Industrial Security

Vejen til implementering

Morten Kromann

SIEMENS

Safty IEC61508-1

7.4 Hazard and risk analysis

7.4.2.3 The hazards, hazardous events and hazardous situations of the EUC and the EUC control system shall be determined under all reasonably foreseeable circumstances (including fault conditions, reasonably foreseeable misuse and malevolent or unauthorised action). This shall include all relevant human factor issues, and shall give particular attention to abnormal or infrequent modes of operation of the EUC. If the hazard analysis identifies that malevolent or unauthorised action, constituting a security threat, as being reasonably foreseeable, then a security threats analysis should be carried out.

NOTE 1 For reasonably foreseeable misuse see 3.1.14 of IEC 61508-4.

NOTE 2 For guidance on hazard identification including guidance on representation and analysis of human factor issues, see reference [11] in the bibliography.

NOTE 3 For guidance on security risks analysis, see **IEC 62443 series.**

NOTE 4 Malevolent or unauthorised action covers security threats.

SIEMENS

Agenda

SIEMENS

Hvordan kommer man i gang?

SIEMENS

What are the drivers...?

Legislation

Productivity

Insurances

"Alm. Brand har sammenlignet med sidste år oplevet en stigning på 76 pct. i tegnede cyberforsikringer blandt deres erhvervskunder" *)

*)Kilde ING/VERSION2 30. aug. 2021

SIEMENS

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

NERC CIP

BDSG

WIB

ISO 27032

ISA 99

NIST

ANSSI

IEC 62443

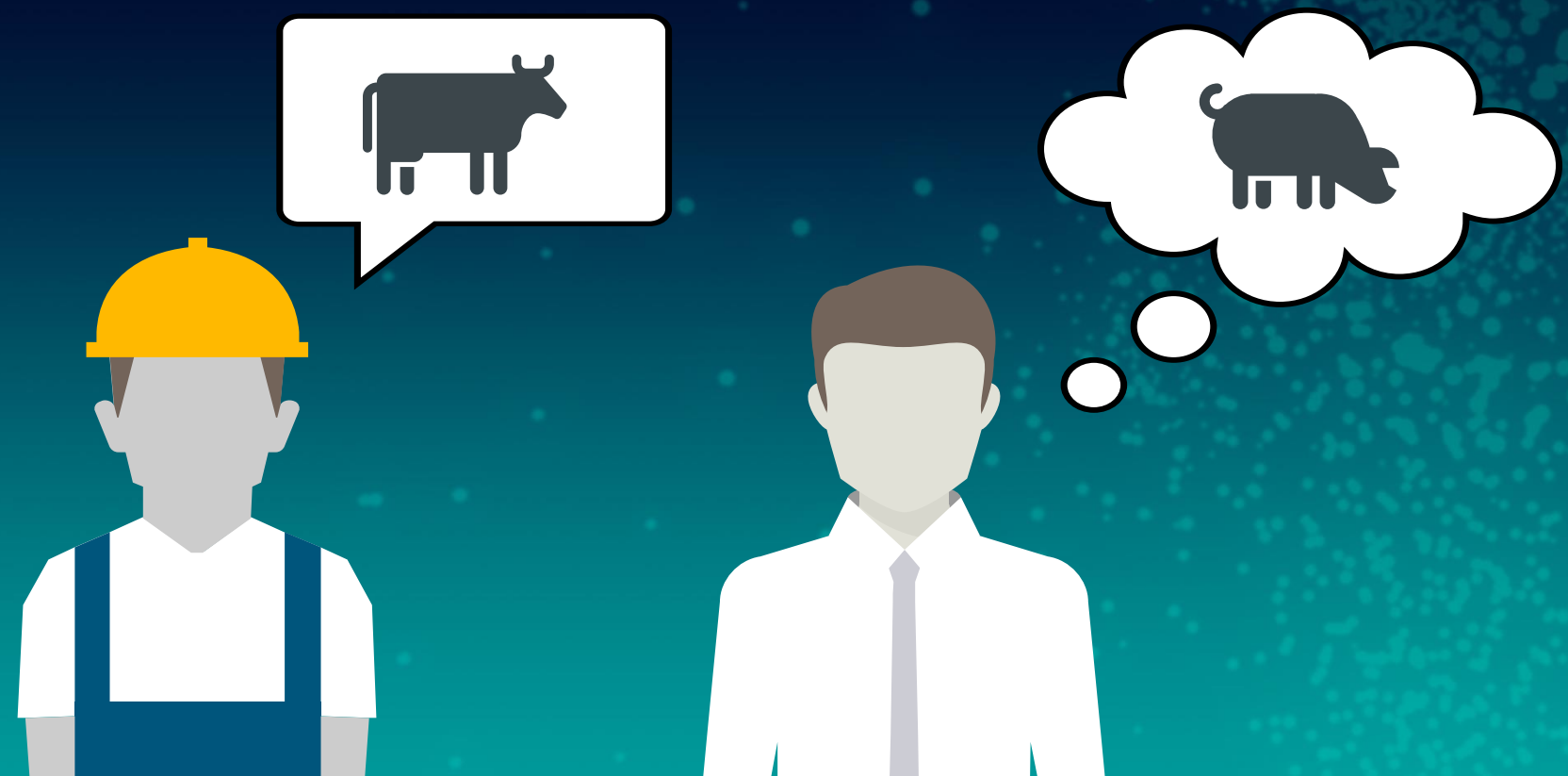
SIEMENS

IEC 62443

SIEMENS

IEC 62443

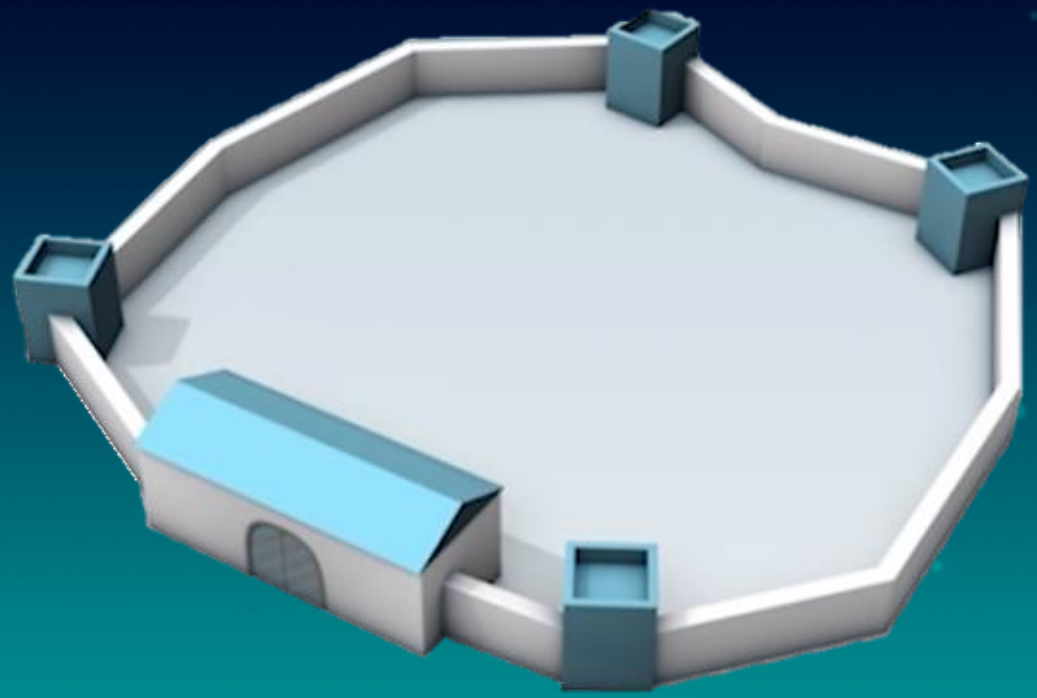
gives us the ability to **communicate**
in an **unambiguous** way



SIEMENS

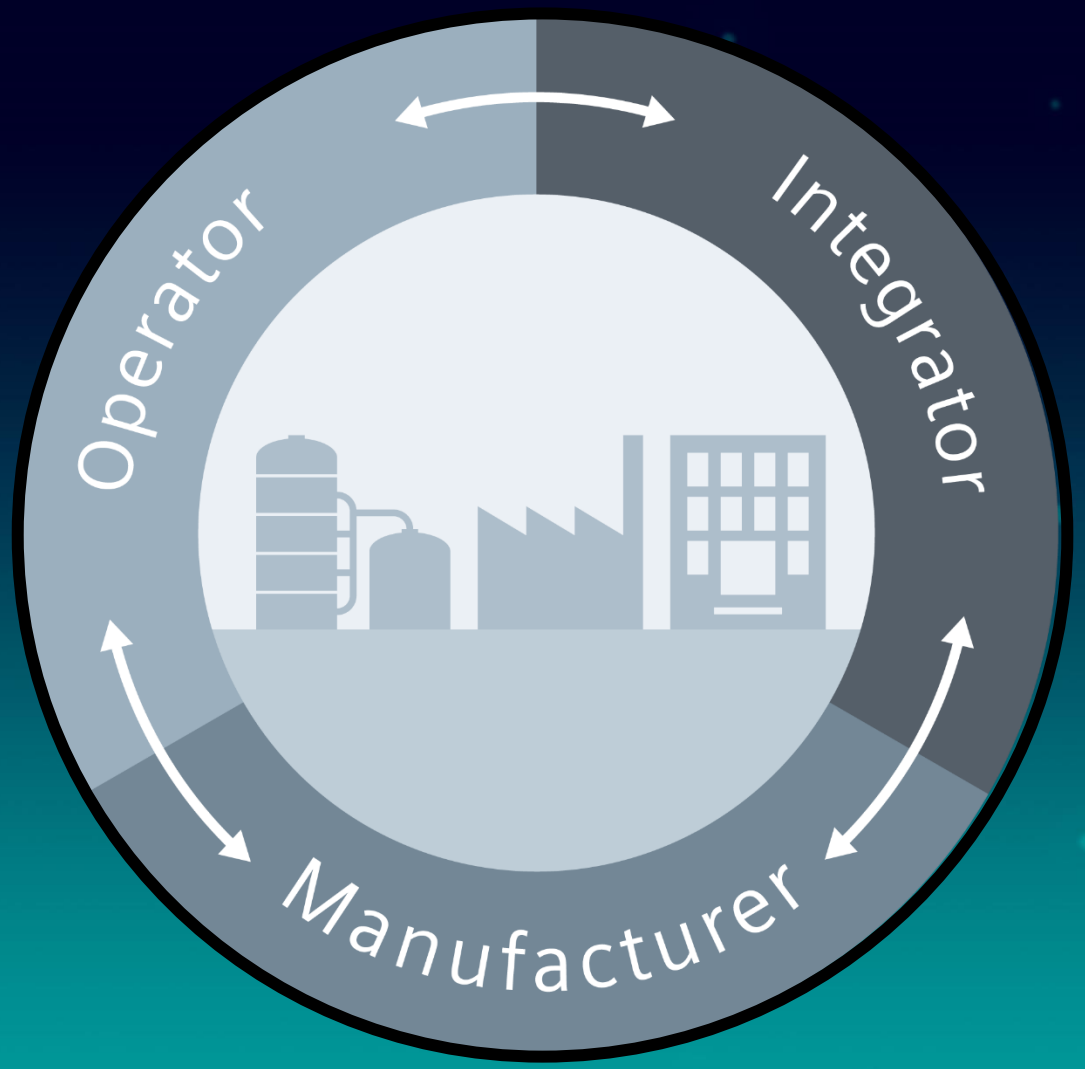
IEC 62443

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



SIEMENS

IEC 62443



Focus on the **interfaces** between all stakeholders

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

SIEMENS

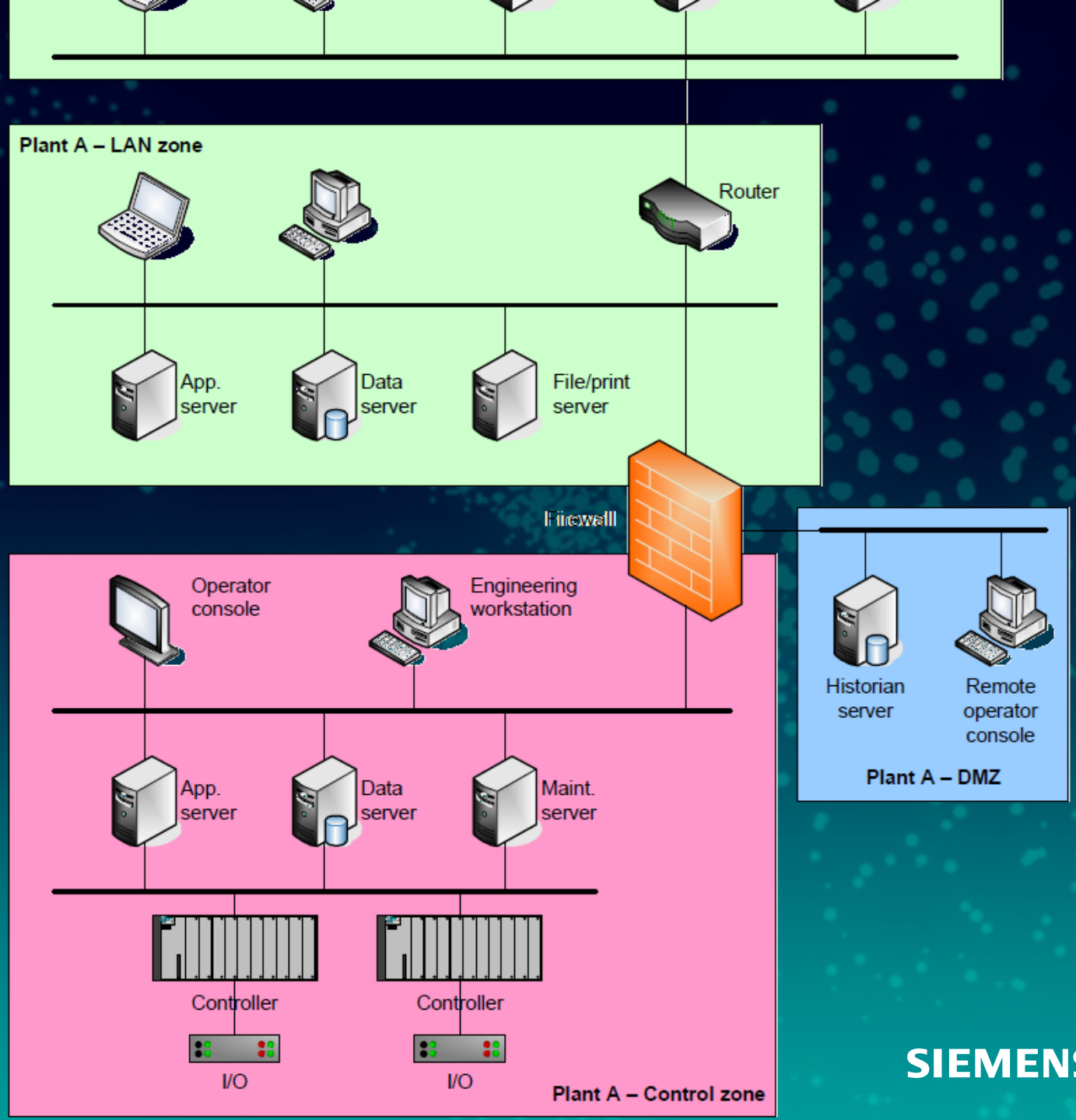
IEC 62443

Is **scalable**

SIEMENS

IEC 62443

provides system design guidelines



SIEMENS

IEC 62443

Addresses the entire **life cycle**

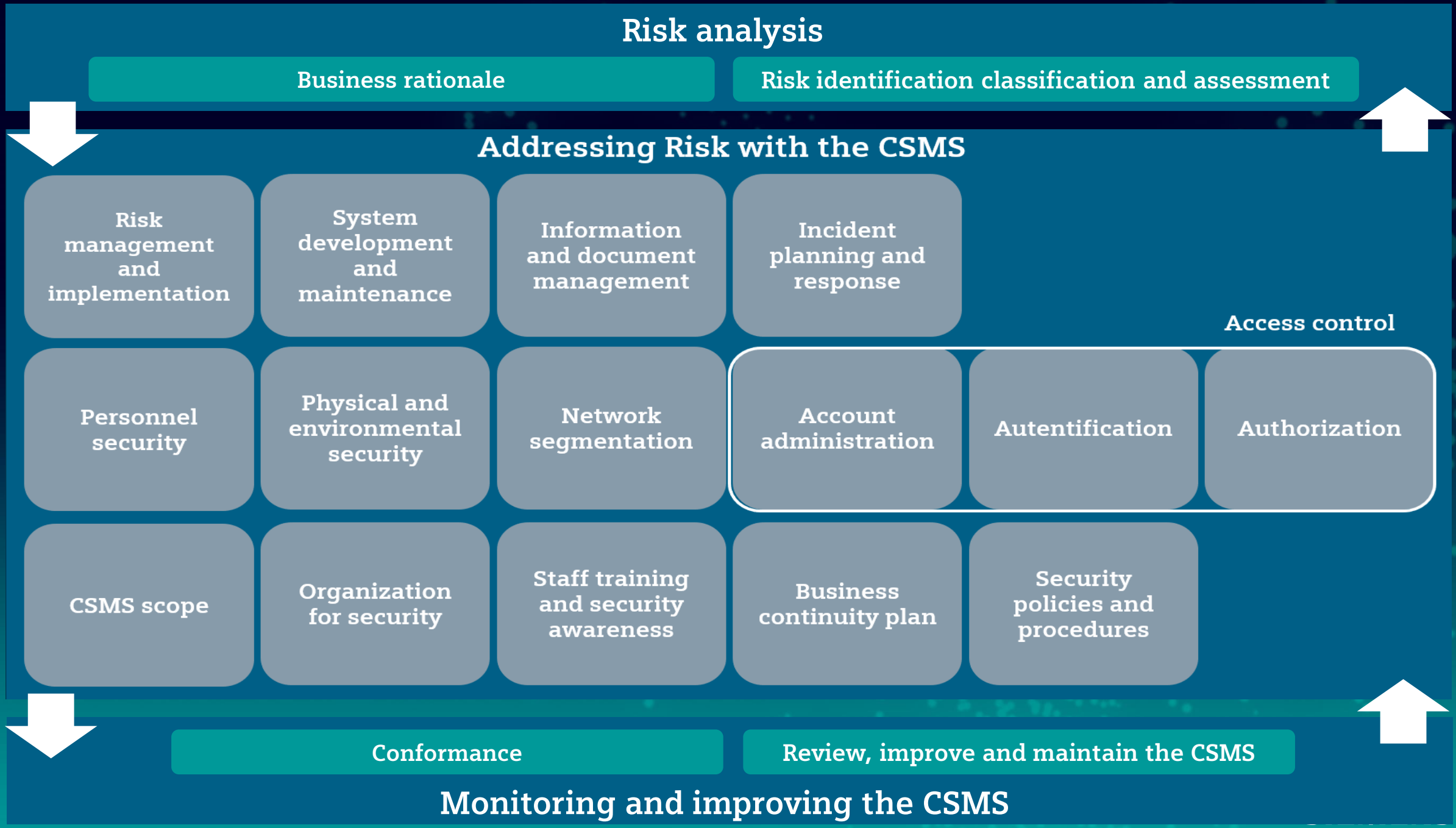
SIEMENS

IEC 62443

provides a complete

Cyber Security Management System

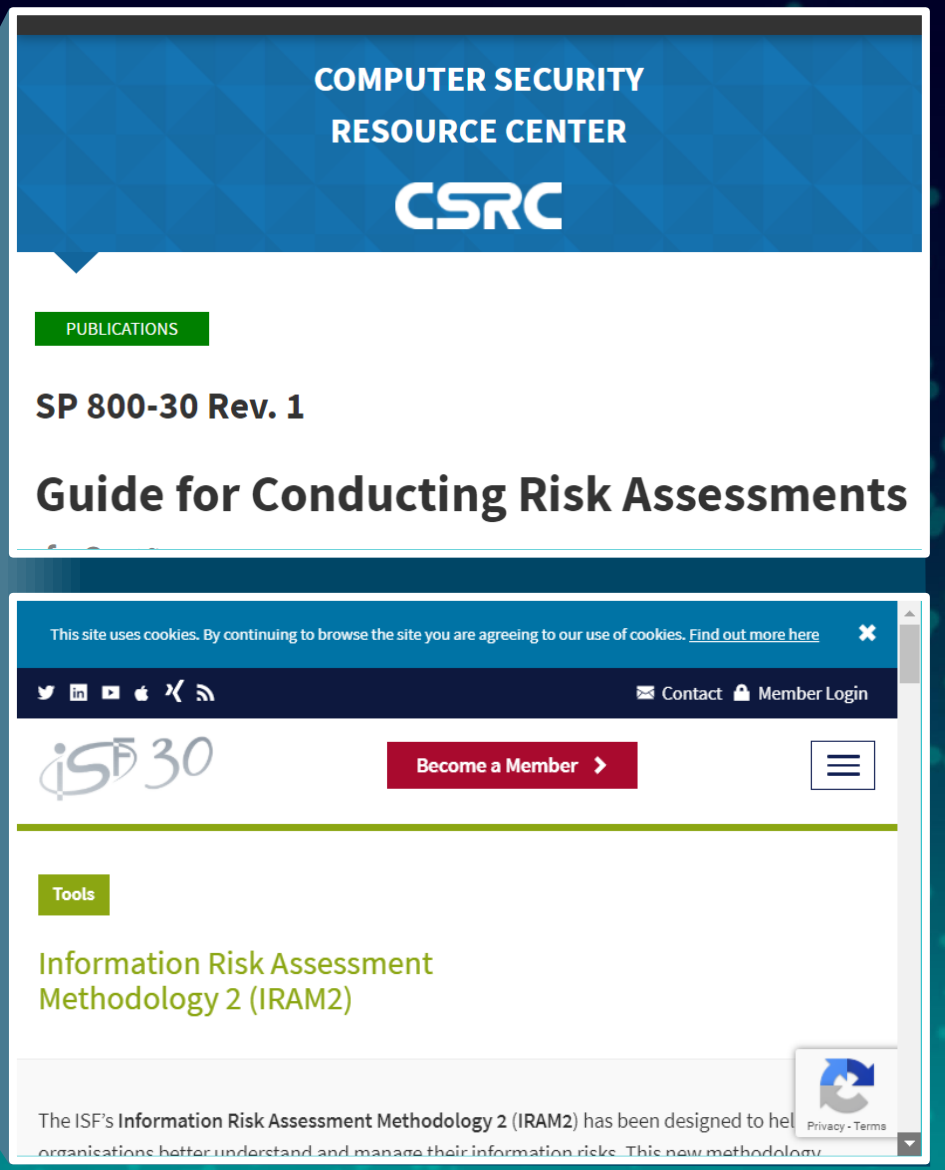
SIEMENS


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

Risk methods and frameworks

National Cyber Security Centre
a part of GCHQ

"A good overview"

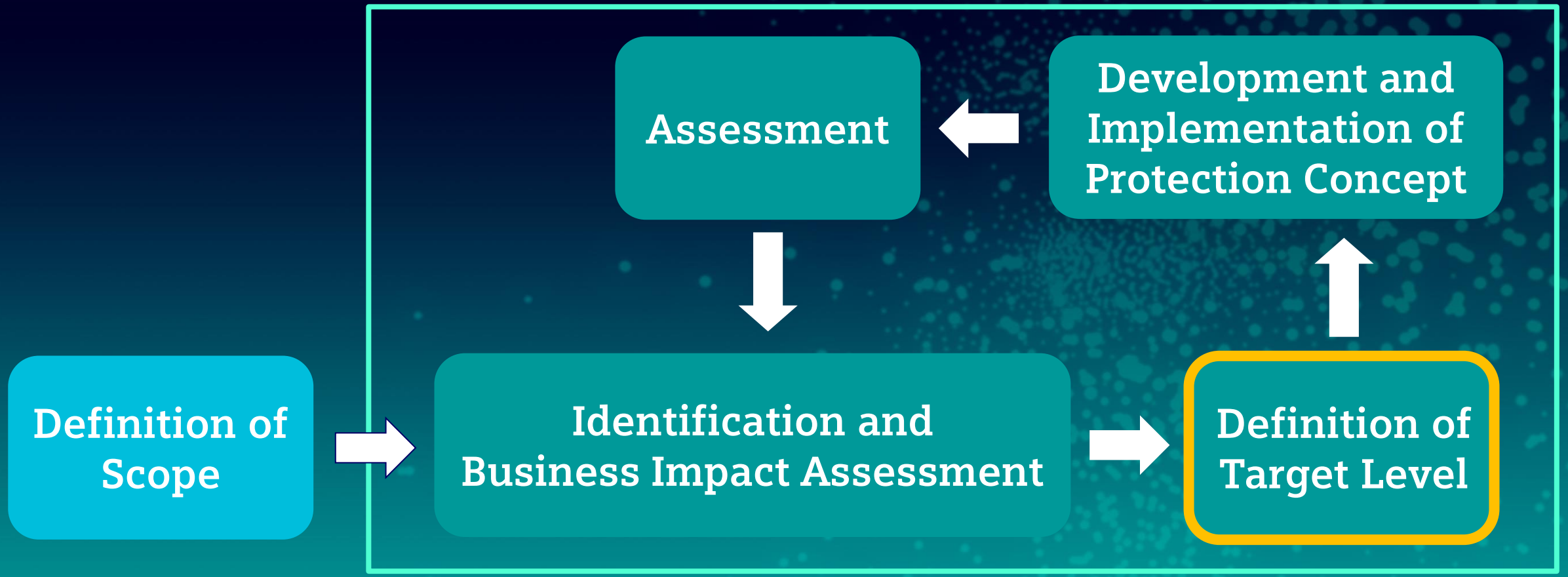


More info: https://www.ncsc.gov.uk/collection/risk-management-collection/component-system-driven-approaches/understanding-component-driven-risk-management

SIEMENS

Getting started

The IEC62443/ISO27001 based method



SIEMENS

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

SIEMENS

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

Hvilke konkrete erfaringer har vi fået undervejs?

SIEMENS

Brownfield

IT

OT

Greenfield

SIEMENS

Industrial Security Implementation hierarchy

SIEMENS

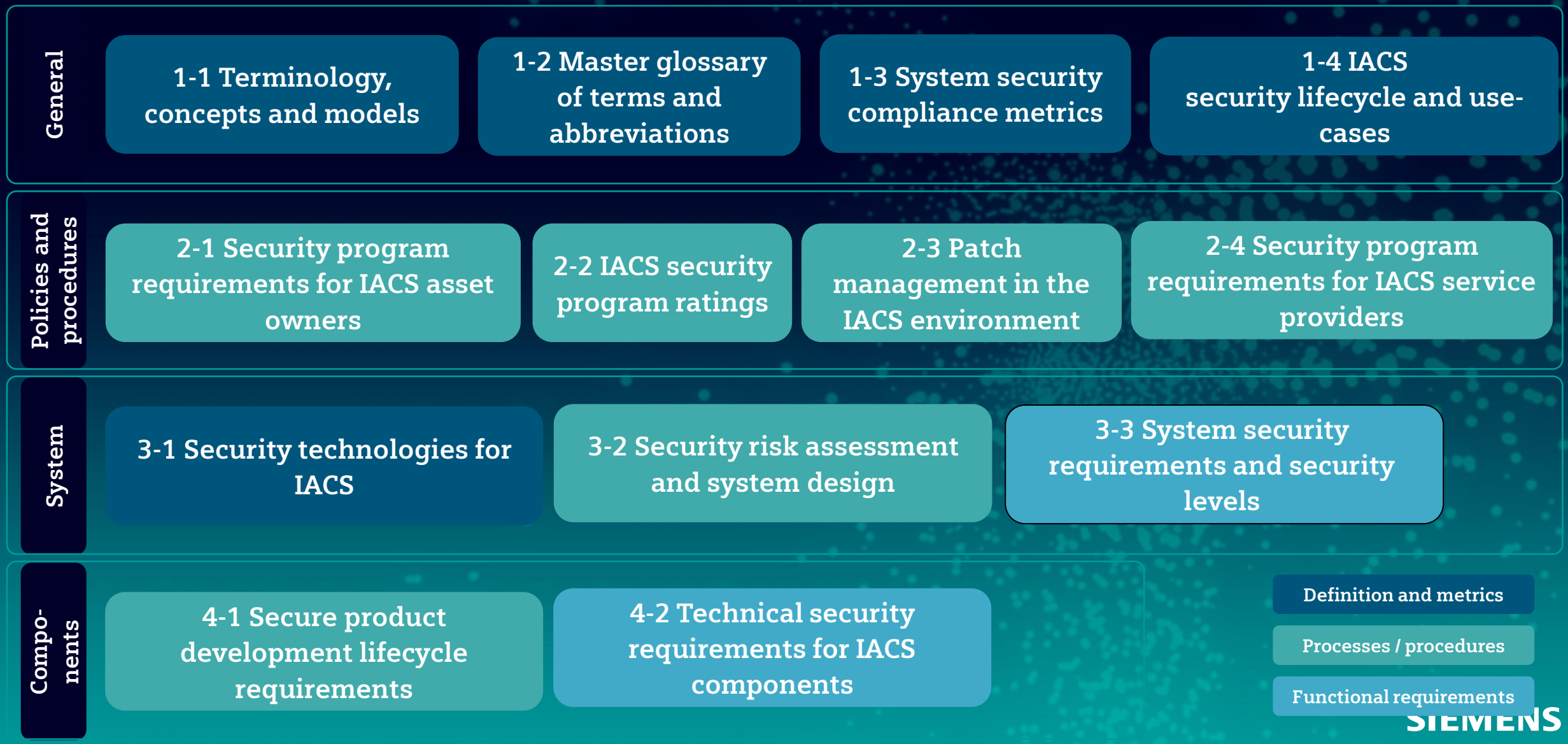
A piece of a **bigger picture**

SIEMENS

Hvor finder man inspiration?

SIEMENS

The IEC 62443 structure



SIEMENS

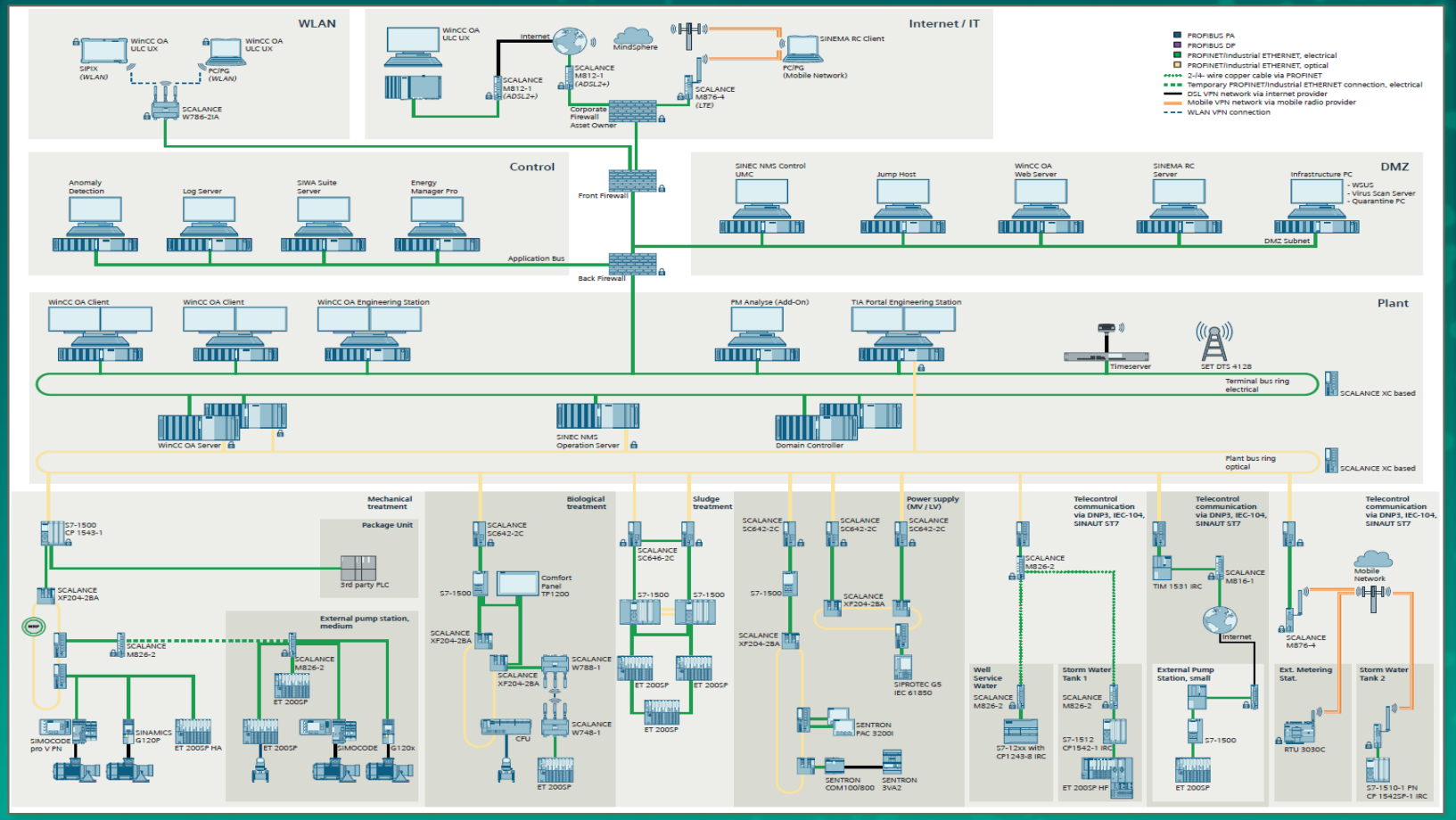
Operational Guidelines for Industrial Security

Contents

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

SIEMENS

IEC 62443-3-2 Complaint Blueprint



https://support.industry.siemens.com/cs/document/109780322/cybersecurity-defense-in-depth-concept-for-the-water-and-waste-water-industry?dti=0&lc=en-WW

SIEMENS

Se meget mere på:
www.siemens.dk/di-webinarer

SIEMENS