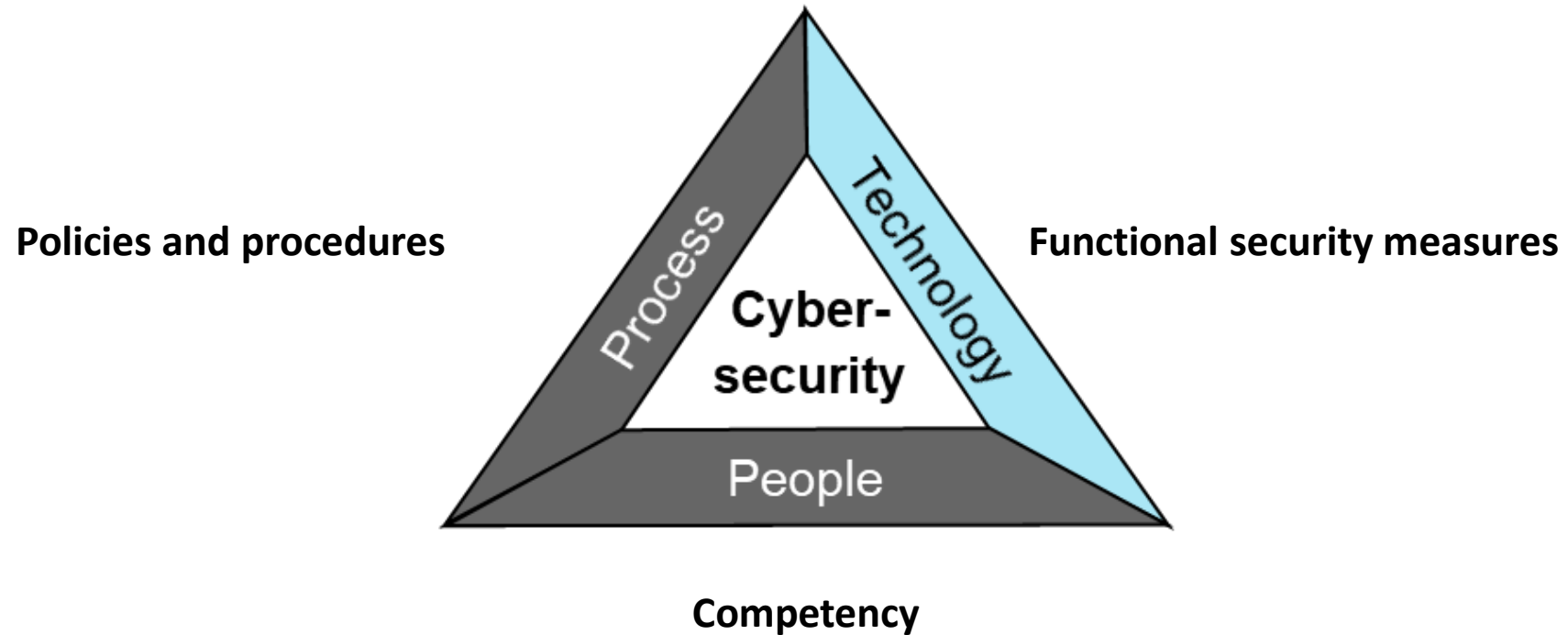


## Quo Vadis ISA/IEC 62443?

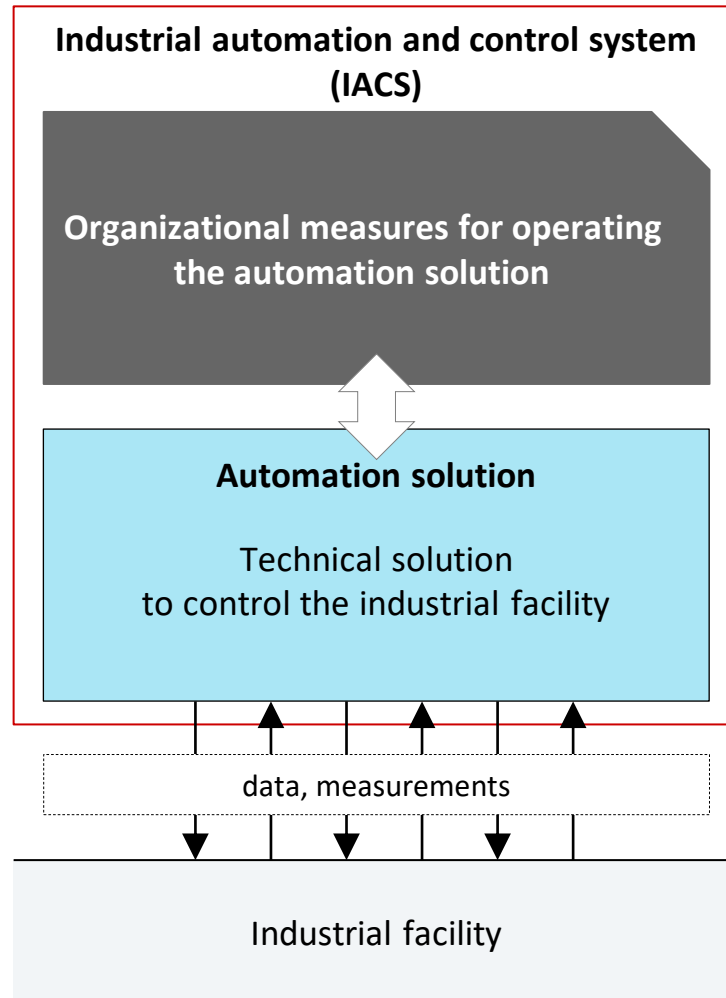
## Quo vadis ISA/IEC 62443?

- 1 **Overview and basic concepts of ISA/IEC 62443**
- 2 New organizational structure of ISA/IEC 62443
- 3 Relationship between ISA/IEC 62443 and ISO/IEC 27000

# Security is about technology, processes and people



**A holistic security protection concept has to include technology, processes and people**

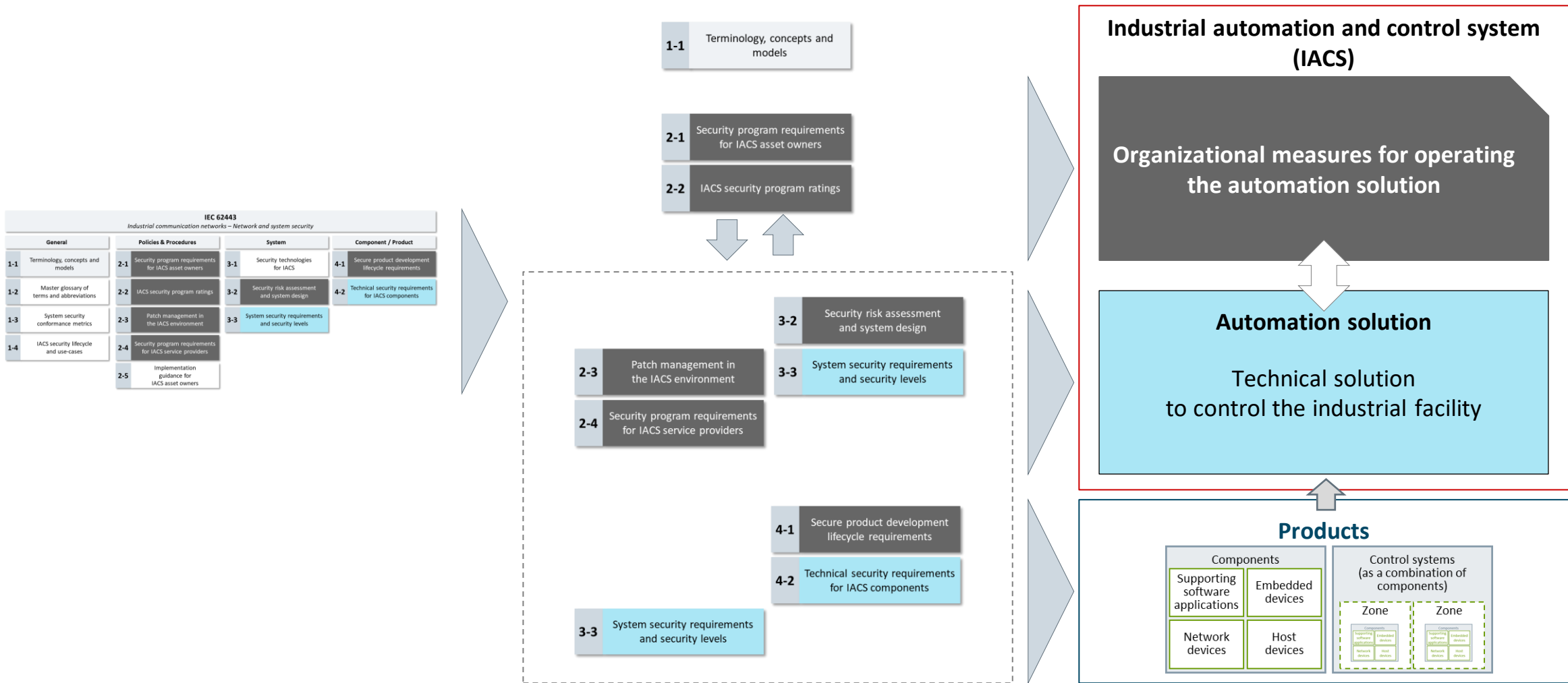


# Actual structure of IEC / ISA-62443

## Main documents to be published

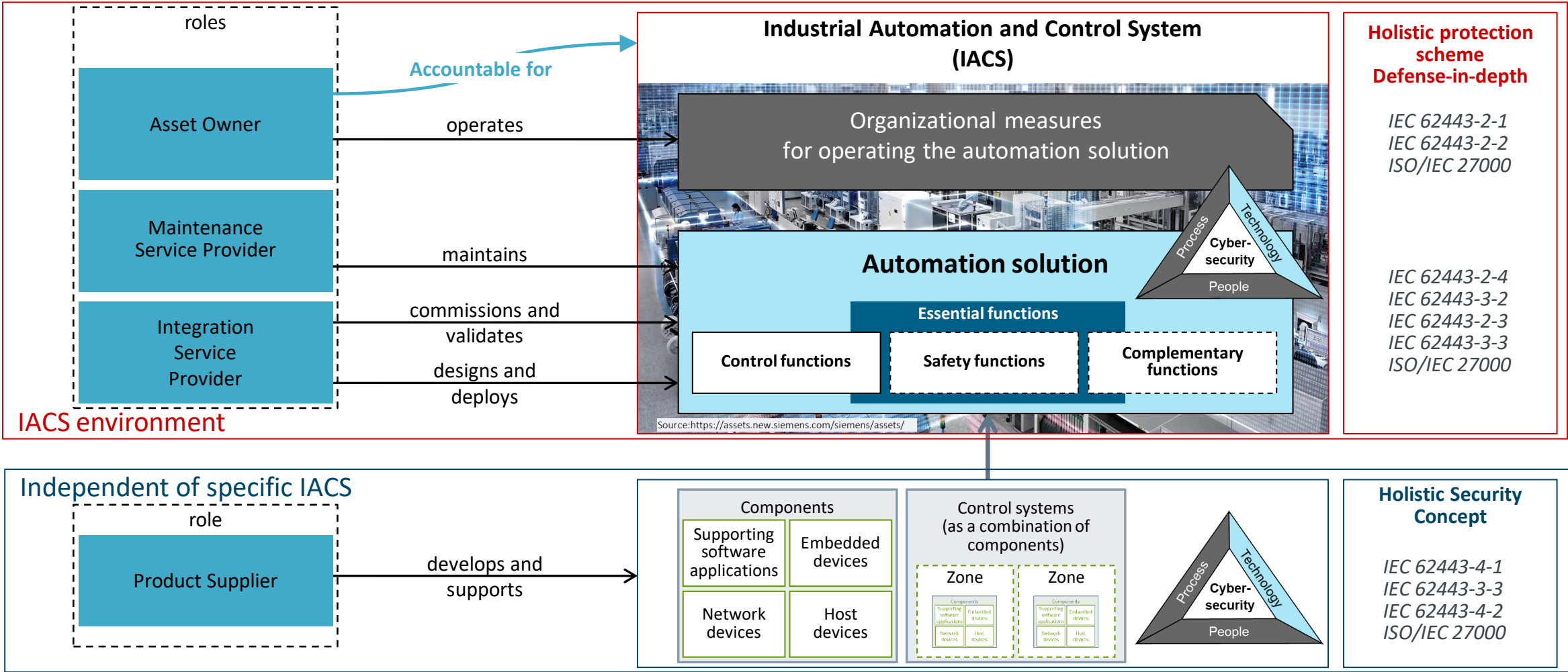
IEC 62443					
Industrial communication networks – Network and system security					
General		Policies & Procedures		System	
Component / Product					
1-1	Terminology, concepts and models	2-1	Security program requirements for IACS asset owners	3-1	Security technologies for IACS
1-2	Master glossary of terms and abbreviations	2-2	IACS security program ratings	3-2	Security risk assessment and system design
1-3	System security conformance metrics	2-3	Patch management in the IACS environment	3-3	System security requirements and security levels
1-4	IACS security lifecycle and use-cases	2-4	Security program requirements for IACS service providers		
		2-5	Implementation guidance for IACS asset owners		
	</				

# The IEC 62443 series addresses all constituents of an IACS

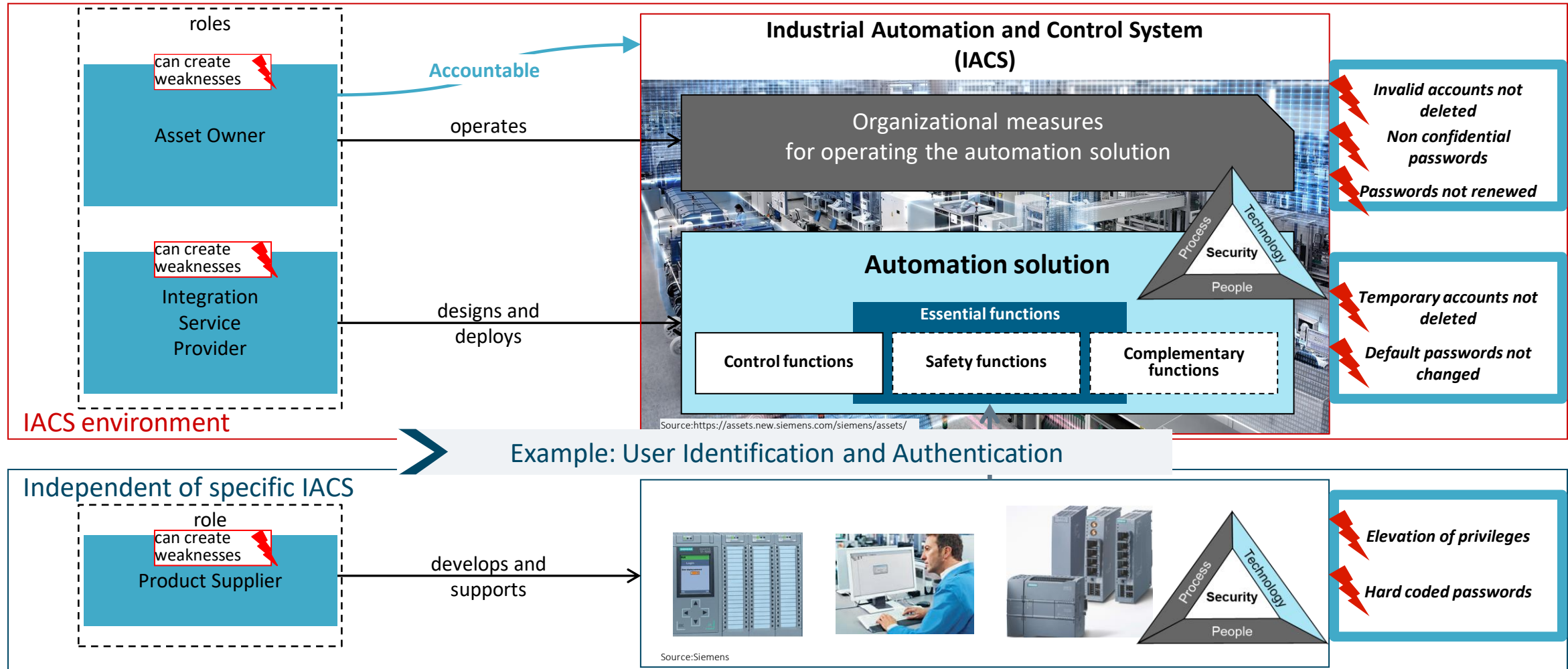




# Roles and responsibilities in IEC 62443 for a holistic protection scheme

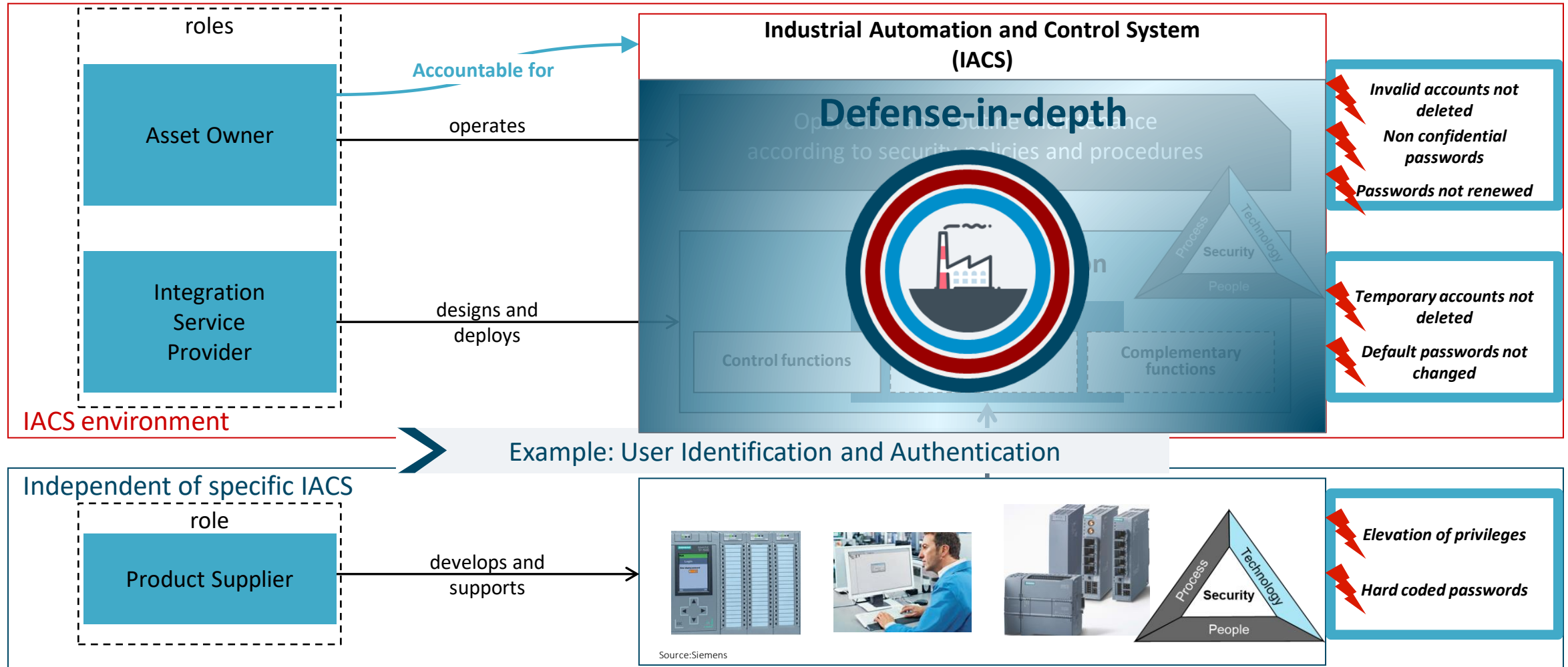


# Each actor can create weaknesses which can be used for misuse of the IACS in operation

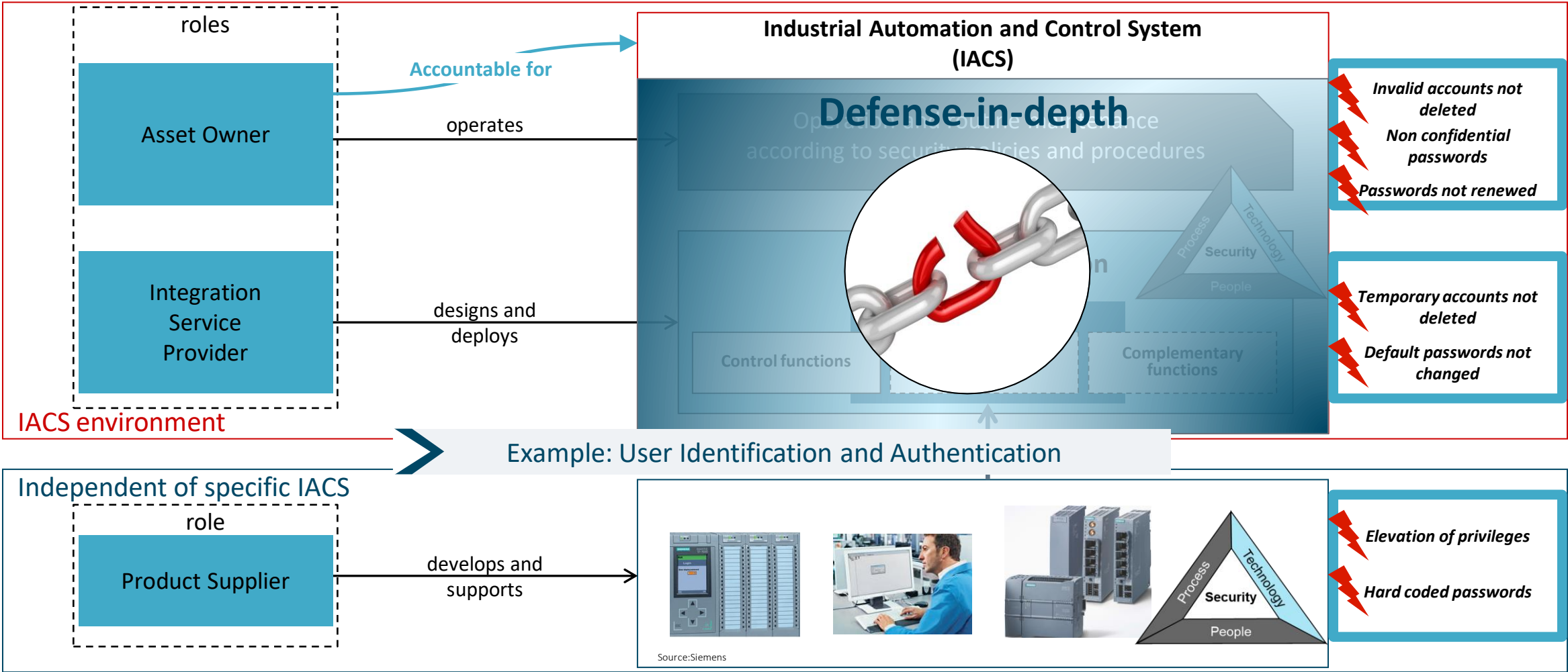




# A holistic protection scheme based on defense-in-depth is needed



# The weakest link defines the strength of the chain



## Quo vadis ISA/IEC 62443?

- 1 Overview and basic concepts of ISA/IEC 62443
- 2 **New organizational structure of ISA/IEC 62443**
- 3 Relationship between ISA/IEC 62443 and ISO/IEC 27000

## Existing 62443 standards:

- have little commonality in their organization
- are viewed as complex by our users
- have a significant level of duplicate requirements
- some 62443 standards mix process and technical requirements

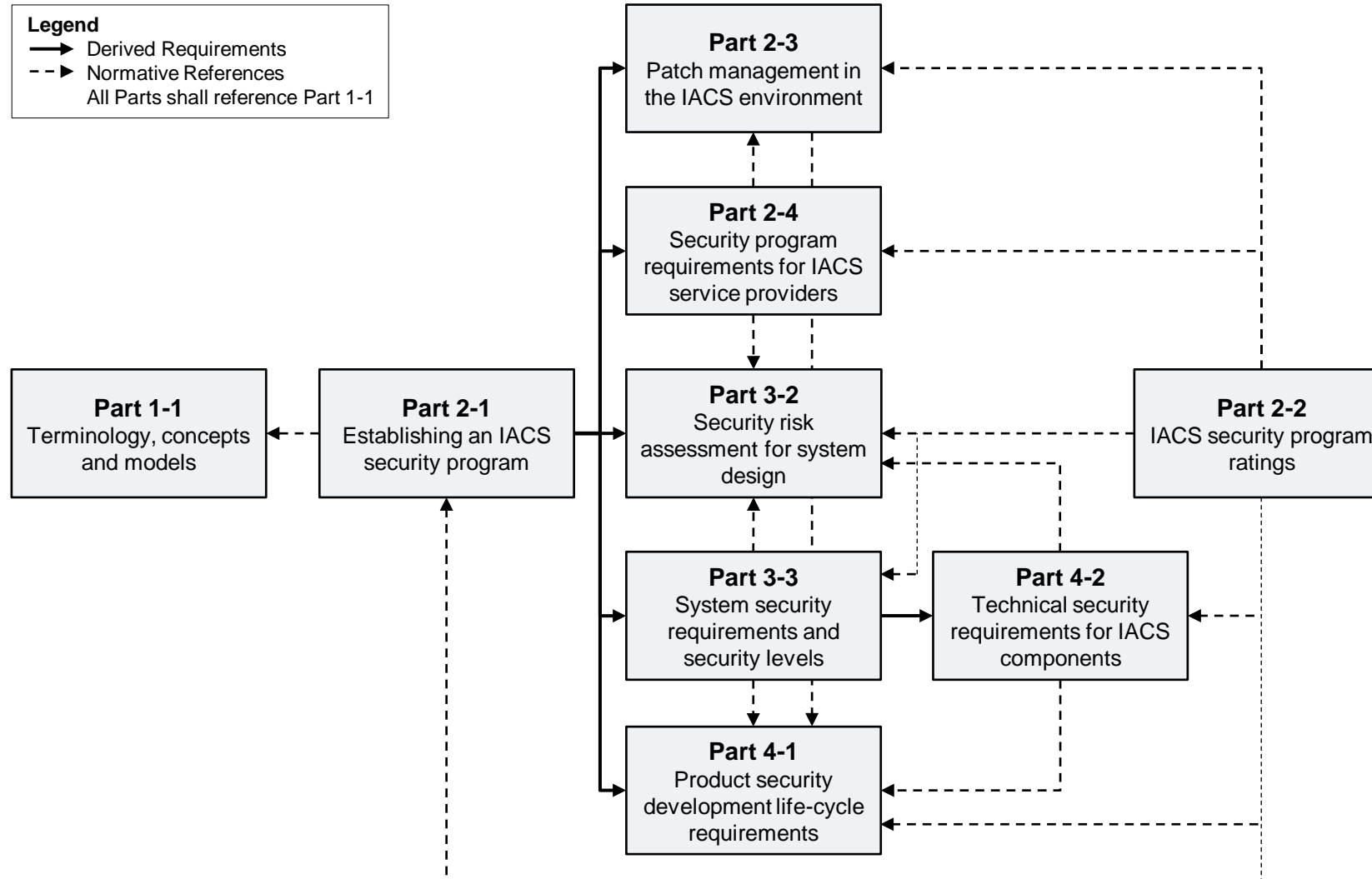
## A common Organizational Structure would:

- improve consistency between the parts of 62443
- allow for easier navigation through the 62443 set of standards
- allow for traceability of requirements between 62443 standards
- allow standards developers to test for completeness
- make it easier to communicate security objectives to all stakeholders
- make it easier to map requirements between 62443 and other standards
- make it easier to develop the 62443 Workbench

The new Organization Structure is:

- a way to organize the set of requirements in a 62443 standard
- a guideline document that describes the methodology
- a replacement for the Foundational Requirements
- required to be used by all 62443 Technical Specifications (TS) and International Standards (IS)
- not required to be used by 62443 Technical Reports (TR)
- used to test for completeness of a 62443 standard
- used to test for redundancy of requirements across 62443 standards
- used to facilitate traceability of requirements across 62443 standards
- simple to understand by end users of the 62443 standard

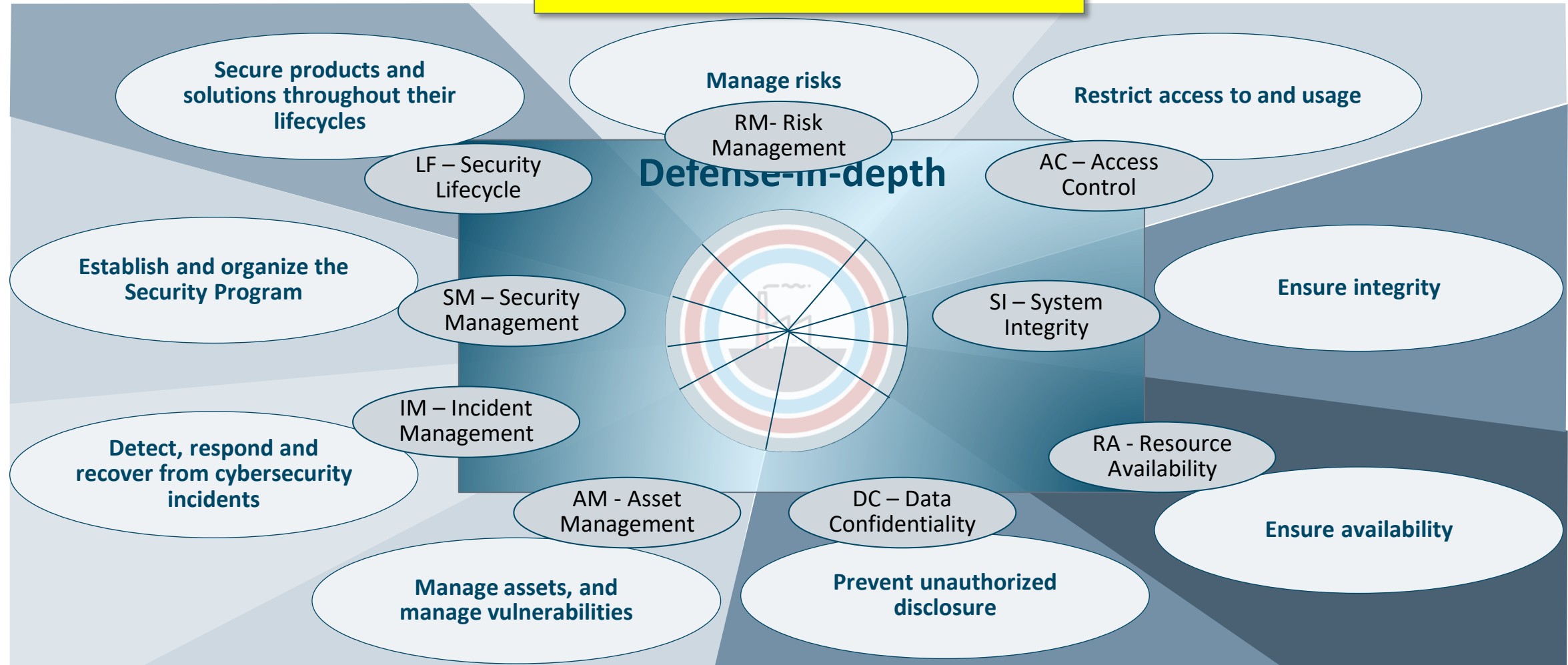
# Hierarchy of IEC 62443 Requirements





# The nine Security Objectives

Not yet finally approved in ISA-99 and IEC TC 65



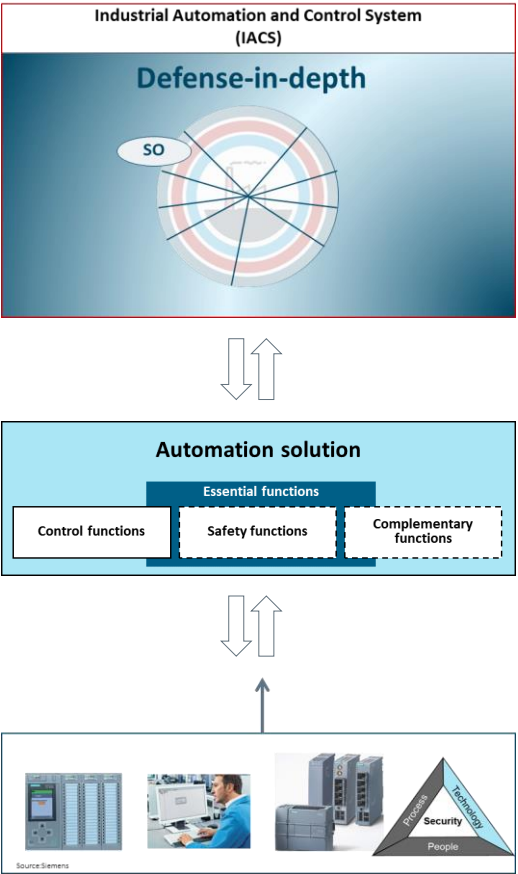
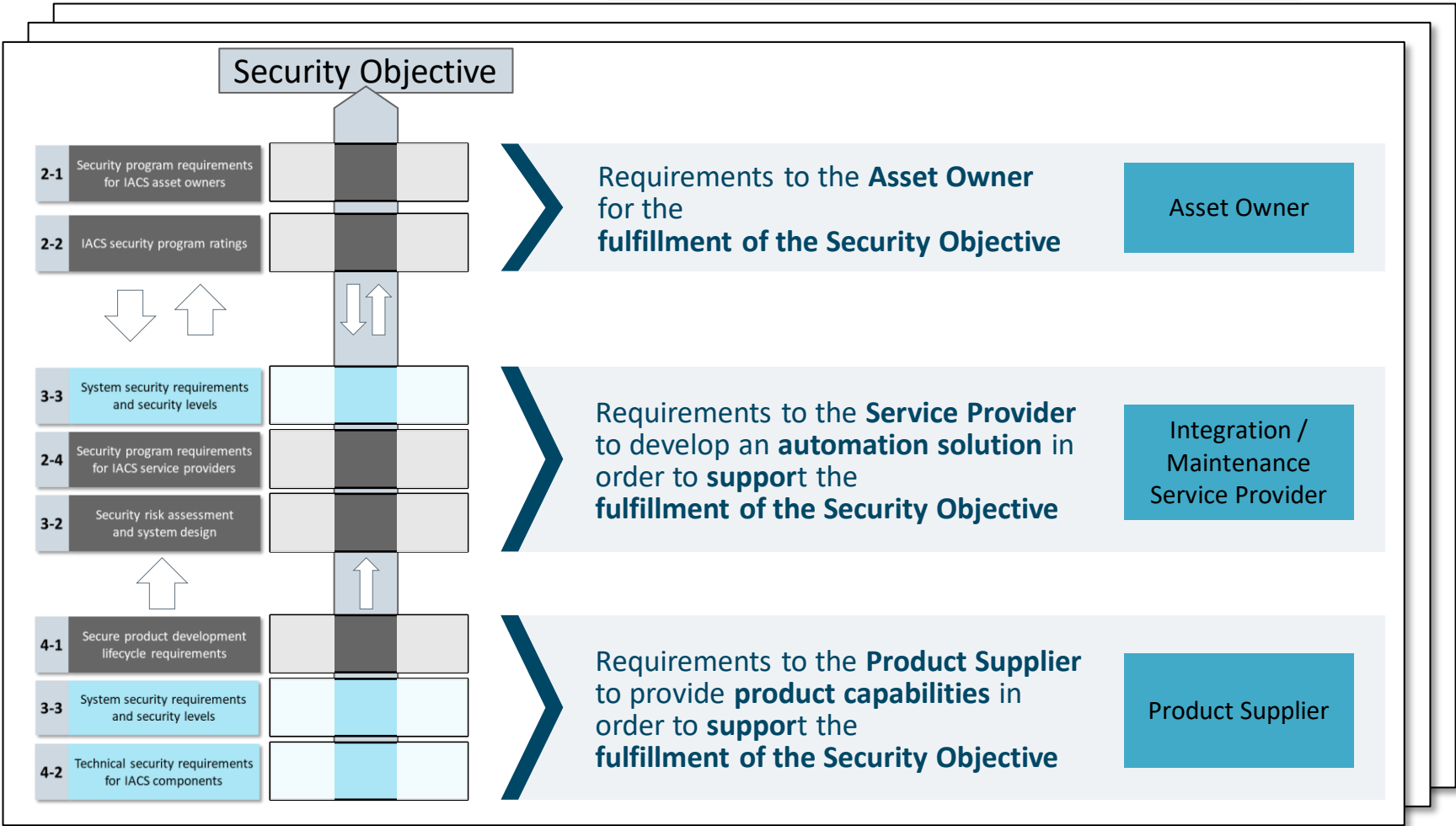
# Definitions of the Security Objectives

Not yet finally approved in ISA-99 and IEC TC 65

SM – Security Management	<b>Establish</b> and sustain the elements of an IACS <b>Security Program</b>
LF – Security Lifecycle	<b>Secure</b> products and automation solution <b>throughout their lifecycles</b>
RM- Risk Management	<b>Manage risks</b> to products and IACS throughout their Lifecycles
AC – Access Control	<b>Restrict</b> physical and logical <b>access to and usage</b> of products and automation solution
SI – System Integrity	<b>Ensure</b> system, communication and data <b>integrity</b> for products and automation solution
RA - Resource Availability	<b>Ensure</b> system, communication and data <b>availability</b> for products and automation solution
DC – Data Confidentiality	<b>Prevent unauthorized disclosure</b> of sensitive data for products and automation solution
AM - Asset Management	<b>Manage assets</b> , understand criticality and <b>manage vulnerabilities</b> for products and automation solution
IM – Incident Management	Detect, respond and <b>recover from cybersecurity</b> incidents for products and automation solution

# Each document of the 62443 series will be structured along the Security Objectives

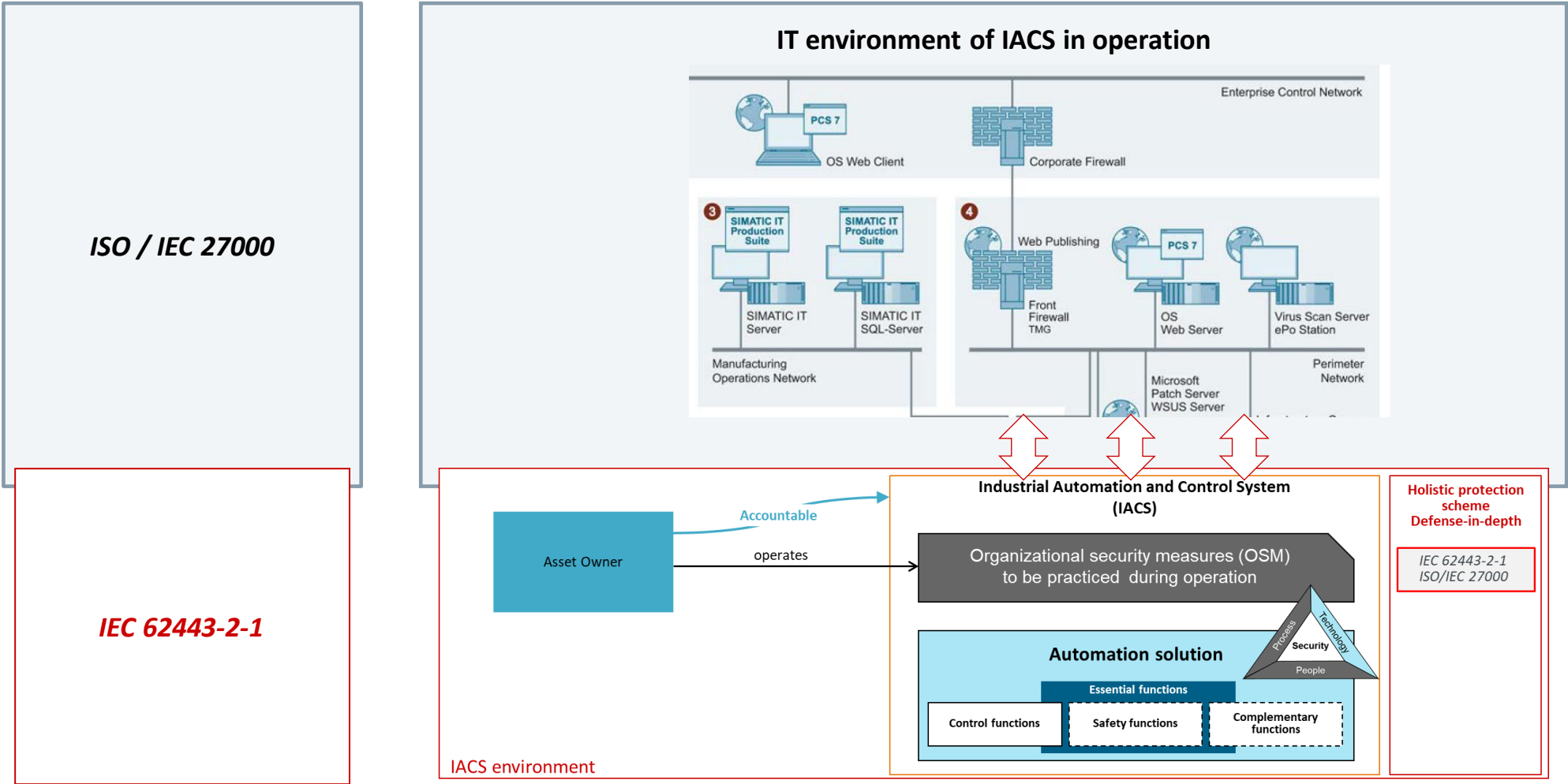
Not yet finally approved in ISA-99 and IEC TC 65



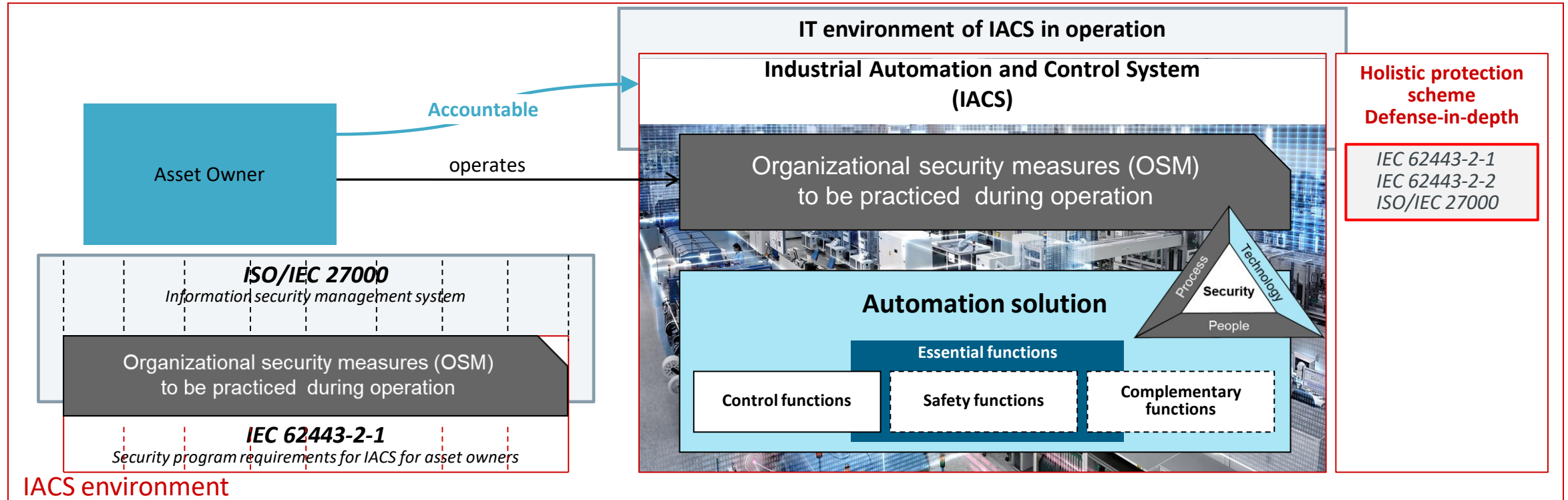
## Cybersecurity: Basics and concepts of IEC 62443

- 1 Introduction and motivation
- 2 Roles and responsibilities, Defense-in-Depth, Elements of a Security Program, risk-based Approach
- 3 **Relationship between ISA/IEC 62443 and ISO/IEC 27000**

# The IACS is embedded in the IT infrastructure of the asset owner



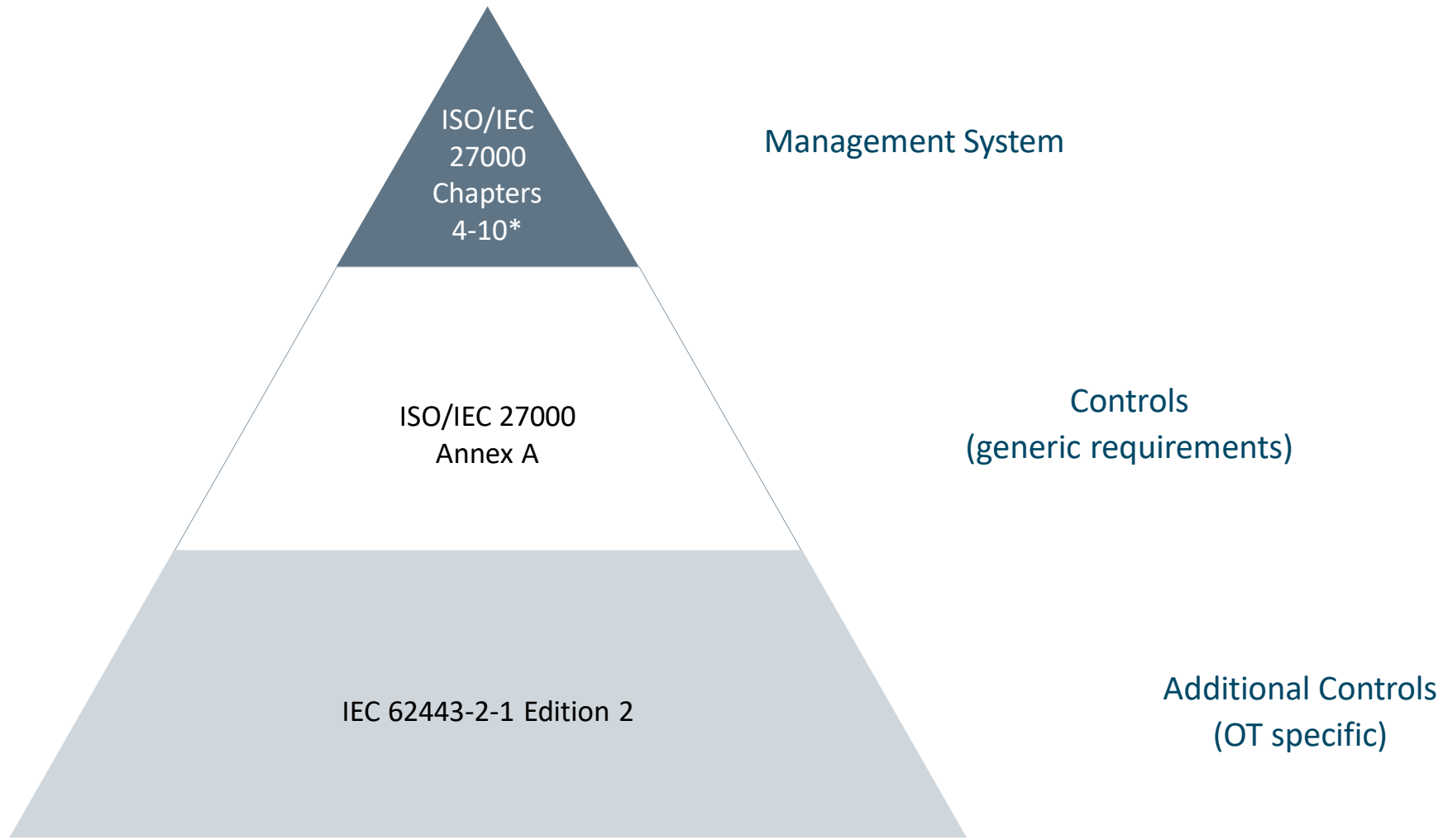
# Matched IEC 62443-2-1 and ISO/IEC 27000 requirements are relevant for asset owners during operation of the IACS



- Asset Owner must have an established ISMS for the IT environment of the IACS in operation e.g. according to ISO/IEC 27000
- Asset Owner operates a security program for the IACS in operation according to IEC 62443-2-1 and a holistic protection scheme
- Requirements of IEC 62443-2-1 are specific to IACS and are aligned / matched to ISMS requirements (e.g. ISO/IEC 27000 controls)

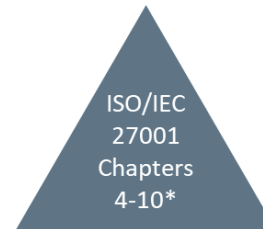


# Relationship between ISO/IEC 27000 and IEC 62443-2-1



\* According to chapter 6.1.3 Note 2 the controls listed in Annex A are not exhaustive. Additional objectives and controls are provided in IEC62443-2-1 Edition 2

# IEC 62443-2-1 requires an established ISMS

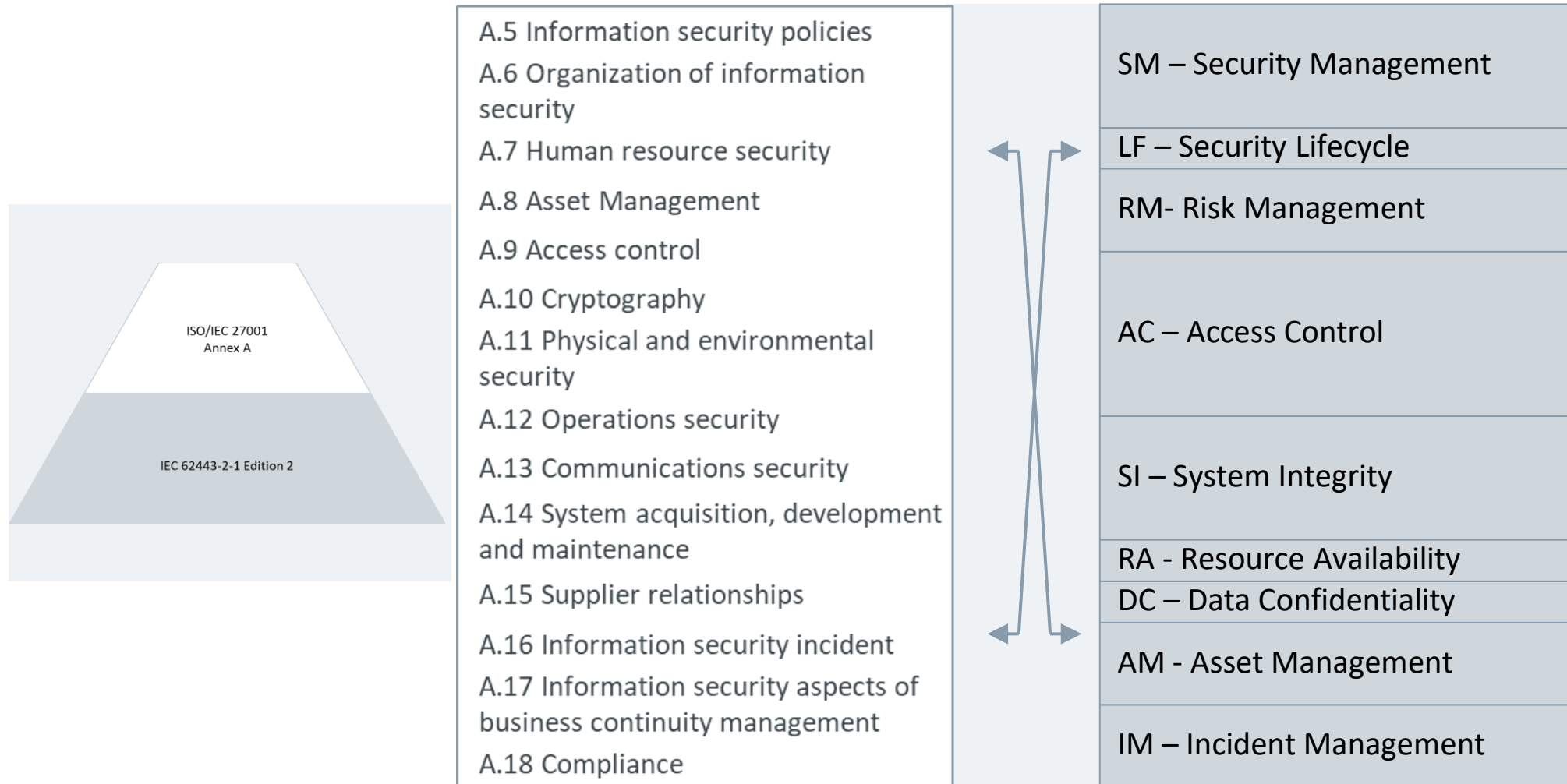


## Management System

4. Context of the organization	4.1	Understanding the organization and its context	7. Support	7.5 Documented information	7.1	Resources
	4.2	Understanding the needs and expectations of interested parties			7.2	Competence
	4.3	Determining the scope of the information security management system			7.3	Awareness
	4.4	Information security management system			7.4	Communication
5. Leadership	5.1	Leadership and commitment	8. Operation		7.5.1	General
	5.2	Policy			7.5.2	Creating and updating
	5.3	Organizational roles, responsibilities and authorities			7.5.3	Control of documented information
6. Planning	6.1 Actions to address risks and opportunities	6.1.1	9. Performance evaluation		8.1	Operational planning and control
		6.1.2			8.2	Information security risk assessment
		6.1.3			8.3	Information security risk treatment
	6.2	Information security objectives and planning to achieve them	10. Improvement		9.1	Monitoring, measurement, analysis and evaluation
					9.2	Internal audit
					9.3	Management review
					10.1	Nonconformity and corrective action
					10.2	Continual improvement

An **established ISMS** is a prerequisite for the implementation of a security program for an OT application.

# All controls of the ISMS are mapped to the Security Sub-Objectives



## Example of mapping: AC 2 Use control

### AC / Use control

#### Requirements of ISO/IEC 27001 to the coordinated ISMS (Asset Owner)

Number of requirements: 6

✓ A.06.2.1	Mobile device policy
✓ A.09.4.1	Information access restriction
✓ A.09.4.2	Secure log-on procedures
✓ A.09.4.3	Password management system
✓ A.09.4.4	Use of privileged utility programs
✓ A.09.4.5	Access control to program source code

#### Requirements of ISA/IEC 62443-2-1 to the Security Program (Asset Owner)

Number of requirements: 9

✓ NET 1.9	User messaging
✓ COMP 1.2	Dedicated portable media
✓ DATA 1.3	Safety system configuration mode
✓ USER 1.16	Session integrity
✓ USER 1.18	Screen lock
✓ USER 2.1	Authorization
✓ USER 2.2	Administrative rights authorization
✓ USER 2.3	Multiple approvals
✓ USER 2.4	Manual elevation of privileges

## Example of mapping: AC 3 Remote access

### AC / Remote access

Requirements of ISO/IEC 27001 to the coordinated ISMS (Asset Owner)

Number of requirements: 7

✓ A.06.2.2	Teleworking
✓ A.12.1.1	Documented operating procedures
✓ A.13.1.1	Network controls
✓ A.13.1.2	Security of network services
✓ A.13.2.1	Information transfer policies and procedures

Requirements of ISA/IEC 62443-2-1 to the Security Program (Asset Owner)

Number of requirements: 3

✓ NET 3.1	Remote access applications
✓ NET 3.2	Remote access connections
✓ NET 3.3	Remote access termination

Thank you! Questions?



Dr. Pierre Kobes

[kobes@kobesconsulting.de](mailto:kobes@kobesconsulting.de)

Training Basic Concepts of IEC 62443:

<https://www.pw-akademie.eu/seminar/cybersecurity/>

[info@pw-akademie.eu](mailto:info@pw-akademie.eu)

