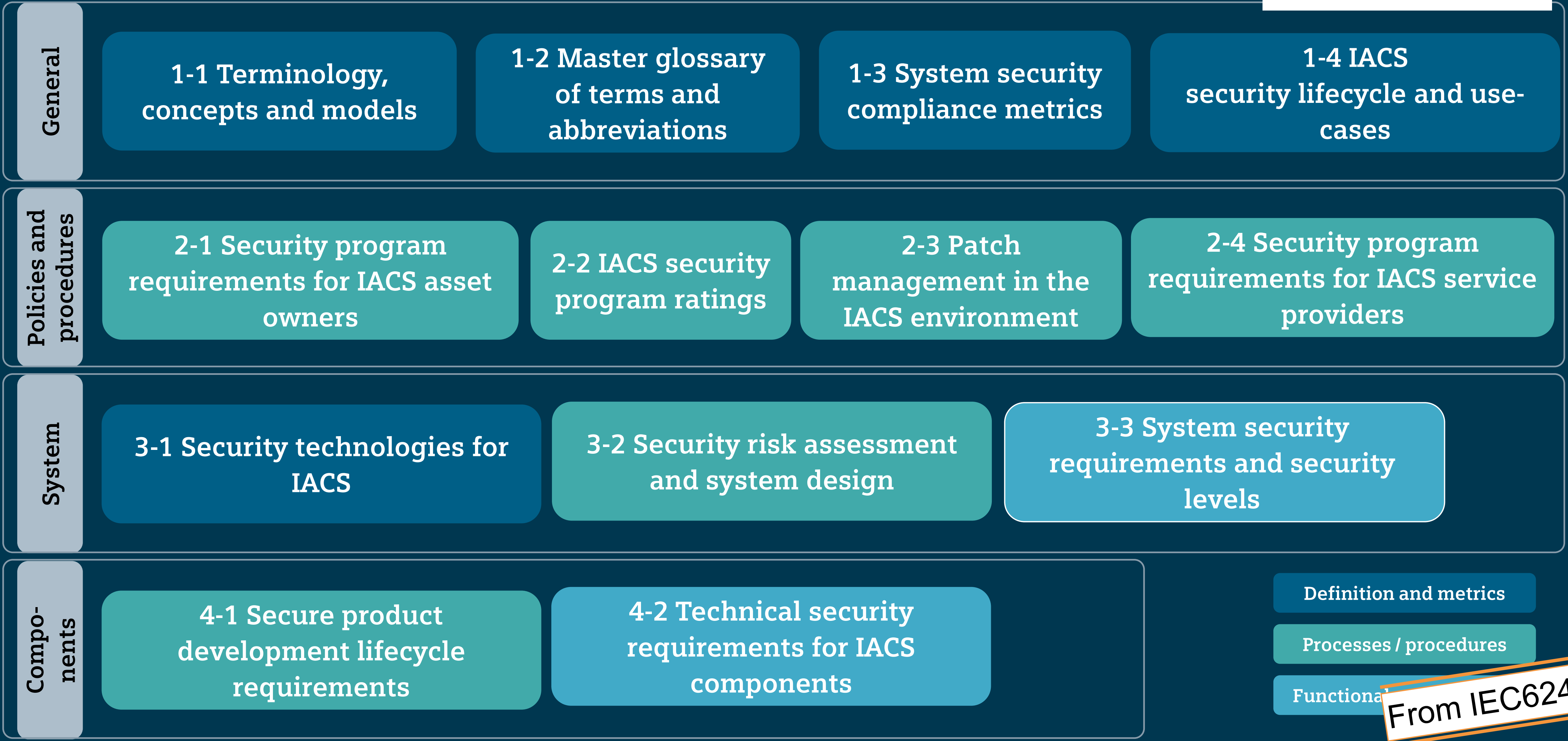
From IEC62443-3-2

The...

Standard

The structure of IEC 62443?

SIEMENS
Ingenuity for life



General	1-1 Terminology, concepts and models	1-2 Master glossary of terms and abbreviations	1-3 System security compliance metrics	1-4 IACS security lifecycle and use-cases
Policies and procedures	2-1 Security program requirements for IACS asset owners	2-2 IACS security program ratings	2-3 Patch management in the IACS environment	2-4 Security program requirements for IACS service providers
System	3-1 Security technologies for IACS	3-2 Security risk assessment and system design	3-3 System security requirements and security levels	
Compo-nents	4-1 Secure product development lifecycle requirements	4-2 Technical security requirements for IACS components		

Definition and metrics

Processes / procedures

Functiona

From IEC62443

Protection Levels are the key criteria and cover security **functionalities** and **processes**

Security process

- Based on IEC 62443-2-4 and ISO27001
- Maturity Level 1 - 4

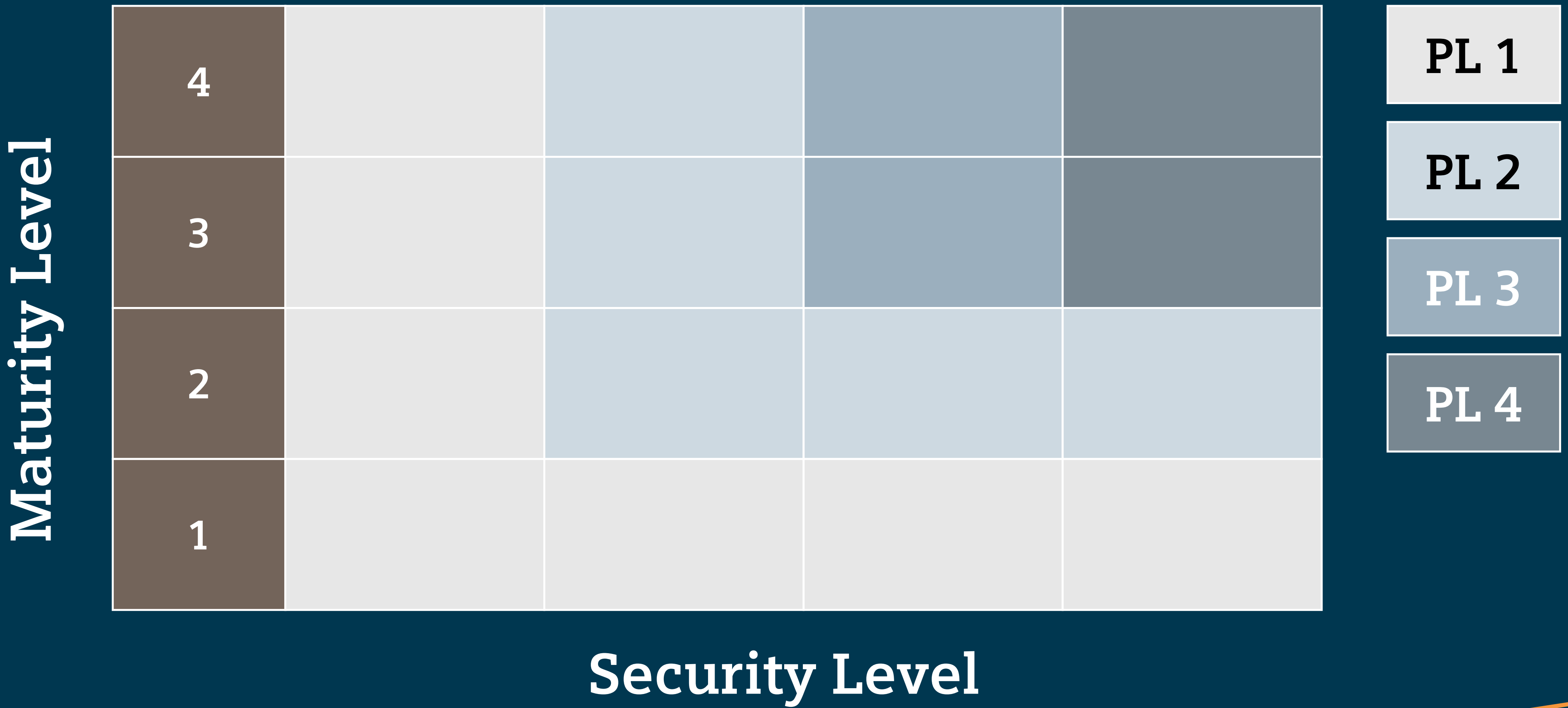
Protection Level (PL)

Security functions

- Based on IEC 62443-3-3
- Security Level 1 - 4

From IEC62443

Protection Levels are the key criteria and cover security **functionalities** and **processes**



From IEC62443

Protection Levels

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

From IEC62443

Consequences –
Some randomly selected points

SIEMENS
Ingenuity for life

PL 1	Use of VLAN, network hardening, managed switches and capability to backup are mandatory …
PL 2	A distributed Firewalls concept has to be implemented Inventory and Network Management are mandatory Capability to automate the backup are mandatory …
PL 3	Even more…
PL 4	Even way more…

From IEC62443

IEC 62443-3-3

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

Defines security requirements for industrial control systems

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

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

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

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

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				✓

From IEC62443-3-3

FR 5 – Restricted data flow
System Requirement Overview (Part 2)

SRs und REs	SL 1	SL 2	SL 3	SL 4
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

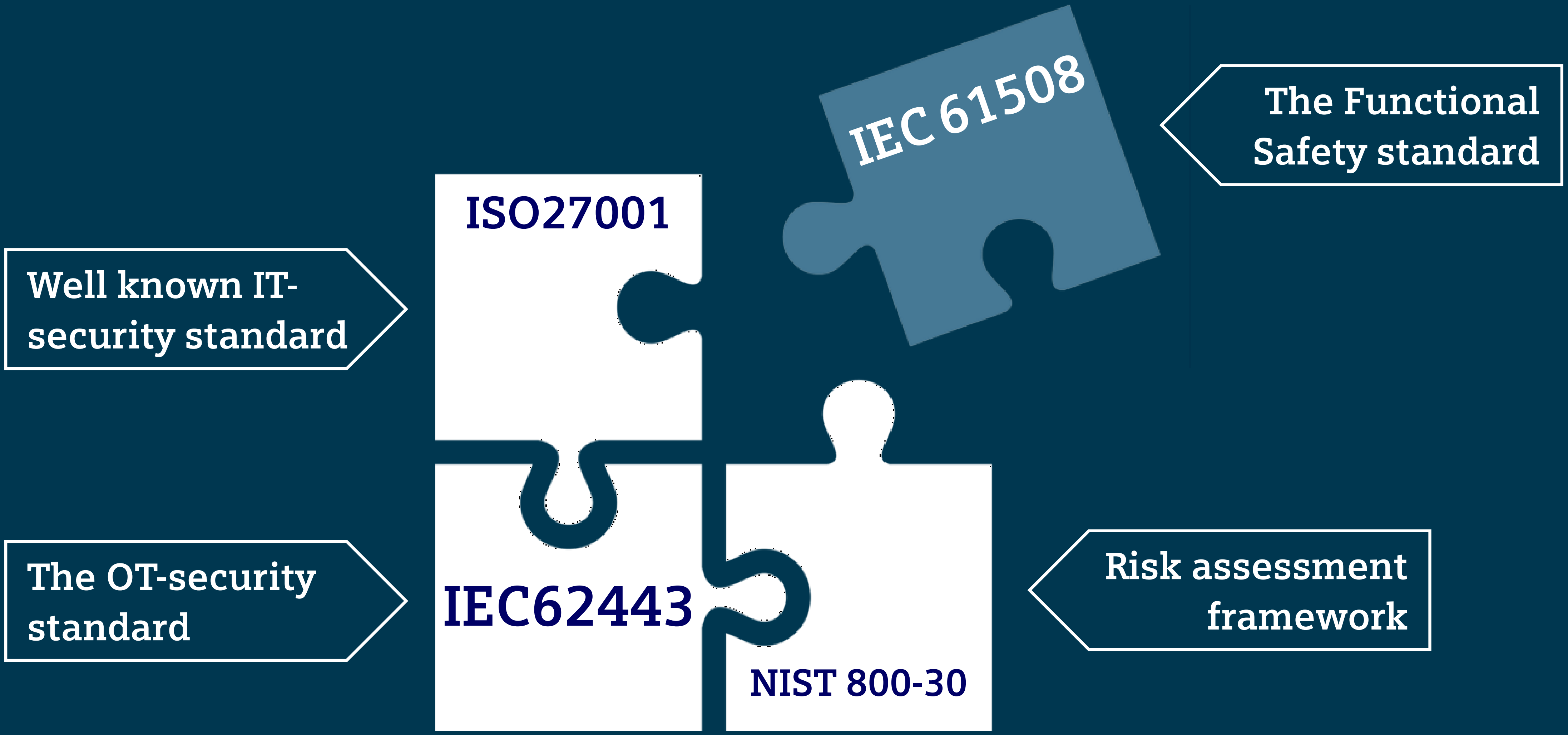
FR 7 – Resource availability
System Requirement Overview

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

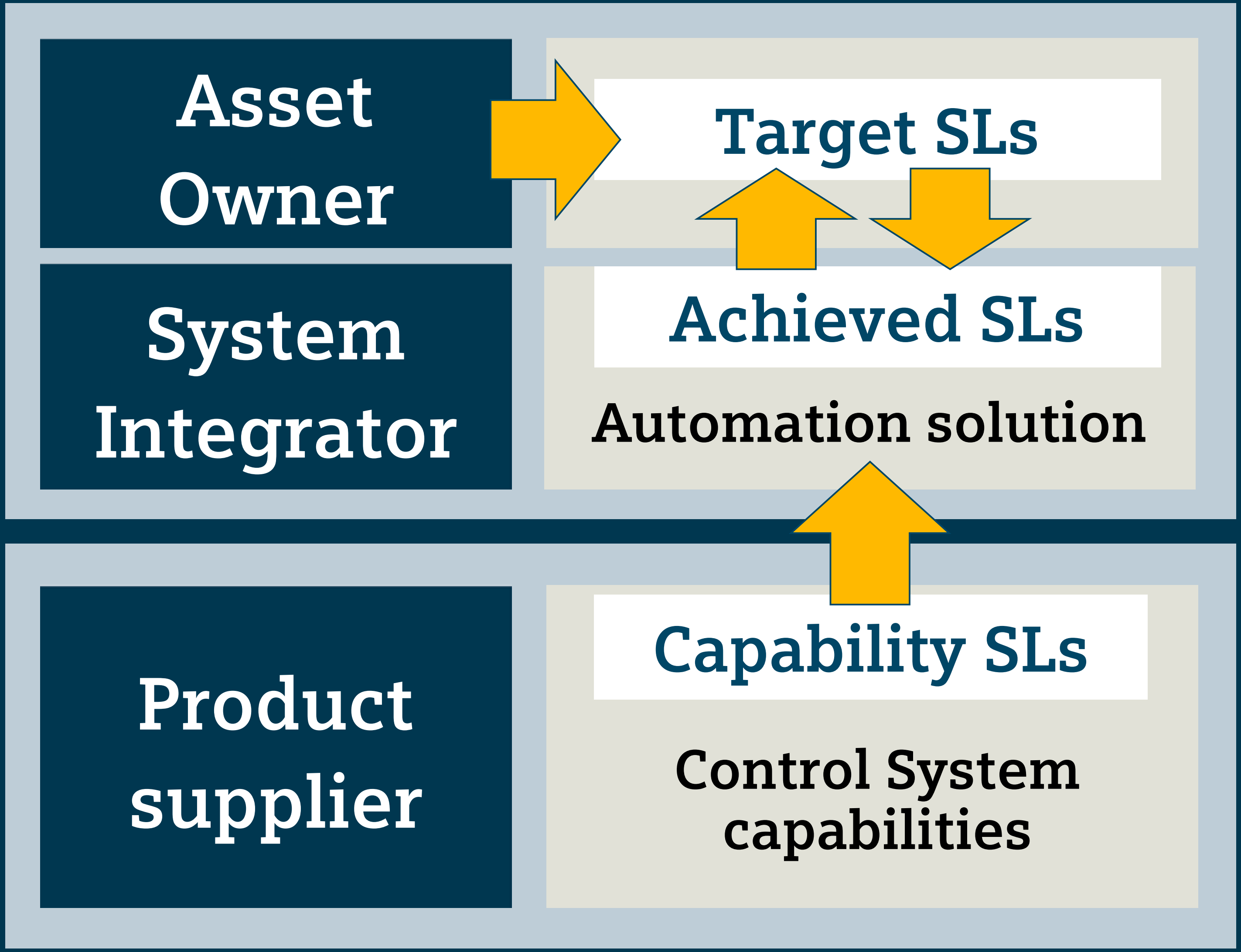
A piece of a **bigger picture**

SIEMENS
Ingenuity for life


IEC 61508
The Functional Safety standard
ISO27001
Well known IT-security standard
IEC62443
The OT-security standard
NIST 800-30
Risk assessment framework

Recap - Contributions of the stakeholders

SIEMENS
Ingenuity for life



Asset Owner

Target SLs

System Integrator

Achieved SLs

Automation solution

Product supplier

Capability SLs

Control System capabilities

IEC 62443

- 3-2 Security risk assessment and system design
- 3-3 System security requirements and Security levels
- 4-1 Product development requirements
- 4-2 Technical security requirements for IACS products

We are Certified !

Product development

Product life cycle management

Systems and network blueprints

Products

We are **Certified** !

Security assessments
Security design and consulting

The...

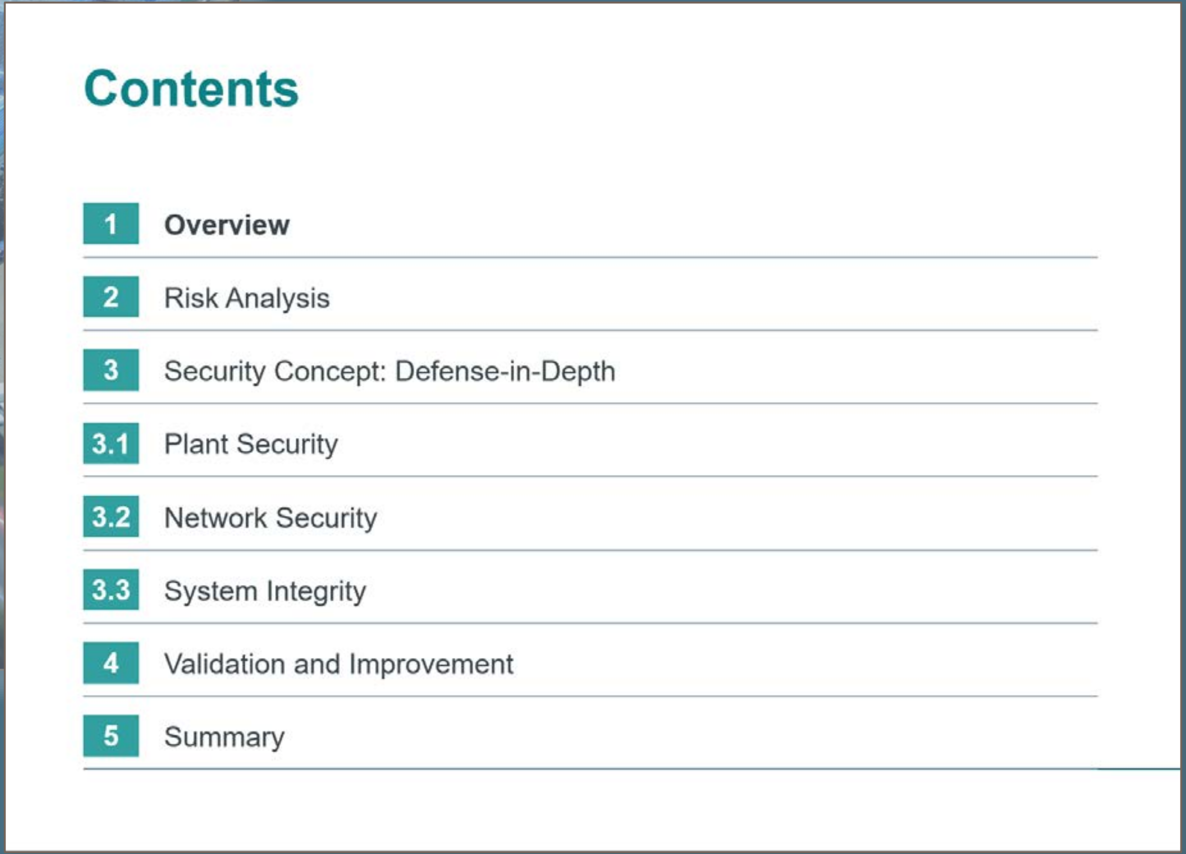
Operational Guidelines

Operational Guidelines for Industrial Security

Operational Guidelines for Industrial Security

Unrestricted © Siemens 2020

Version 2.1

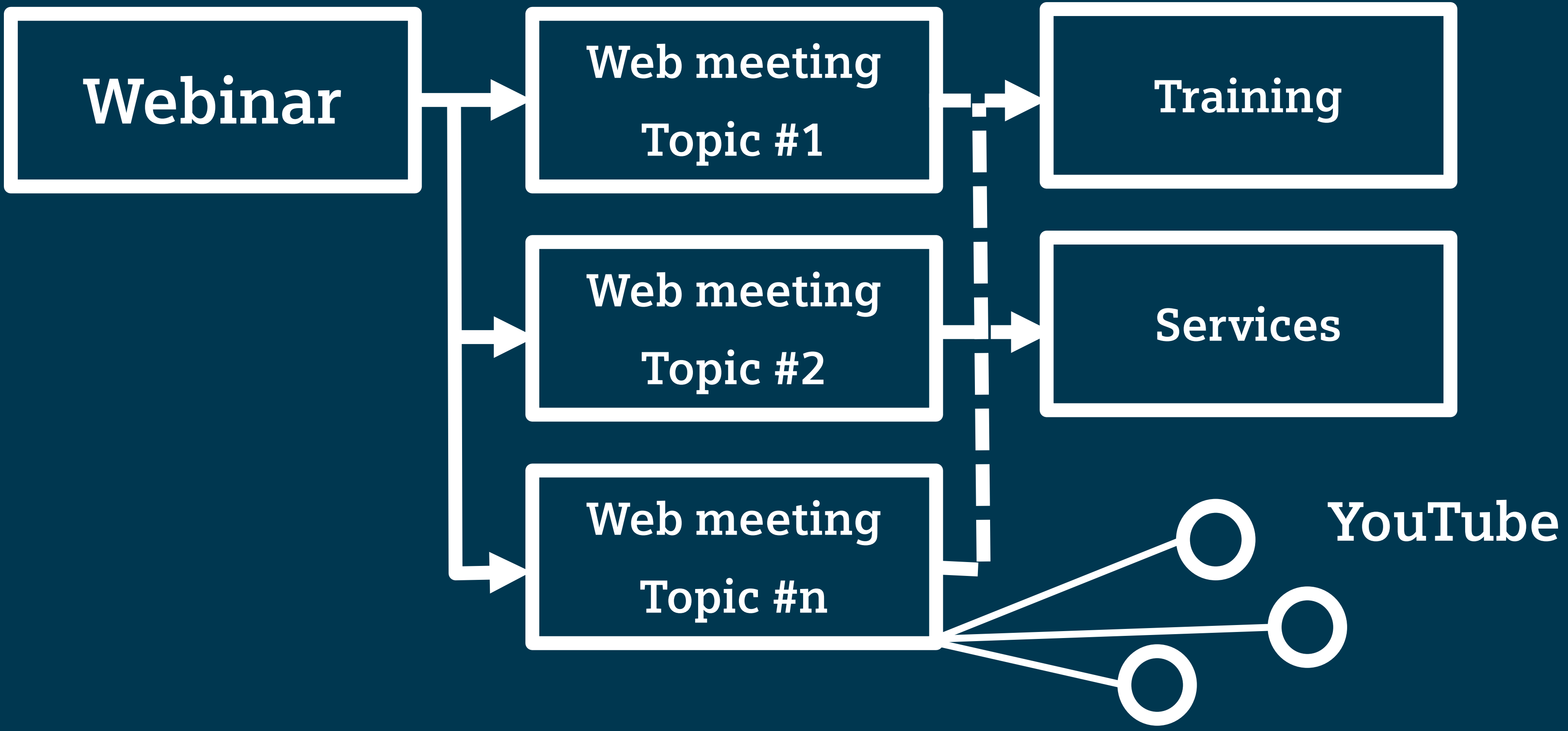


Contents

https://cert-portal.siemens.com/operational-guidelines-industrial-security.pdf

Way more information – **NO spam**...!

SIEMENS
Ingenuity for life


Webinar

Web meeting
Topic #1

Web meeting
Topic #2

Web meeting
Topic #n

Training

Services

YouTube

Getting **concrete**

Asset and
Network Management

Security Services

Product and system
Hardening

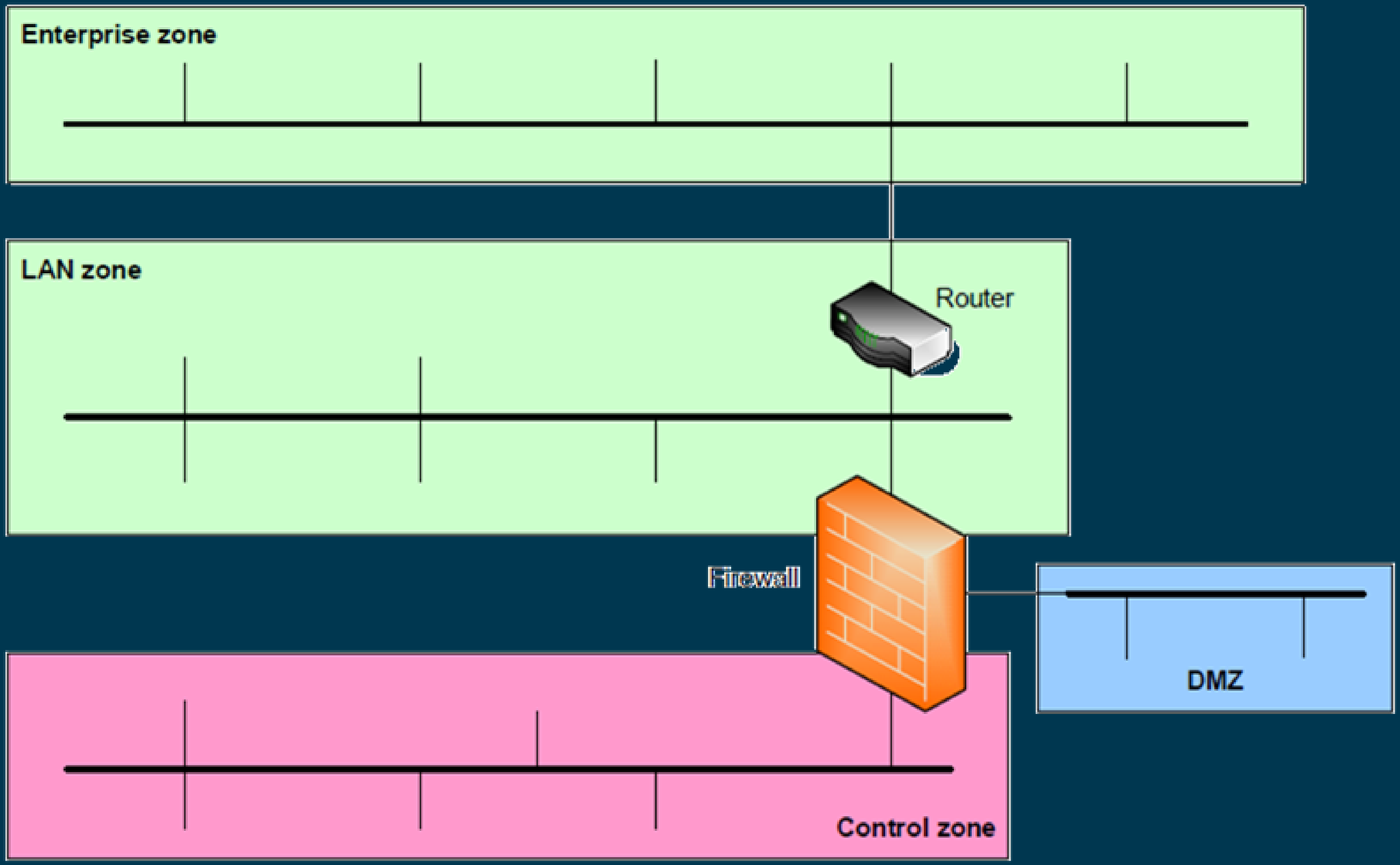
Segmentation and
Network design

Authentication
and User
Management

Patching and
Vulnerability Management

Segmentation and Network Designs

IEC 62443-3-2 **Generic Blueprint**

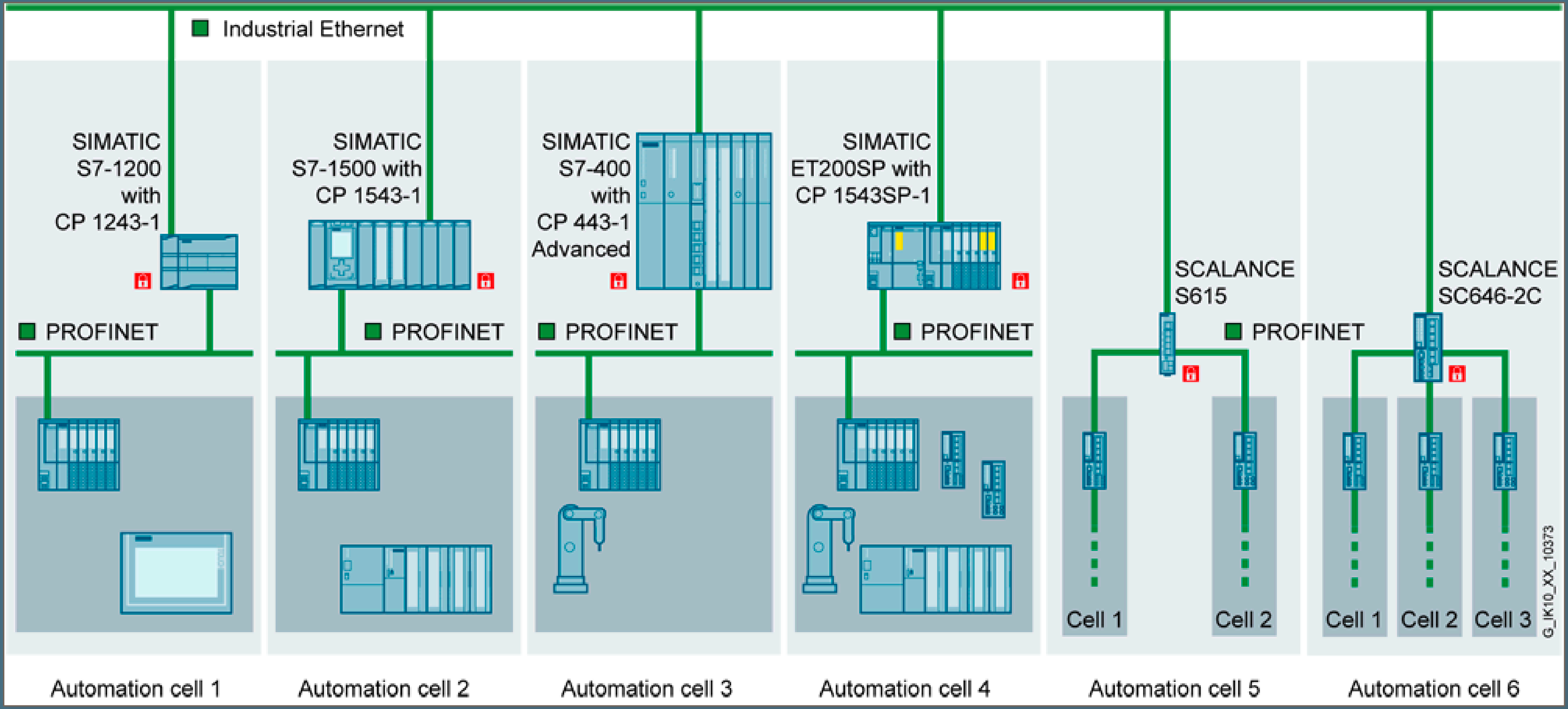


From IEC62443-3-2

Segmentation and cell protection

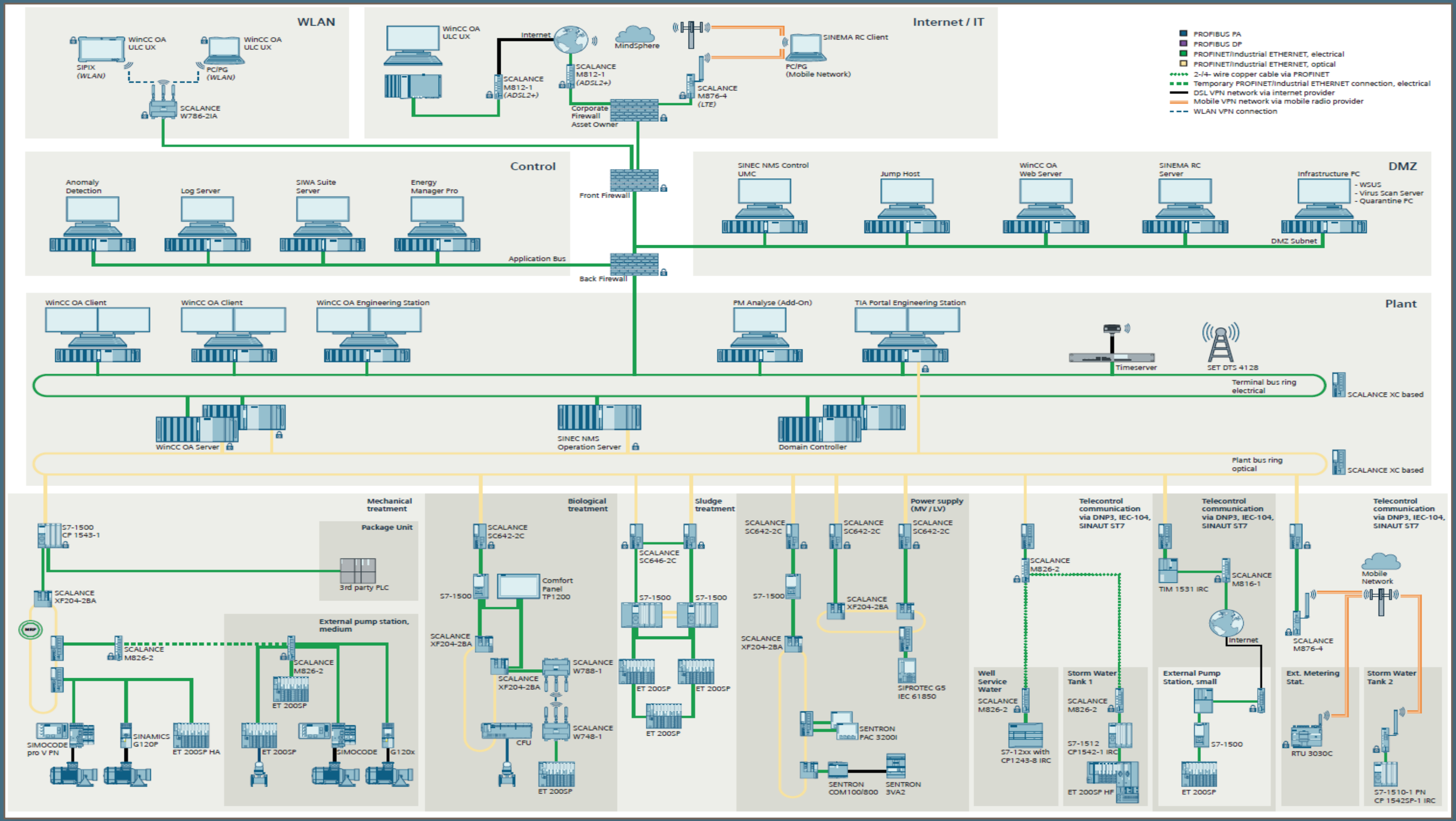
Zones and Conduits

SIEMENS
Ingenuity for life



IEC 62443-3-2 Certified Blueprint

SIEMENS
Ingenuity for life



How to handle

Patching and **Vulnerability Management**

Always **up to date**

SIEMENS
Ingenuity for life

https://new.siemens.com/global/en/products/services/cert.html#SecurityPublications

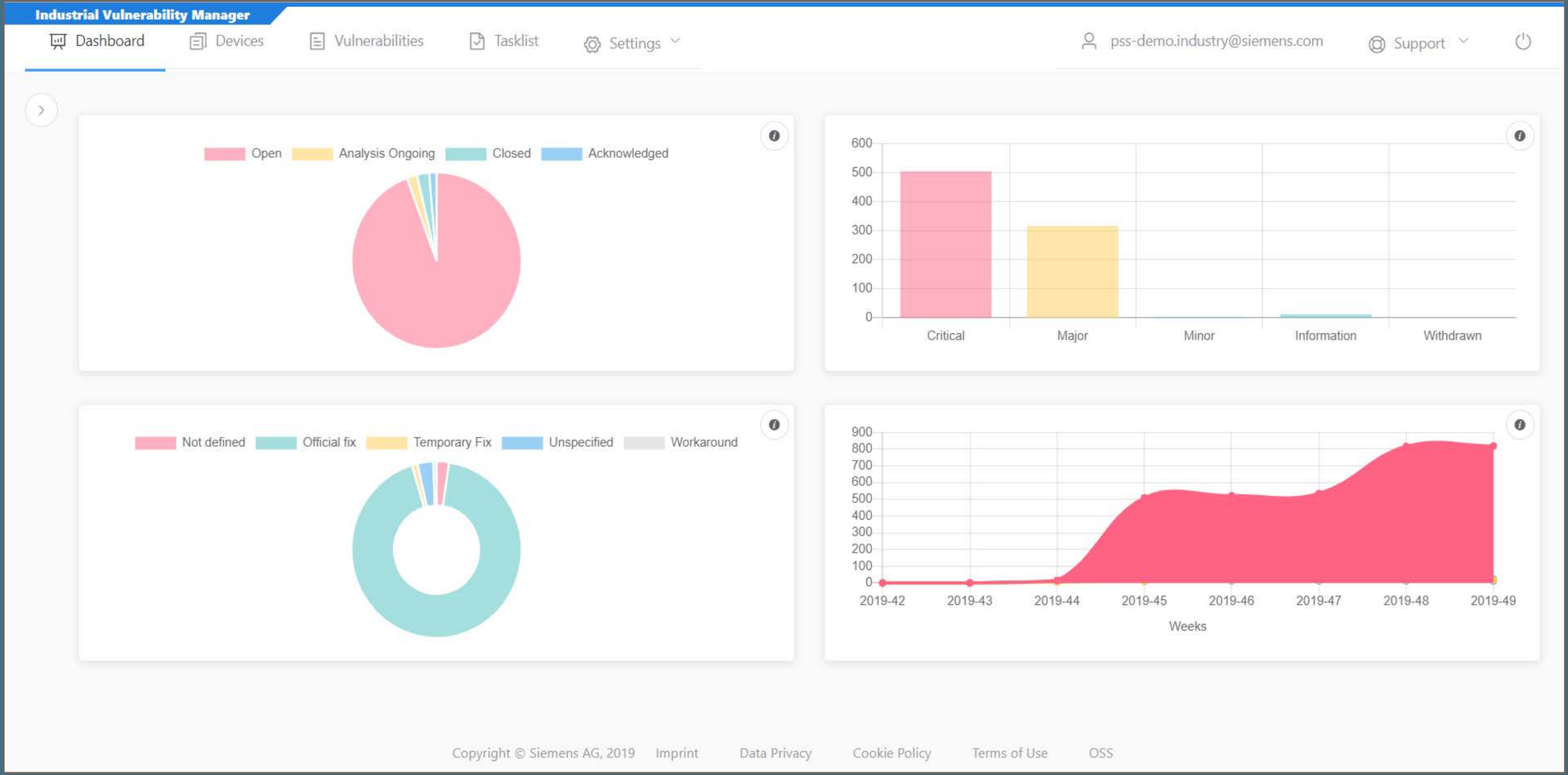
Patching and Vulnerability Management

Industrial Vulnerability Manager

SIEMENS
Ingenuity for life

Vulnerability Manager Report

Overview and Status of the Vulnerabilities
Confidential
Report generated on 2019-12-9
Based on Vulnerability database 2019-12-9



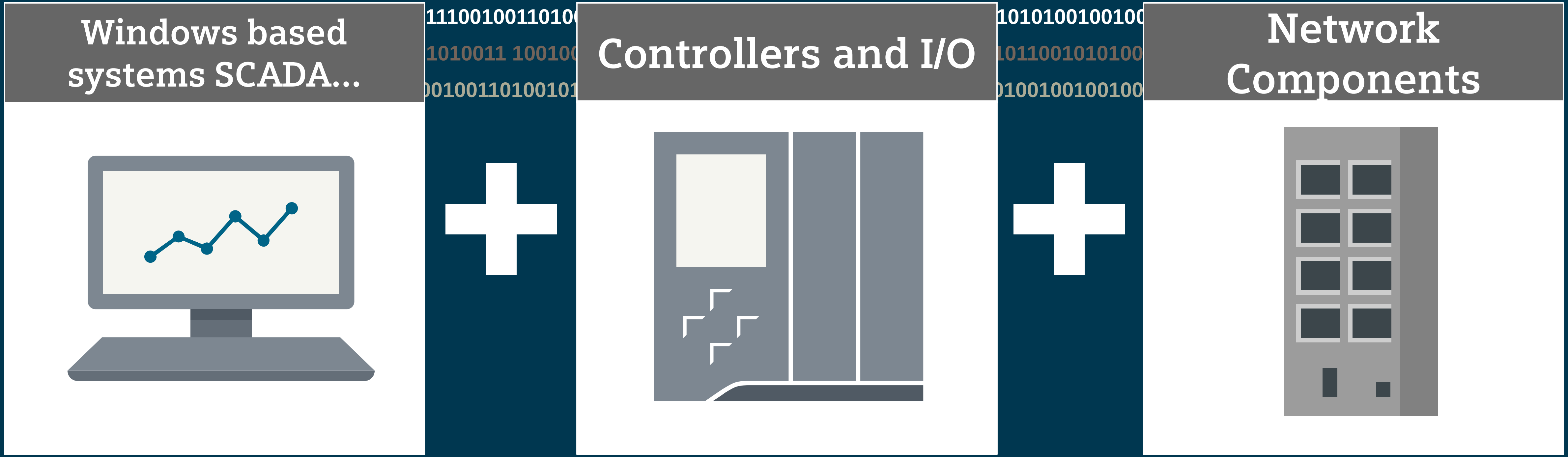
https://support.industry.siemens.com/cs/sc/4990/industrial-vulnerability-manager?lc=en-WW

Product and system

Hardening

Hardening

One size doesn't fit all



Windows based systems SCADA…

+

Controllers and I/O

+

Network Components

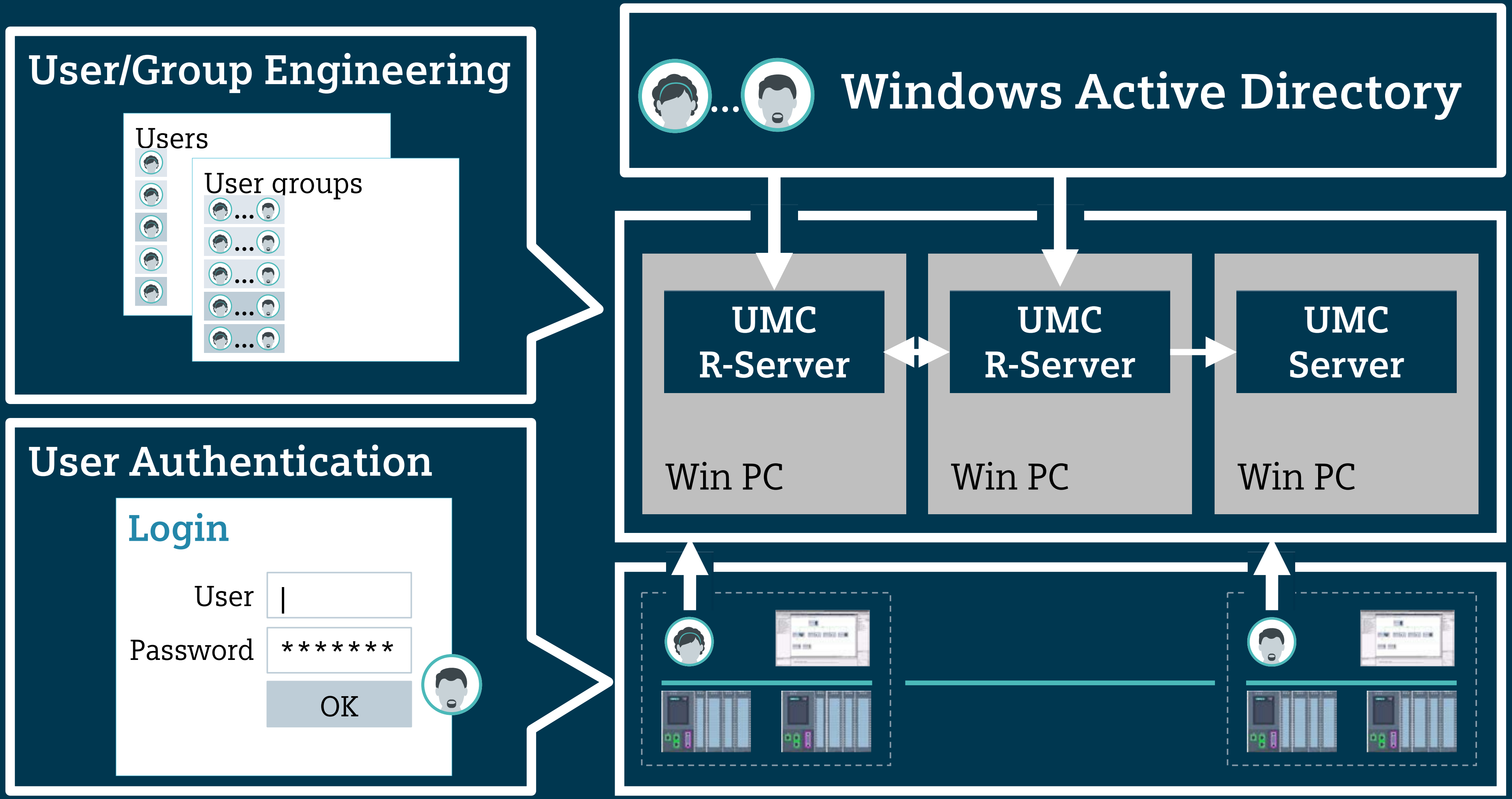
Authentication and User Management

Integrated Security engineering

UMC

Authentication and user administration in TIA-portal

SIEMENS
Ingenuity for life



User/Group Engineering

Users

User groups

User Authentication

Login

User |

Password *******

OK

Windows Active Directory

UMC R-Server

Win PC

UMC R-Server

Win PC

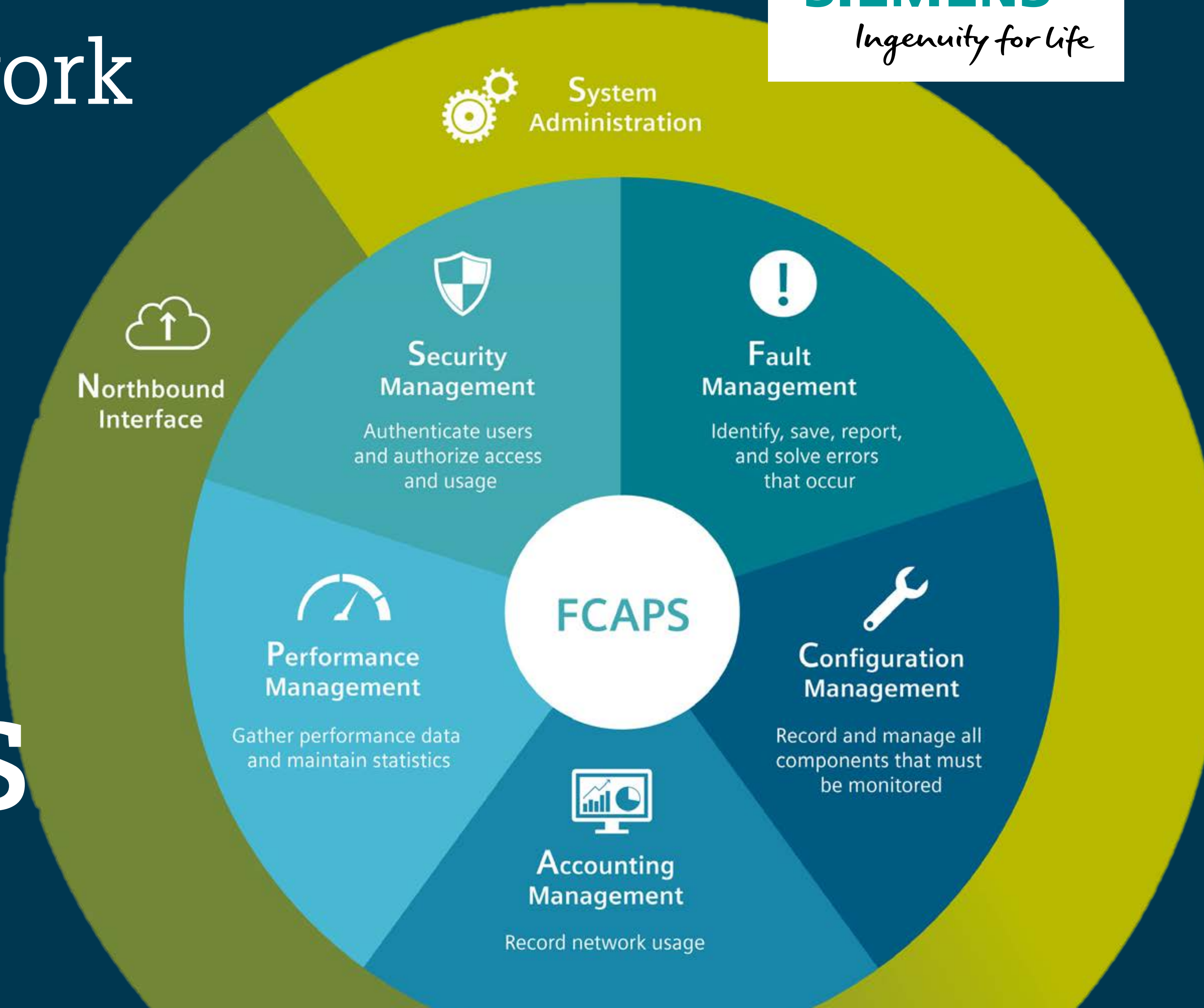
UMC Server

Win PC

Asset and Network Management

Asset and Network Management

SIEMENS
Ingenuity for life


System Administration
Northbound Interface
Security Management
Authenticate users and authorize access and usage
Fault Management
Identify, save, report, and solve errors that occur
FCAPS
Performance Management
Gather performance data and maintain statistics
Configuration Management
Record and manage all components that must be monitored
Accounting Management
Record network usage

SINEC NMS

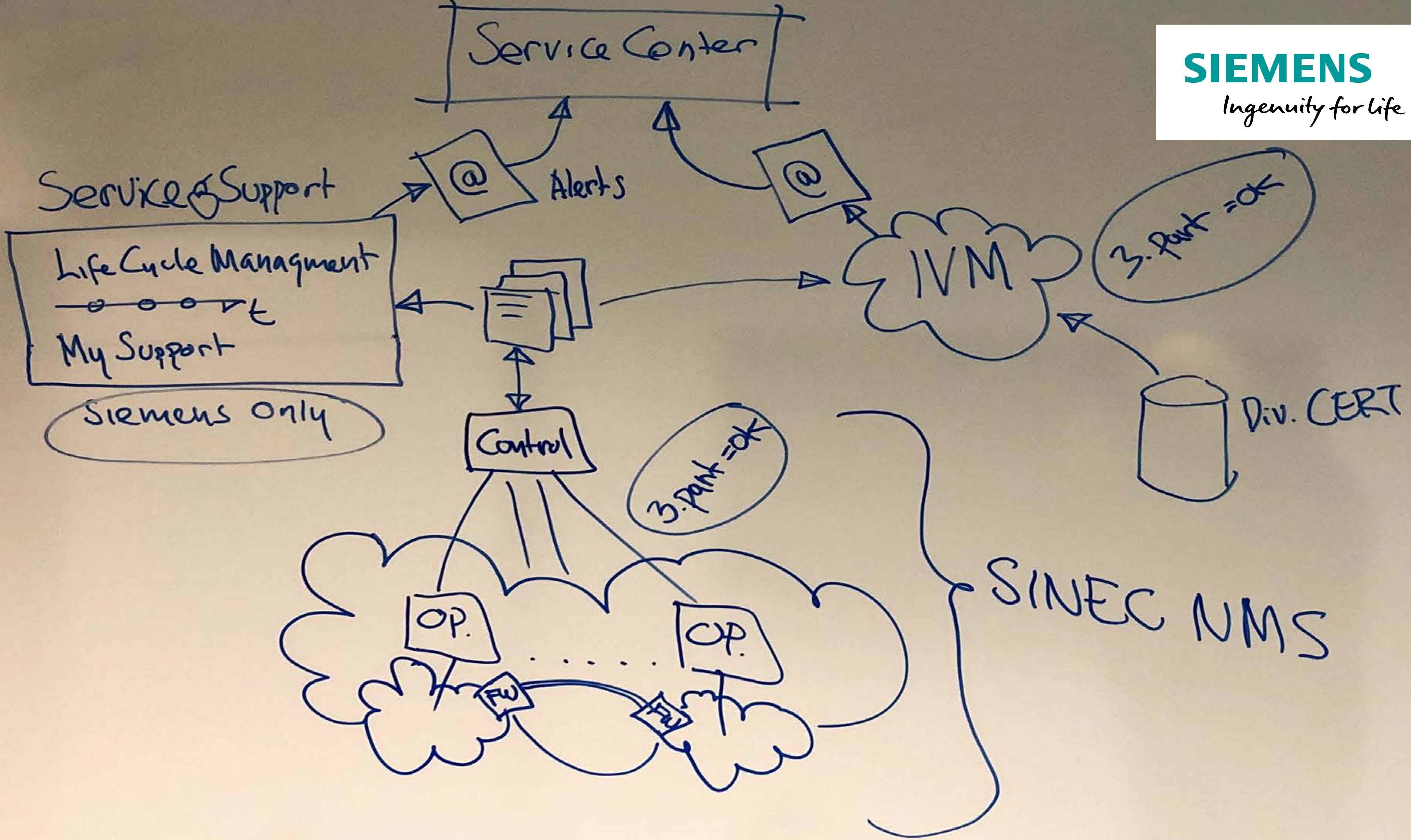
It’s a

system…

It’s a **standard**

SIEMENS

Ingenuity for life



Yderligere information

SIEMENS
Ingenuity for life

Gense webinar og download materiale på
www.siemens.dk/di-webinarer
Find tips og trick på YouTube

Kontakt

Per Krogh Christiansen
per.christiansen@siemens.com
Jesper Kristiansen
jesper.kristiansen@siemens.com
Morten Kromann
morten.kromann@siemens.com
Lars Peter Hansen
lars-peter.hansen@siemens.com

Security information

SIEMENS
Ingenuity for life

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.

SIEMENS
Ingenuity for life

www.siemens.dk/di-webinarer