10th EDITION EUROPEAN CONGRESS

ERTS 2020

FROM 29th TO 31st JANUARY / TOULOUSE, FRANCE
PIERRE BAUDIS CONGRESS CENTER

EMBEDDED
REAL TIME SYSTEMS

Preliminary Safety and Security Co-engineering Process in the Industrial Automation Sector

Alejandra Ruiz, Javier Puelles, Jabier Martinez (Tecnalia)
Thomas Gruber (Austrian Institute of Technology)
Martin Matschnig, Bernhard Fischer (Siemens AG Austria)

AQUAS SAFETY SECURITY PERFORMANCE

H2020-ECSEL Grant agreement 737475

tecnalia Inspiring Business

Agenda

1. Safety and Security in the Industrial Automation Sector

2. Co-engineering

3. IEC 61508 and ISA 62443 standards

4. Do they have something in common?

5. Equivalence map concept

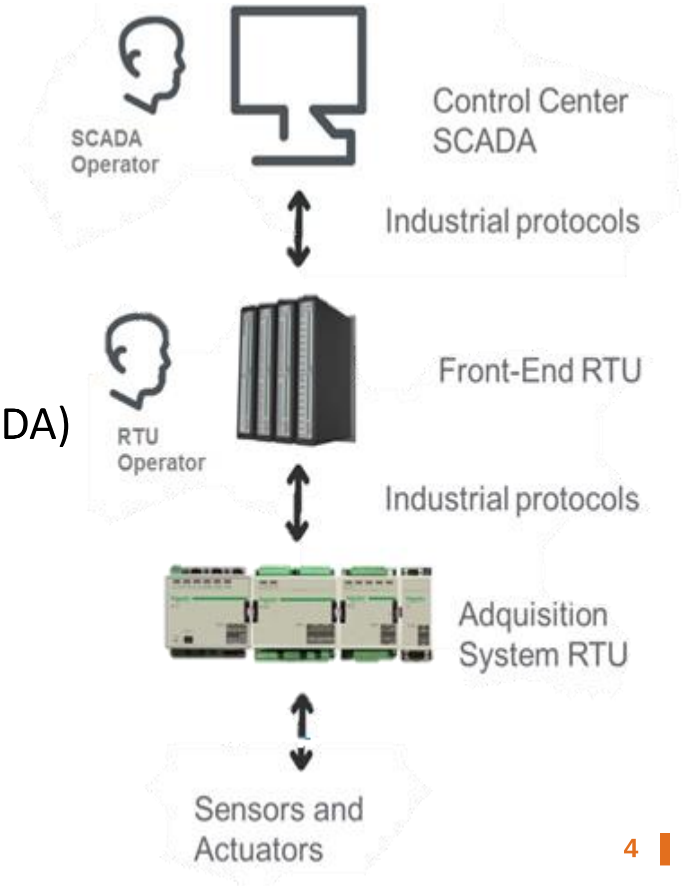
5. Co-engineering process in the automation sector

1. Safety and Security in the Industrial Automation Sector

Industrial Automation Sector

Industrial Control System (ICS)

- 3 levels architecture:
  - Field Site (Acquisition System)
  - Communication Center (Front-End)
  - Control Center
- Main elements:
  - Supervisory Control and Data Acquisition (SCADA)
  - Remote Terminal Units (RTUs)
  - Sensors & Actuators



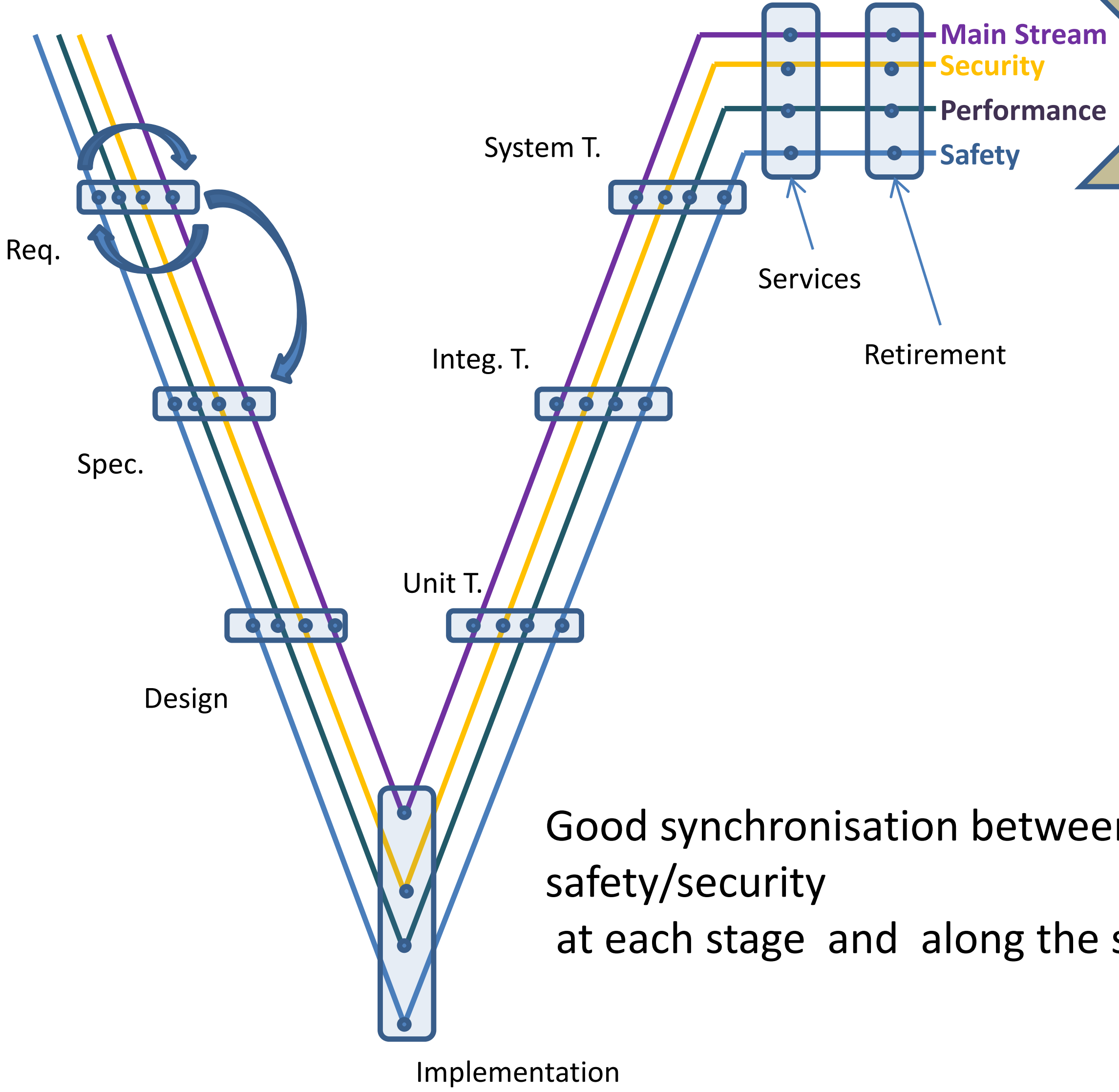
Industrial Automation Sector

- Considered as critical sector
- Safety oriented
- Security reactive

- Costly certification processes
- High risk of redundant work in co-certification *(Safe/Sec)*

2. Co-Engineering

Co-engineering

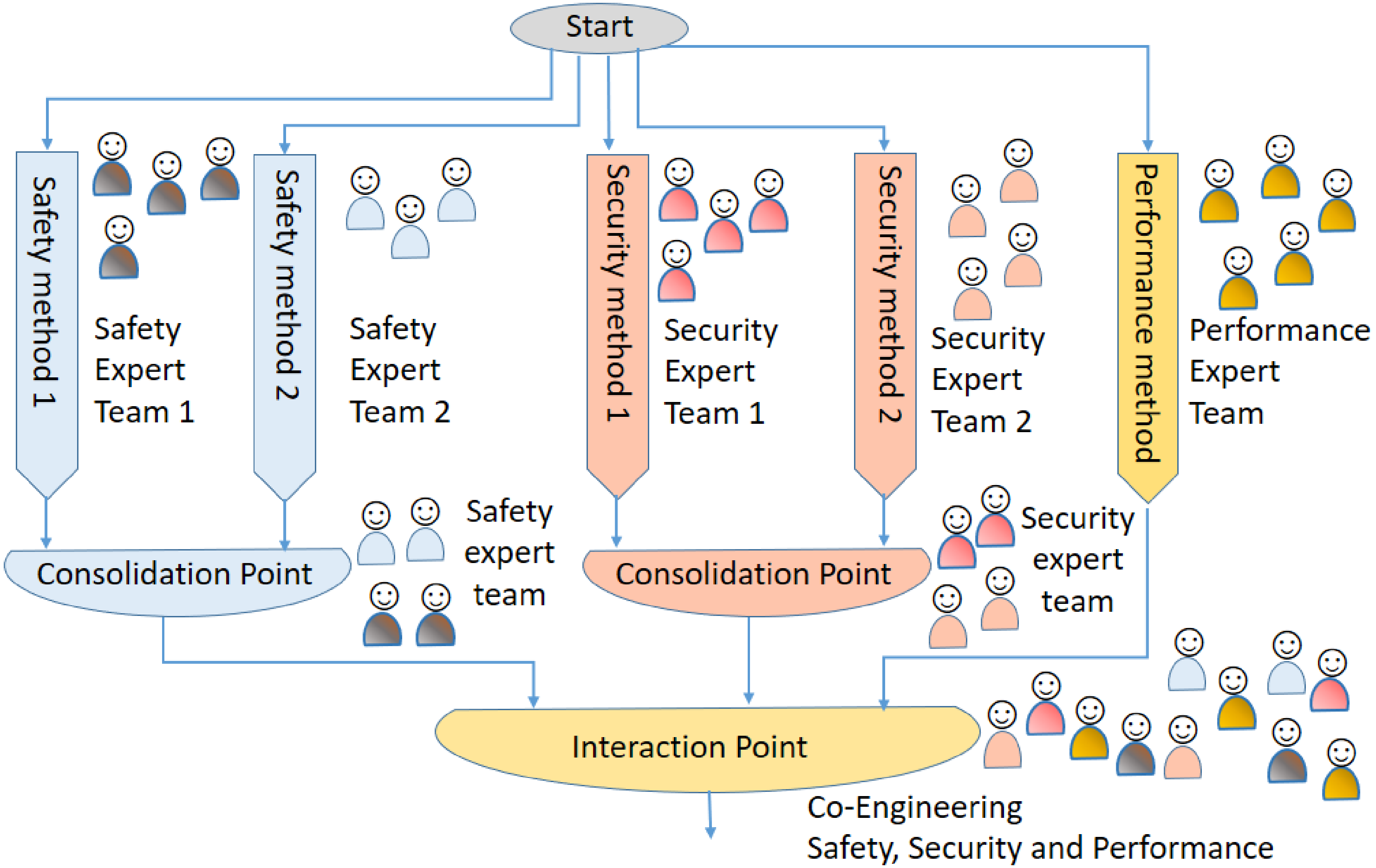


Operation & maintenance
updates, recovery,
decommissioning & disposal

Safety/security
Co-engineering goes
beyond the V-model.

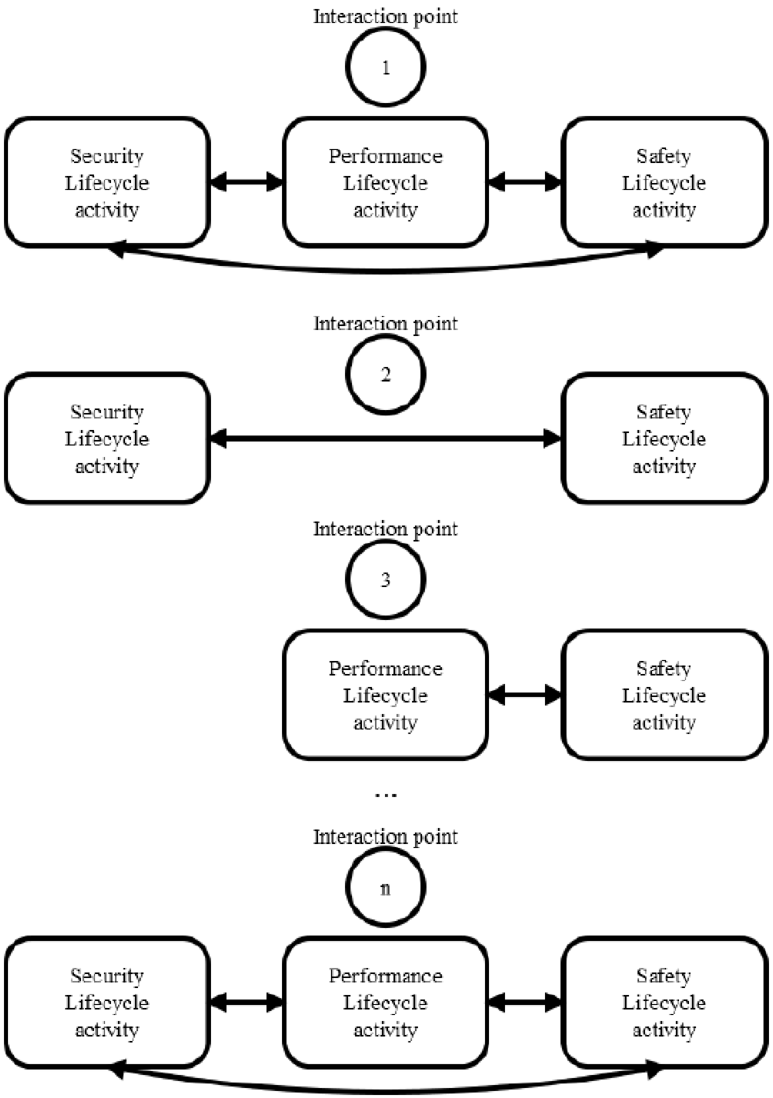
Good synchronisation between safety/security
at each stage and along the stages.

Co-engineering



There will be points in time when system developers will take decisions about how to progress with the development. These decisions should be taken with a *holistic view* on the system.

If as a result of a refinement ***significant deviations*** from the previous allocation of the goals/properties are detected, then an interaction point will be triggered, so that a new trade-off is established between the assigned goals and component properties.


Interaction point
1
Security Lifecycle activity
Performance Lifecycle activity
Safety Lifecycle activity
Interaction point
2
Security Lifecycle activity
Safety Lifecycle activity
Interaction point
3
Performance Lifecycle activity
Safety Lifecycle activity
...
Interaction point
n
Security Lifecycle activity
Performance Lifecycle activity
Safety Lifecycle activity

3. IEC 61508 and ISA 62443 standards

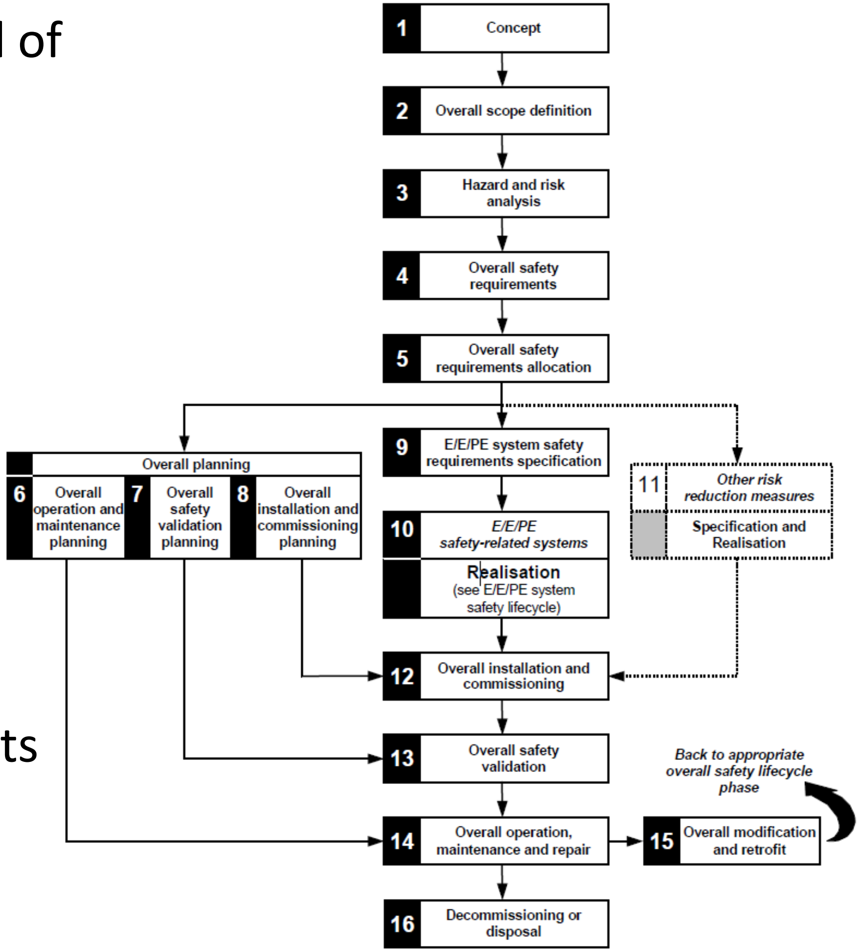
IEC 61508

- It is considered as the core functional safety standard.
- It defines functional safety as: “part of the overall safety relating to the EUC (Equipment Under Control) and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities.”

IEC 61508

The series of standards EN 61508 is composed of the following parts:

- Part 1: Introduction to the concept of functional safety
- Part 2: Requirements for programmable electrical/electronic/electronic systems related to safety
- Part 3: Software requirements
- Part 4: Definitions and abbreviations
- Part 5: Examples to determine the level of safety integrity
- Part 6: Guidelines for the application of parts 2 and 3
- Part 7: Presentation of techniques and measures


1 Concept
2 Overall scope definition
3 Hazard and risk analysis
4 Overall safety requirements
5 Overall safety requirements allocation
Overall planning
6 Overall operation and maintenance planning
7 Overall safety validation planning
8 Overall installation and commissioning planning
9 E/E/PE system safety requirements specification
10 E/E/PE safety-related systems
Realisation (see E/E/PE system safety lifecycle)
11 Other risk reduction measures
Specification and Realisation
12 Overall installation and commissioning
13 Overall safety validation
14 Overall operation, maintenance and repair
15 Overall modification and retrofit
Back to appropriate overall safety lifecycle phase
16 Decommissioning or disposal

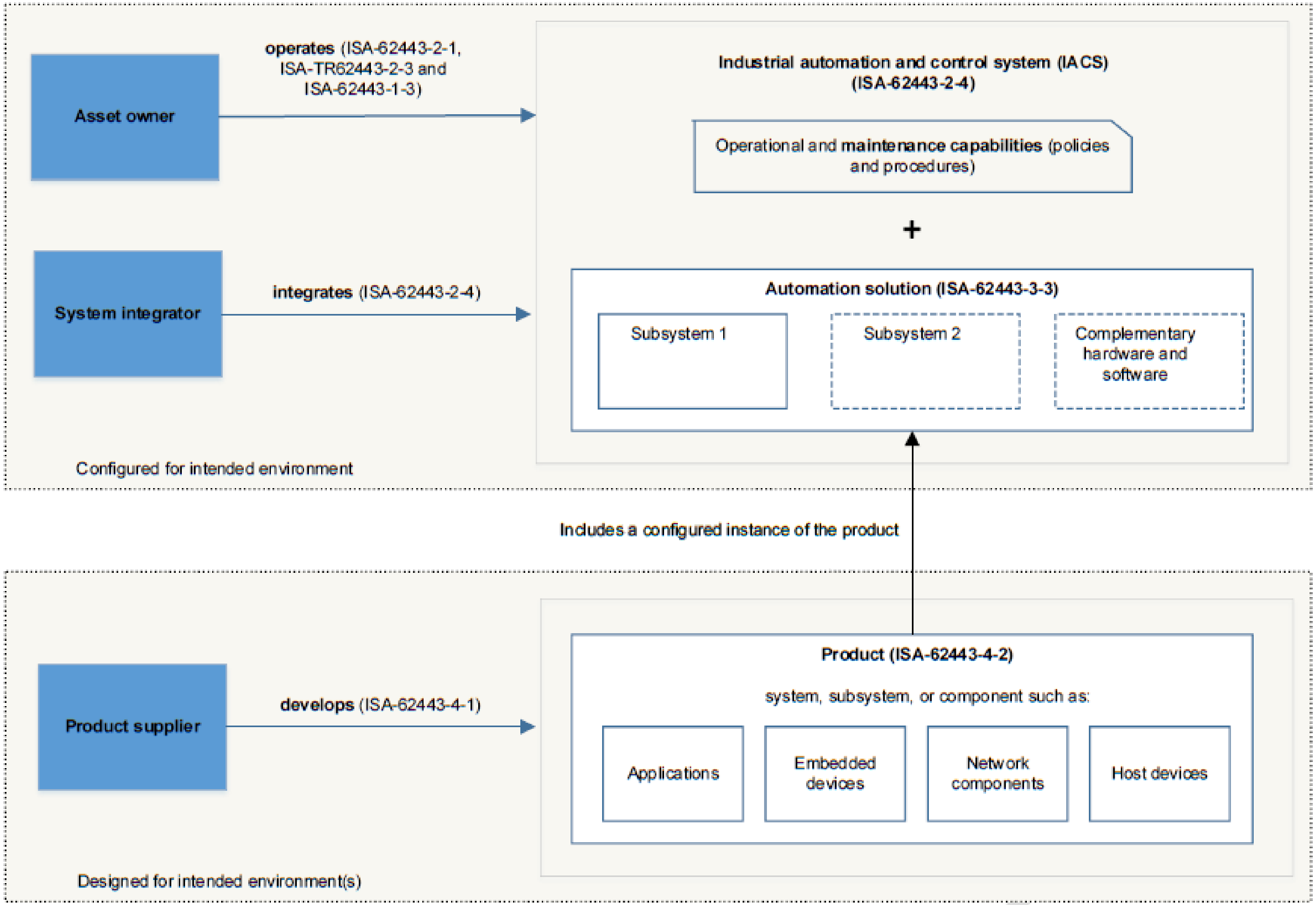
ISA 62443

Standard for Industrial automation and control systems security/ Network and system security for industrial-process measurement and control.

Content: ISA 62443 series and technical reports are classified into the following categories:

1. Information on the concepts, terminology, models and work products that describe the security metrics.
2. Different facets of the generation and maintenance of an effective IACS security program by targeting the owner of the asset.
3. Security of the control systems, and the guidelines and design requirements of the system.
4. Technical requirements and the specific product development of the control system updates.

ISA 62443

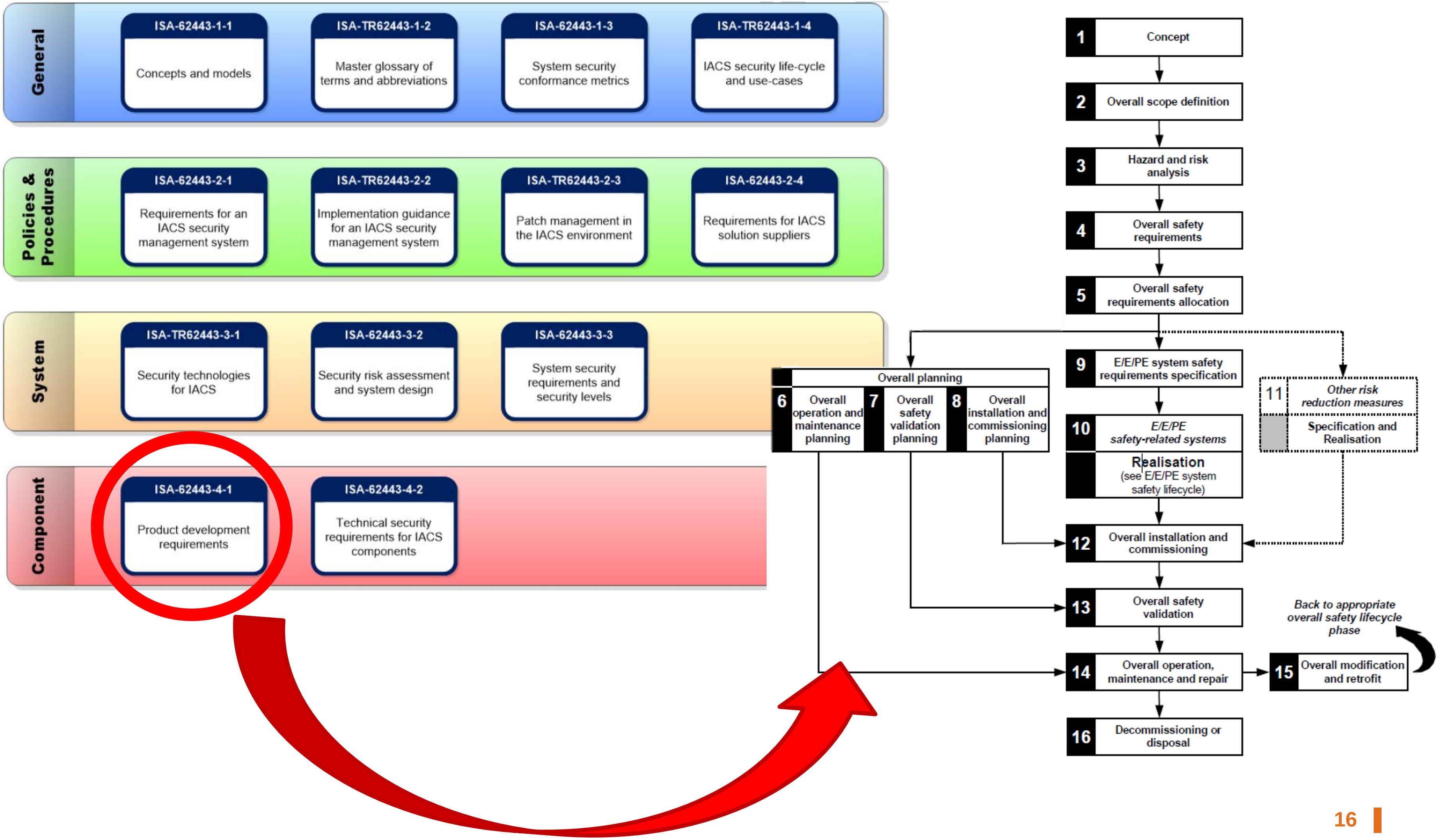

Asset owner
operates (ISA-62443-2-1, ISA-TR62443-2-3 and ISA-62443-1-3)
Industrial automation and control system (IACS) (ISA-62443-2-4)
Operational and maintenance capabilities (policies and procedures)
+
System integrator
integrates (ISA-62443-2-4)
Automation solution (ISA-62443-3-3)
Subsystem 1
Subsystem 2
Complementary hardware and software
Configured for intended environment
Includes a configured instance of the product
Product supplier
develops (ISA-62443-4-1)
Product (ISA-62443-4-2)
system, subsystem, or component such as:
Applications
Embedded devices
Network components
Host devices
Designed for intended environment(s)

4. Do they have something in common?

Framework for comparison

ISA 62443

IEC 61508



General

- ISA-62443-1-1: Concepts and models
- ISA-TR62443-1-2: Master glossary of terms and abbreviations
- ISA-62443-1-3: System security conformance metrics
- ISA-TR62443-1-4: IACS security life-cycle and use-cases

Policies & Procedures

- ISA-62443-2-1: Requirements for an IACS security management system
- ISA-TR62443-2-2: Implementation guidance for an IACS security management system
- ISA-TR62443-2-3: Patch management in the IACS environment
- ISA-62443-2-4: Requirements for IACS solution suppliers

System

- ISA-TR62443-3-1: Security technologies for IACS
- ISA-62443-3-2: Security risk assessment and system design
- ISA-62443-3-3: System security requirements and security levels

Component

- ISA-62443-4-1: Product development requirements
- ISA-62443-4-2: Technical security requirements for IACS components

1 Concept

2 Overall scope definition

3 Hazard and risk analysis

4 Overall safety requirements

5 Overall safety requirements allocation

Overall planning

6 Overall operation and maintenance planning

7 Overall safety validation planning

8 Overall installation and commissioning planning

9 E/E/PE system safety requirements specification

10 E/E/PE safety-related systems Realisation (see E/E/PE system safety lifecycle)

11 *Other risk reduction measures* Specification and Realisation

12 Overall installation and commissioning

13 Overall safety validation

14 Overall operation, maintenance and repair

15 Overall modification and retrofit

Back to appropriate overall safety lifecycle phase

16 Decommissioning or disposal

5. Equivalence Map Concept

Mappings

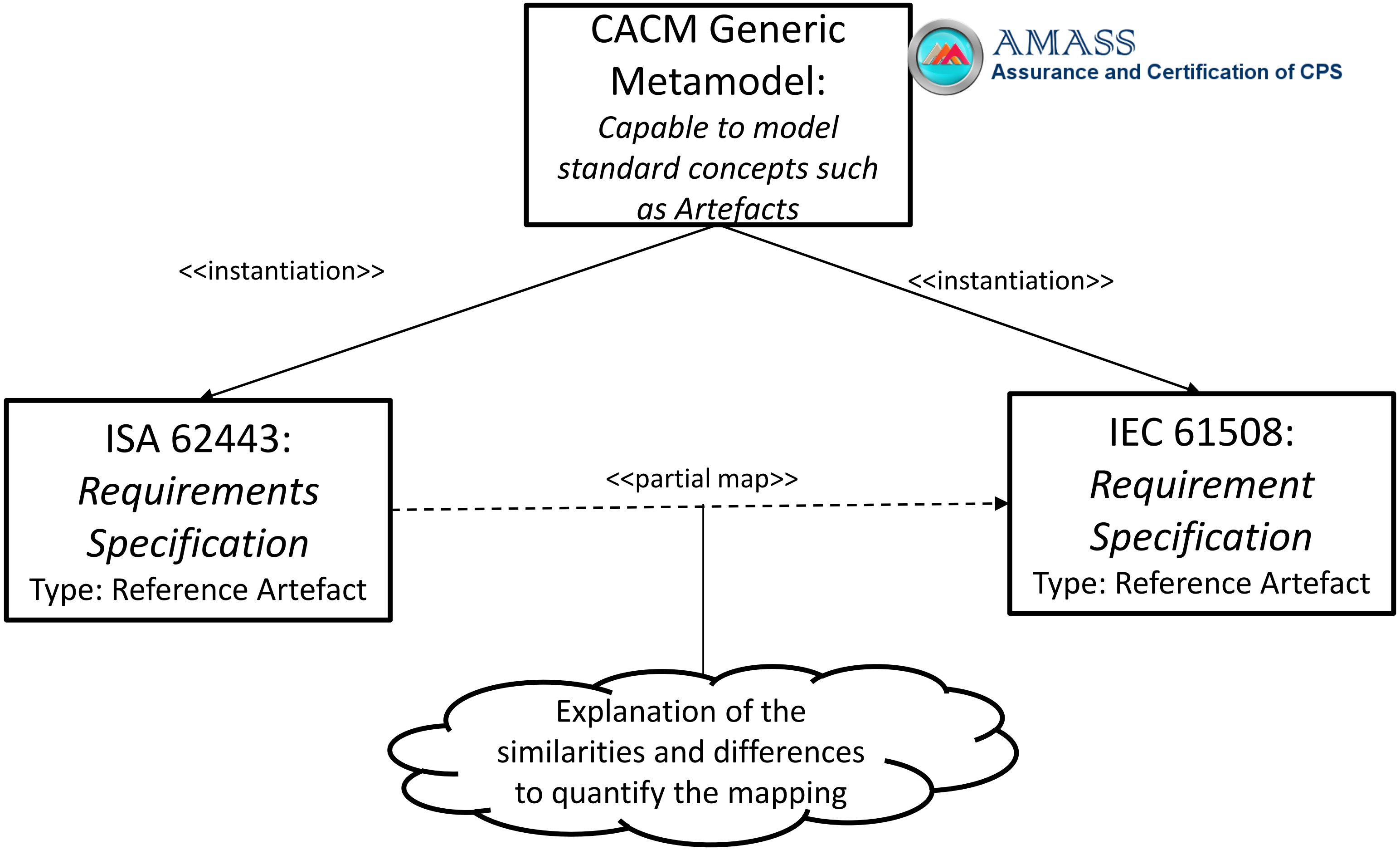
Why do we need mappings?

- To ‘match’ natural language elements in:
  - Concepts
  - Assurance assets
  - Activities
  - Objectives
  - Requirements
  - Argument claims
- Concept already proposed and used in R&D projects

OPENCOSS

AMASS
Assurance and Certification of CPS

Mappings



CACM Generic Metamodel: *Capable to model standard concepts such as Artefacts*

AMASS Assurance and Certification of CPS

<<instantiation>>

<<instantiation>>

ISA 62443: *Requirements Specification* Type: Reference Artefact

<<partial map>>

IEC 61508: *Requirement Specification* Type: Reference Artefact

Explanation of the similarities and differences to quantify the mapping

Mappings

Match of a mapping

- Full match
  - Terms are identical. The characteristics of the element referred to by Term A in its original context (its form, required content, objectives) fully satisfy those required of the element referred to by Term B
- Partial match
  - There is some similarity between the elements referred to by two terms, but they are not identical. Differences may be significant or insignificant
- No match
  - There is insufficient similarity between the elements to permit a match

Full Map example

ISA 62443 Cyber security	IEC 61508 Functional safety
Part 4-1 Practice 1 Security management. SM2: Identification of responsibilities A process shall be employed that identifies the organizational roles and personnel responsible for duties for each of the processes required by this standard.	***Part 1 - 6.2.1 Requirement*** An organisation with responsibility for an E/E/PE safety-related system, or for one or more phases of the overall, E/E/PE system or software safety life cycle, shall appoint one or more persons to take overall responsibility for: the system and for its life cycle phases; coordinating the safety-related activities carried out in those phases; (many other items were not included for space limitations)

Full Map example

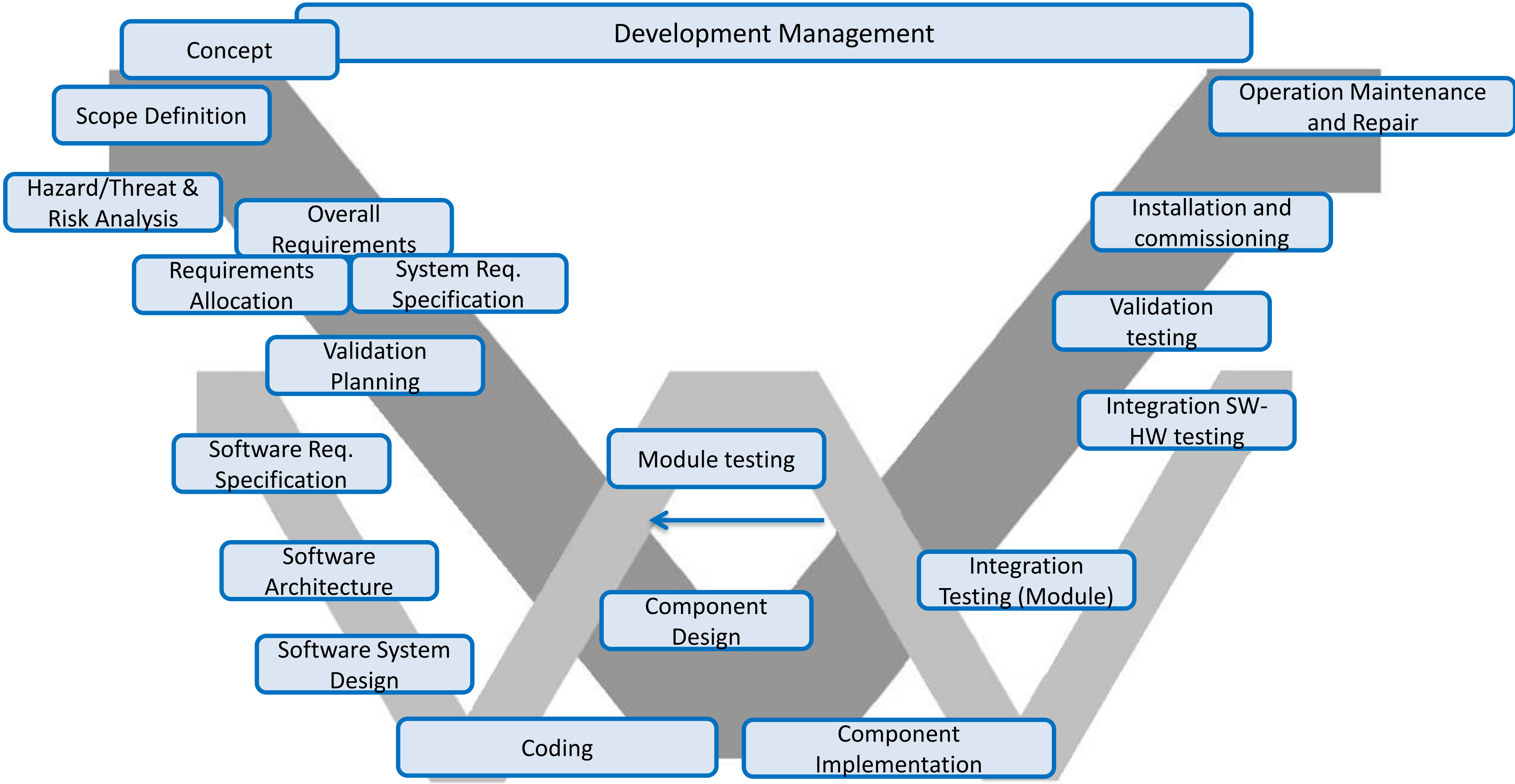
ISA 62443 Cyber security	IEC 61508 Functional safety
Part 4-1 Practice 1 Security management. SM4: Security Expertise process A process shall be employed for defining security training and assessment programs to ensure that personnel assigned to the organizational roles and duties specified in 6.3, SM2 - Identification of responsibilities, have demonstrated security expertise appropriate for those processes.	***Part 1 - Requirements:*** • ***6.2.3,*** • ***6.2.12,*** • ***6.2.13,*** • ***6.2.14,*** • ***6.2.15,*** • ***6.2.16***

Partial Map example

ISA 62443 Cyber security	IEC 61508 Functional safety
Part 4-1 Practice 1 Security management. ***SM7:*** ***Development environmental security*** A process that includes procedural and technical controls shall be employed for protecting the integrity of the development environment, production and delivery, including private keys, and the design, implementation and release of a product or product update (patch).	***Part 1 - 6.2.3 c) Requirement*** Software configuration management shall [...] maintain accurately and with unique identification all configuration items which are necessary to meet the safety integrity requirements of the E/E/PE safety related system. Configuration items include at least the following: safety analysis and requirements; software specification and design documents; software source code modules; test plans and results; verification documents; pre-existing software elements and packages which are to be incorporated into the E/E/PE safety related systems; all tools and development environment which are used to create or test or carry out any action on the software of the E/E/PE safety related system.

6. Co-engineering process in the automation sector

Co-engineering process



Life-cycle phase	IEC 61508 Functional safety	ISA 62443 Cyber security
Development Management	Part 1 6 Management of functional safety	Part 4-1 Practice 1: SM1, SM2, SM3, SM4, SM5
Concept Part	1 7.2 Concept	
Overall scope definition	Part 1 7.3 Overall scope definition	Part 4-1 Practice 2: SR1
Hazard/Threat and Risk Analysis	Part 1 7.4 Hazard and risk analysis	Part 4-1 Practice 2: SR2; Part 4-1 Practice 3: SD4, SD5; Part 4-1 Practice 5: SV3
Overall requirements	Part 1 7.5 Overall safety requirements	Part 4-1 Practice 2: SR3, Part 4-1 Practice 3: SD5; Part 4-1 Practice 8: SG1, SG2
Overall Requirements Allocation	Part 1 7.6 Overall safety Requirements Allocation	Part 4-1 Practice 2: SR3
System requirements Specification	Part 1 7.10 E/E/PE system safety requirements specification	Part 4-1 Practice 2: SR4
Software Requirement Specification	Part 3 7.2 Software safety requirements Specification	Part 4-1 Practice 2: SR4
Validation planning	Part 1 7.8 Overall safety validation planning Part 3 7.3 Validation Plan for SW aspects of system safety	Part 4-1 Practice 2: SR5 Part 4-1 Practice 3: SD3 Part 4-1 Practice 5: SV2, SV5
Software Architecture	Part 3 7.4.2 SW design and development. General Requirements Part 3 7.4.3 SW design and development. Requirements for SW Architecture design Part 3 7.4.4 SW design and development. Programming languages	Part 4-1 Practice 1: SM7 Part 4-1 Practice 3: SD1, SD2, SD6 Part 4-1 Practice 4: SI4
Software System Design	Part 3 7.4.5 SW design and development. Requirements for detailed designed - SW system design	
Coding	Part 3 7.4.6 requirements for code implementation	Part 4-1 Practice 1: SM6, SM7
Module Testing	Part 3 7.4.7 Requirements for SW module testing	Part 4-1 Practice 4: SI1, SI2, SI3
Integration Testing (Module)	Part 3 7.4.8 Requirements for SW integration testing	Part 4-1 Practice 4: SI2, SI3
Integration Testing (components, subsystems and programmable electronics)	Part 3 7.5 Programmable electronics integration (HW-SW)	Part 4-1 Practice 4: C17,SI2, SI3
Validation testing	Part 3 7.7 SW aspects of system safety validation	Part 4-1 Practice 5: SV3, SV4
Overall installation and commissioning	Part 1 7.14 Overall installation and commissioning	Part 4-1 Practice 8: SG1, SG2, SG3. SG4,SG5, SG6, SG7
Operation, maintenance and repair	Part 1 7.15 overall operation, maintenance and repair	Part 4-1 Practice 6: DM1, DM2, DM3, DM4, DM5, DM6 Part 4-1 Practice 7: PM1, PM2, PM3, PM4,PM5

Outcome from practitioners

- Promising approach to save effort
- Early trade-off identifications
- Still some reticence for common understanding between disciplines
- Co-engineering can be introduced for individual phases and, thus, step-by-step

Conclusions

- Current co-certification needs demand the introduction of co-engineering in mainstream practices
- Mapping of IEC 61508 and ISA 62443
- Suggested co-engineering process for the industrial automation sector

10th EDITION EUROPEAN CONGRESS
ERTS 2020
FROM 29th TO 31st JANUARY / TOULOUSE, FRANCE
PIERRE BAUDIS CONGRESS CENTER

EMBEDDED
REAL TIME SYSTEMS

Preliminary Safety and Security Co-engineering Process in the Industrial Automation Sector

✉ alejandra.ruiz@tecnalia.com

@a_ruizTECNALIA

Alejandra Ruiz, Javier Puelles, Jabier Martinez (Tecnalia)
Thomas Gruber (Austrian Institute of Technology)
Martin Matschnig, Bernhard Fischer (Siemens AG Austria)

AQUAS SAFETY SECURITY PERFORMANCE
H2020-ECSEL Grant agreement 737475

https://aquas-project.eu/