KU LEUVEN

Co-assuring Security and Safety during Software Development

Dr. Ing. Jens Vankeirsbilck

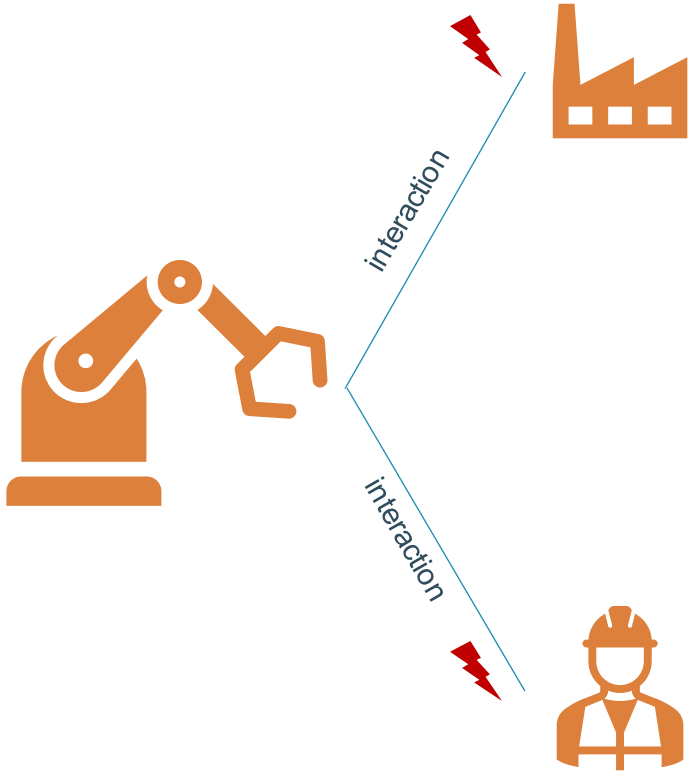
DistriNet m·group

VLAIO Tetra Co-Assurance

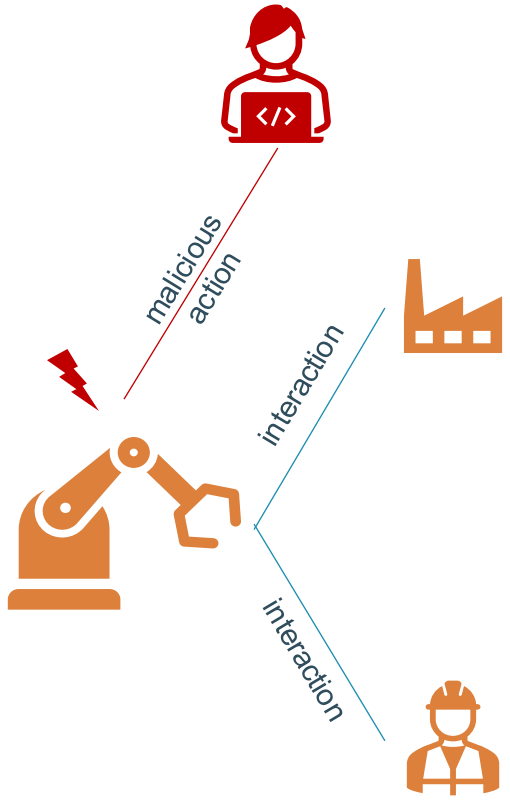
- Following slides are a summary of some of the research performed during the VLAIO Tetra Co-Assurance
- Insights combined into a meta cookbook

Introduction

Safety



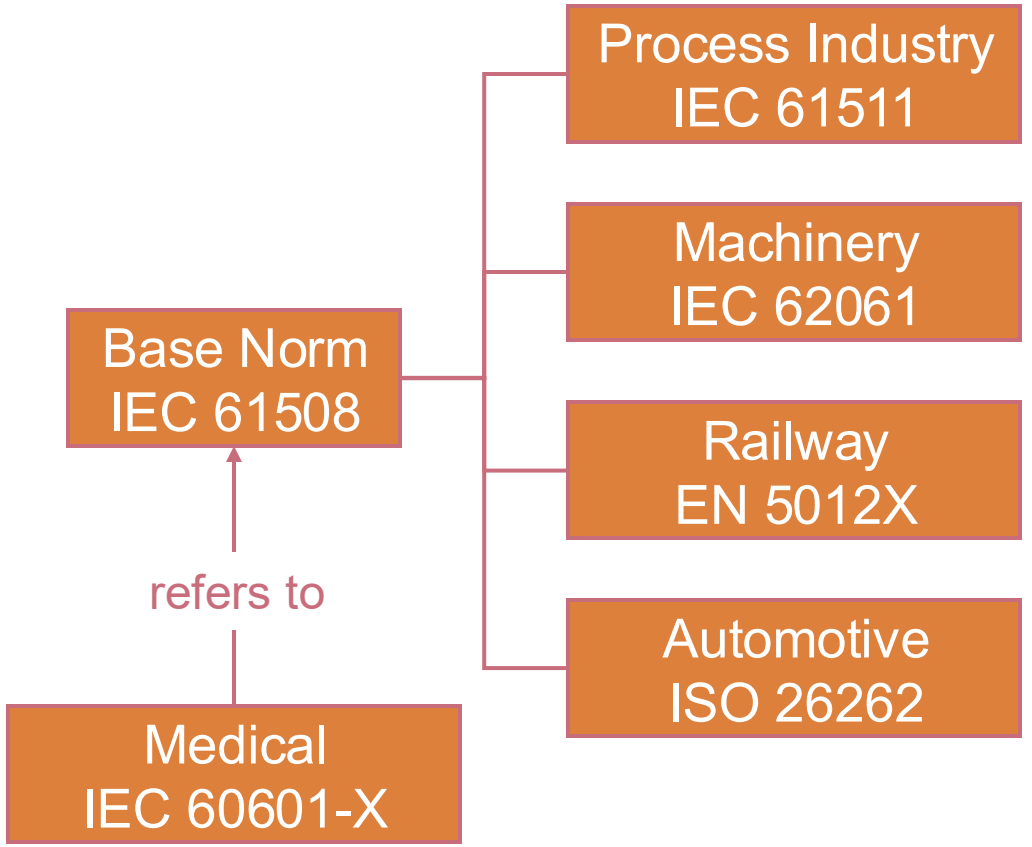
Security



Introduction – Functional Safety and IEC 61508

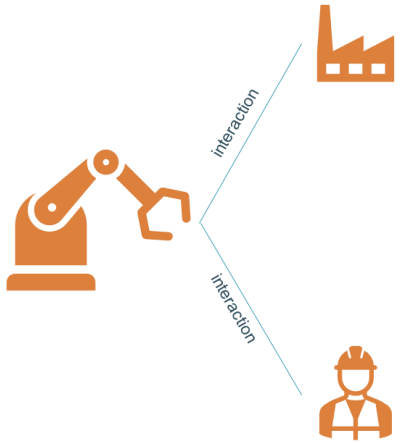
"**Part of the overall safety** relating to the EUC and the EUC control system that **depends** on the **correct functioning** of the **E/E/PE** safety-related systems and other risk reduction measures."

Source: IEC 61508-4:2010, 3.1.12

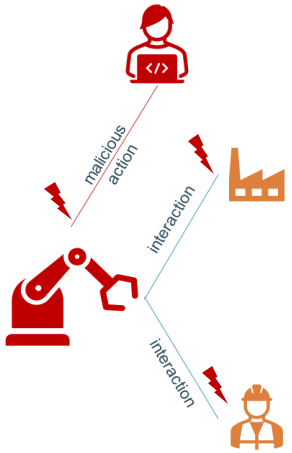


Introduction – Need for Co-engineering

Safety



Security



IoT and I4.0 leads to Cyber-Physical Systems (CPS).

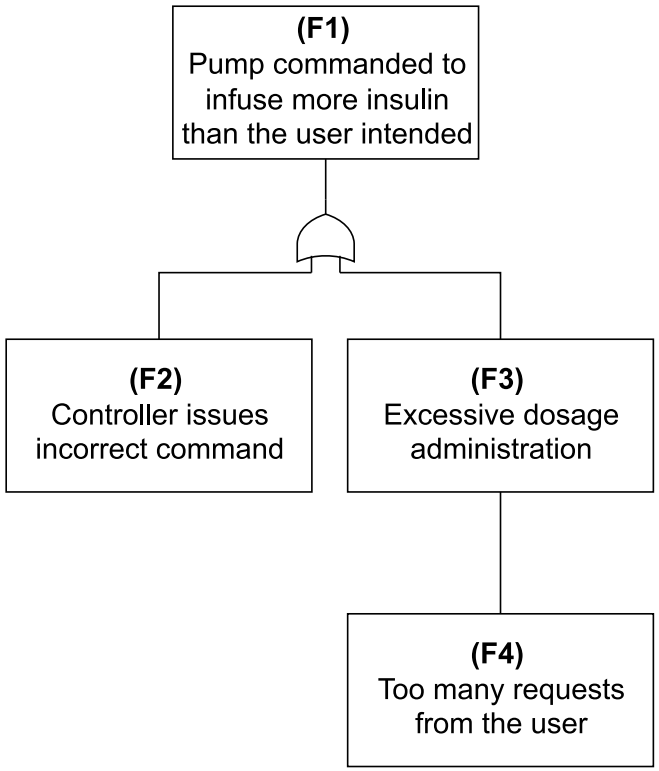
CPS include safety-critical systems: Medical devices, etc.

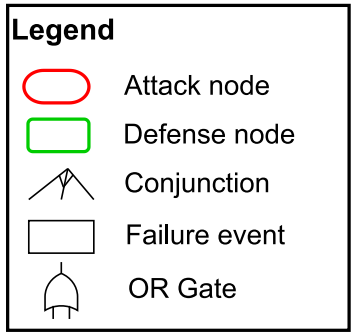
No safety without security, or vice-versa!

Introduction – Need for Co-engineering

Insulin Pump Example: **Without** Co-engineering

Safety assurance artifact: Fault tree analysis





Security assurance artifact: Attack-defense tree

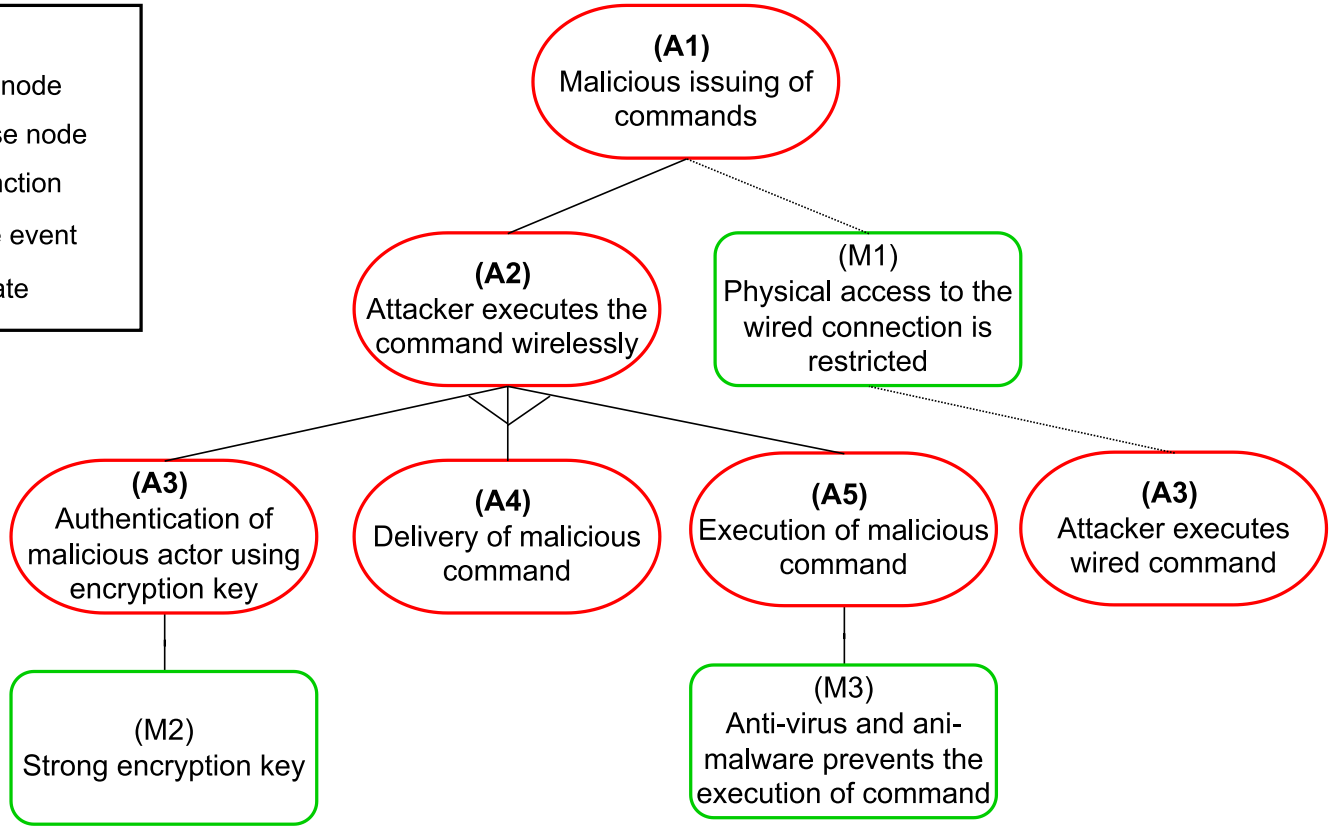
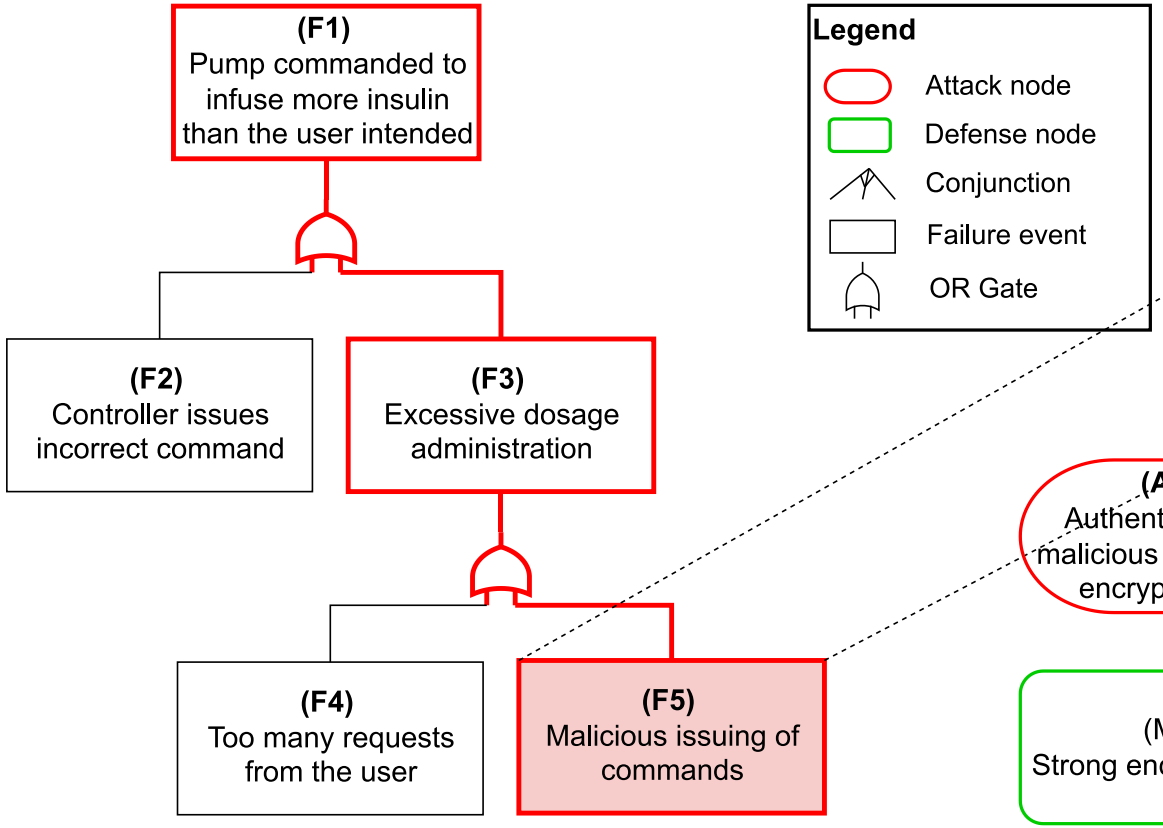


Image adapted from 'Assuring Safety and Security', N. L. Johnson, Ph.D dissertation, University of York, 2020.

Introduction – Need for Co-engineering

Insulin Pump Example: **With** Co-engineering

Co-assurance artifact: Safety fault tree augmented with cross-domain risk



Security assurance artifact: Attack-defense tree

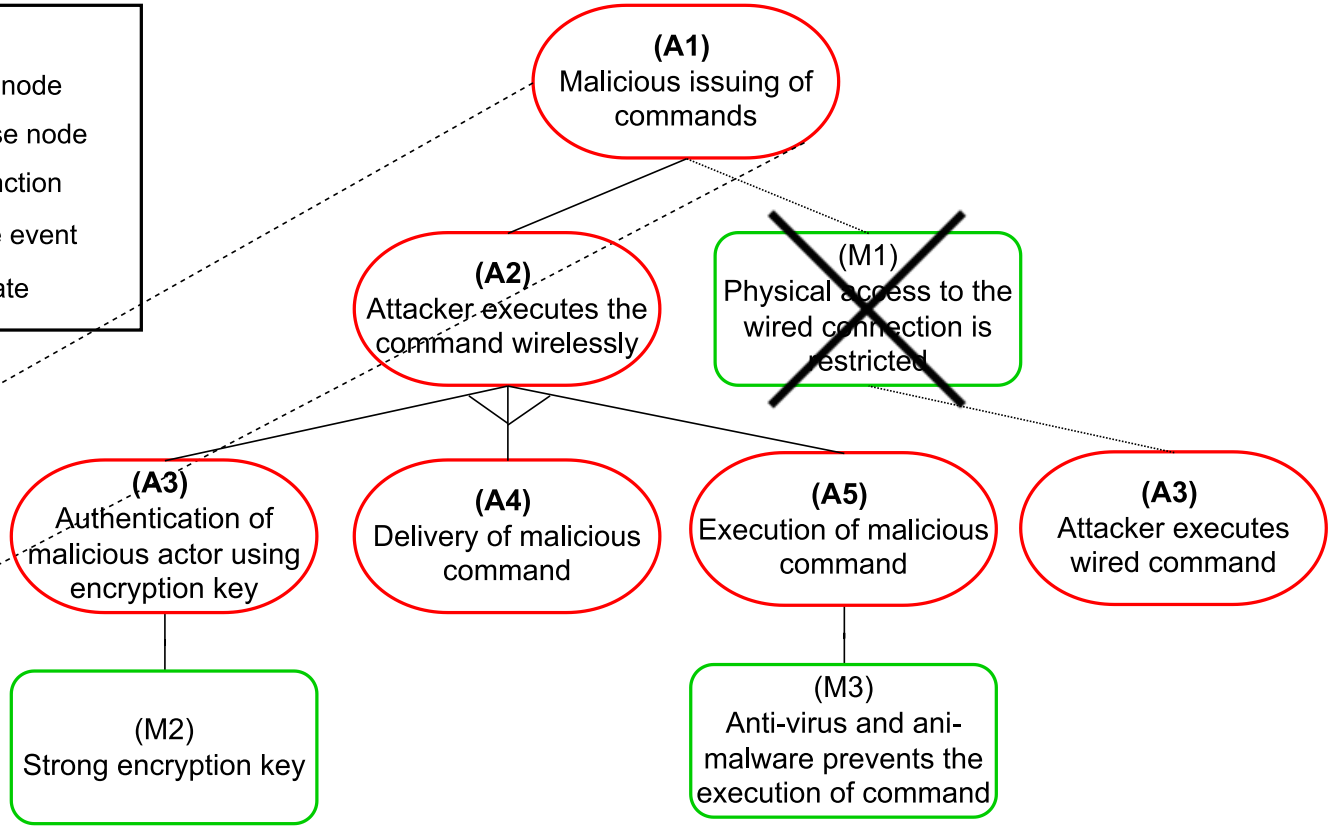


Image adapted from 'Assuring Safety and Security', N. L. Johnson, Ph.D dissertation, University of York, 2020.

Introduction – Need for Co-engineering

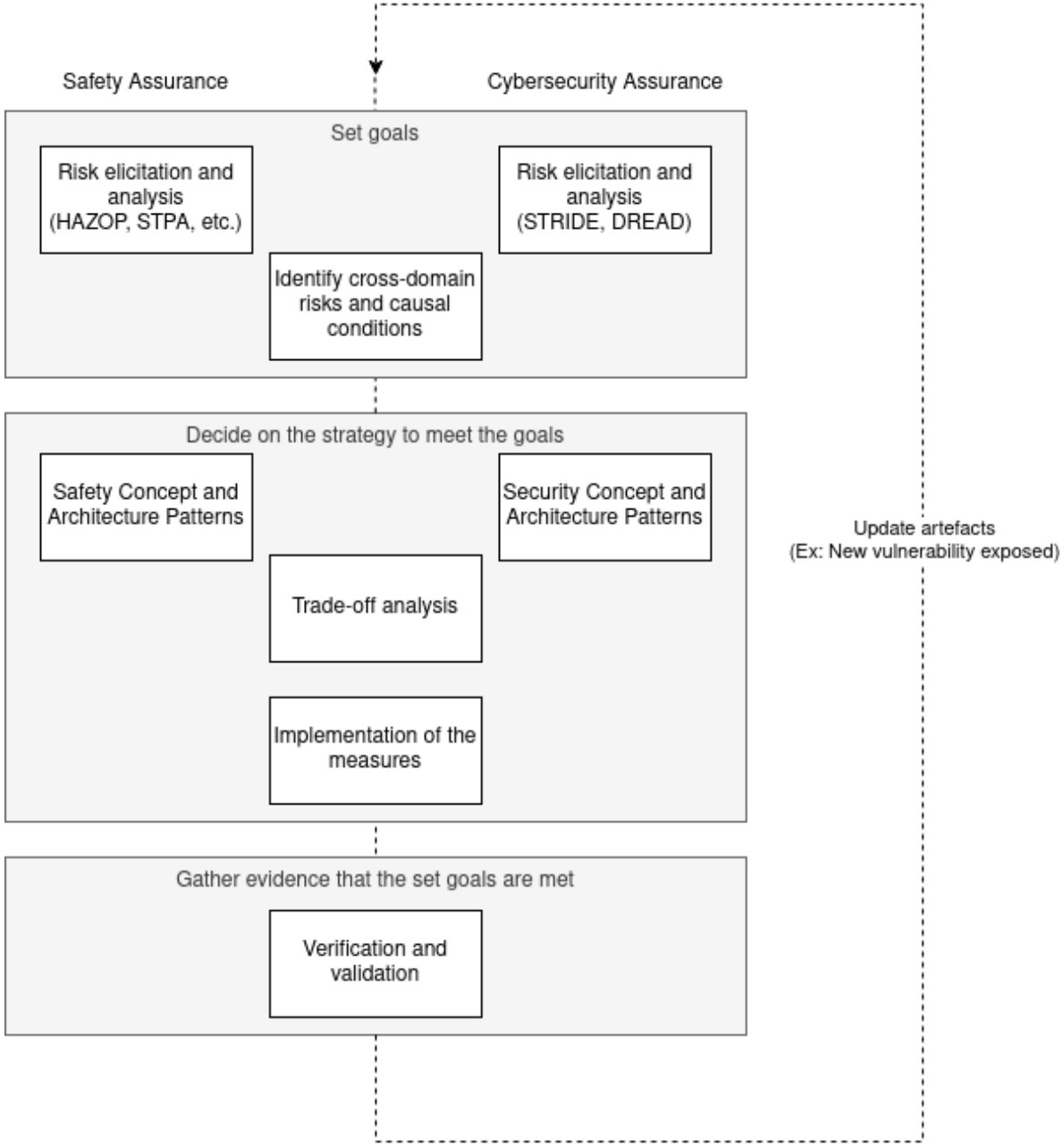
- For most domains, separate safety and security standards exist.
  - Ex: IEC 61508 (Safety), IEC 62443 (Security)
- Interplay between safety and security addressed to varying degrees.

- However, legislation and safety regulations are changing.
  - Cyber Resilience Act
  - EU Vehicle General Safety Regulation mandates the UN R 155 on “Cyber security and cyber security management system”

- Therefore, along with safety & security assurance, co-engineering is needed.

Co-engineering

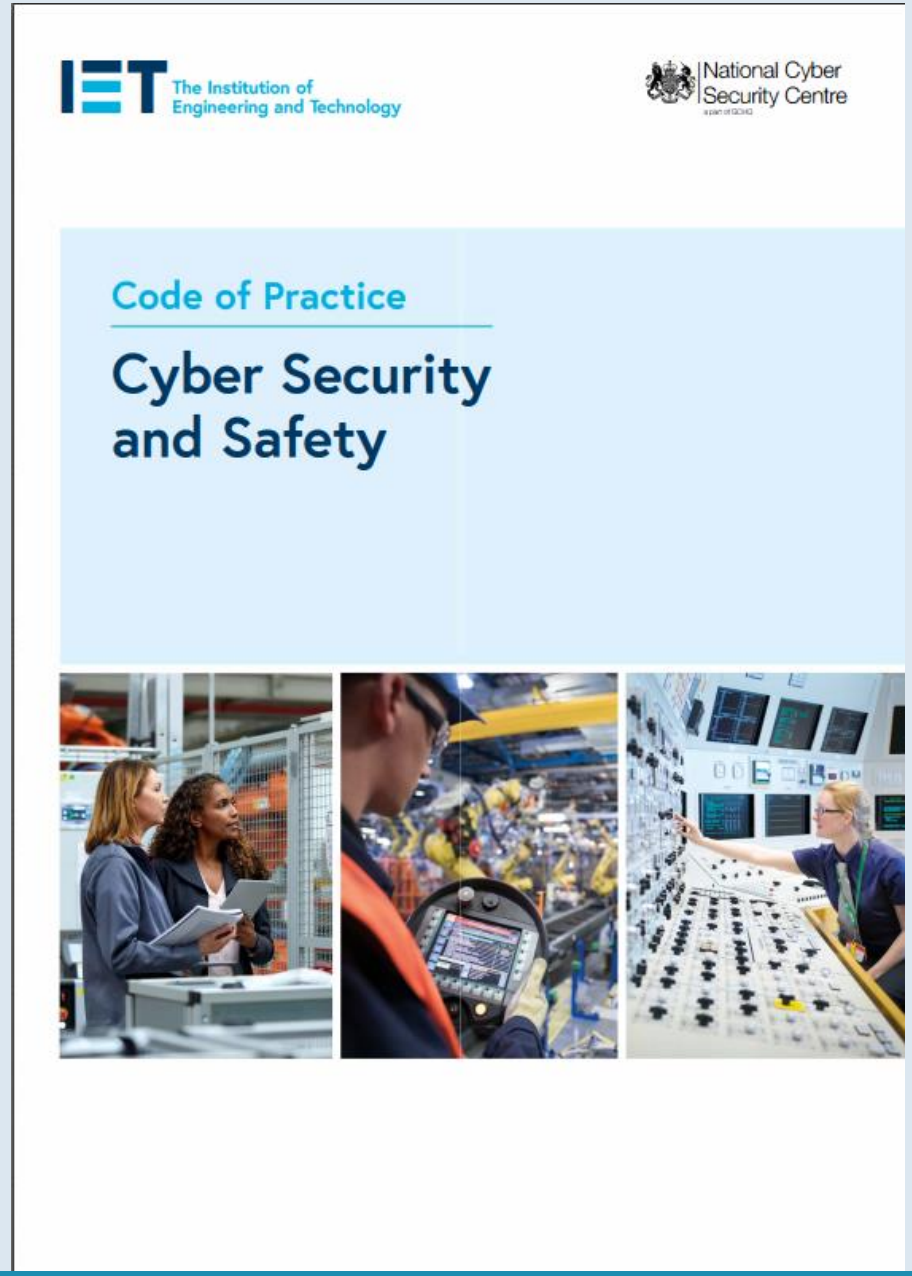
- An extension of single domain assurance
- Management of cross-domain risks
  - Safety → Cyber-security
  - Cyber-security → Safety
- Continuous process
  - As new vulnerabilities get exposed regularly



Co-engineering - Standards and Guidelines

Domain	Assurance		
	Security-informed Safety	Safety-informed Security	Co-engineering Security and Safety
General	IEC 61508	ISO 27000 series ISO/IEC 15408 NIST SP 800-213A	IET Code of Practice: Cybersecurity and Safety
Industrial Control	IEC 61508 IEC 61511 ISO 13849	IEC 62443 NIST SP 800-82	IEC TR 63069 ISA TR 84.00.09
Automotive	ISO 26262 ISO 21448 ISO TR 4808	ISO 21434	
Healthcare & Medical Devices	ISO 14971 IEC 60601 series FDA Safety	AAMI TIR57 IEC 80001 series IEC 81001 series MDCG 2019-16 FDA Security	
Railway	CENELEC EN 50126 CENELEC EN 50128 CENELEC EN 50129	CENELEC TS 50701	

IET Code of Practice – Cyber Security and Safety



IET COP Cyber Security and Safety

COP

Guiding document

Based on discussion between IET's Technical and Professional Networks

Guiding Principles

Systems engineering approach

Safety and Security are mostly complementary risk-based approaches

Target audience

Safety and Cyber security practitioners; and

Their managers

1. Introduction

Aim: help safety-related system practitioners manage cyber security vulnerabilities that could lead to hazards.

Systems have become increasingly interconnected and safety-related systems are being attacked.

Cyber security vulnerabilities that could lead to hazards and accidents must be managed – safety legislation and regulation is changing.

Safety and cyber security specialists need to work together at their intersection.

Annex A: Glossary and abbreviations

2. Challenges at the intersection of safety and security

Functional safety and cyber security are different, having evolved from different paradigms, but have a common high level risk management approach

Safety and cyber security differ in risk identification, assessment, treatment, acceptance and ongoing management control.

Annex C: Introduction to safety, security, systems engineering

3. Shared principles for safety and security

Shared management principles: accountability, governance, management, culture, competence, supply chain

Shared engineering principles: applied to functional safety and cyber security in a common systems engineering approach throughout the lifetime of the system.

Annex D: Indicators of good practice.

4. Applying the Code

Engineers are best placed to understand the need and deliver the change. Boards have an obligation to see that this is done. Regulators, shareholders and the supply chain have responsibilities.

Annex E: Techniques and measures.

Annex F: Bibliography for additional references

15 Shared principles for safety and security

Category	#	Title
Management and Governance	1	Accountability for safety and security of an organization's operations is held at board level
	2	The organization's governance of safety, security and their interaction is defined
	3	Demonstrably effective management systems are in place
	4	The level of independence in assurance is proportionate to the potential harm
Culture and Competence	5	The organization promotes an open/learning culture whilst maintaining appropriate confidentiality
	6	Organizations are demonstrably competent to undertake activities that are critical to achieving security and safety objectives.

15 Shared principles for safety and security

Category	#	Title
Supply Chain	7	The organization manages its supply chain to support the assurance of safety and security in accordance with its overarching safety/security strategy
System Engineering	8	The scope of the system-of-interest, including its boundary and interfaces, is defined
	9	Safety and security are addressed as coordinated views of the integrated systems engineering process.

15 Shared principles for safety and security

Category	#	Title
Risk Management	10	The resources expended in safety and security risk management, and the required integrity and resilience characteristics, are proportionate to the potential harm
	11	Safety and security assessments are used to inform each other and provide a coherent solution
	12	The risks associated with the system-of-interest are identified by considerations including safety and security
	13	System architectures are resilient to faults and attack
	14	The risk justification demonstrates that the safety and security risks have been reduced to an acceptable level
	15	The safety and security considerations are applied and maintained throughout the life of the system

Principles are broken down into practices with indicators of good vs. improve

Principle	Practice(s)	Indicator Good Practice	Indicator Need to Improve
11. Safety and Security assessments are used to inform each other and provide a coherent solution	1)Techniques should be selected that are appropriate to the lifecycle point and the objective of the assessment 2)Interaction points between security and safety assessments should be identified and communicated 3)The results of assessment should be expressed together with a measure of confidence	+The outputs of process hazard analysis procedures, e.g. HAZOP, inform cyber security analysis +HAZOP can consider multiple contingencies to cover malicious action +The generally and inevitably more qualitative nature of security risk assessment is recognized	• There is no interaction of safety and security in the identification of risks to OT • The safety risk analysis does not consider risks arising from malicious action • Security analysis does not consider the outputs of hazard analysis activities

Conclusion

- Very high-level document
  - Useful as a starting point
  - Quick overview of all that's affected by co-engineering Safety and Security
  - If you had some idea already, probably won't learn much new information
- Annexes might hold most value
  - Annex B contains some examples of how cyber attacks impacted safety
  - Annex D contains the indicators of good practice
  - Annex E lists techniques and measures for risk management where security impacts safety

IEC TR 63069:2019

Industrial-process measurement, control and automation –
Framework for functional safety and security

IEC TR 63069:2019
Industrial-process measurement, control and automation - Framework for functional safety and security

Technical Report

Informative

Publication date: 2019-05

On its way to become a Technical Specification

Framework for common application:

IEC 61508

IEC 62443

Scope: Industrial process measurement, control and automation

Also applicable to other areas where above norms apply!

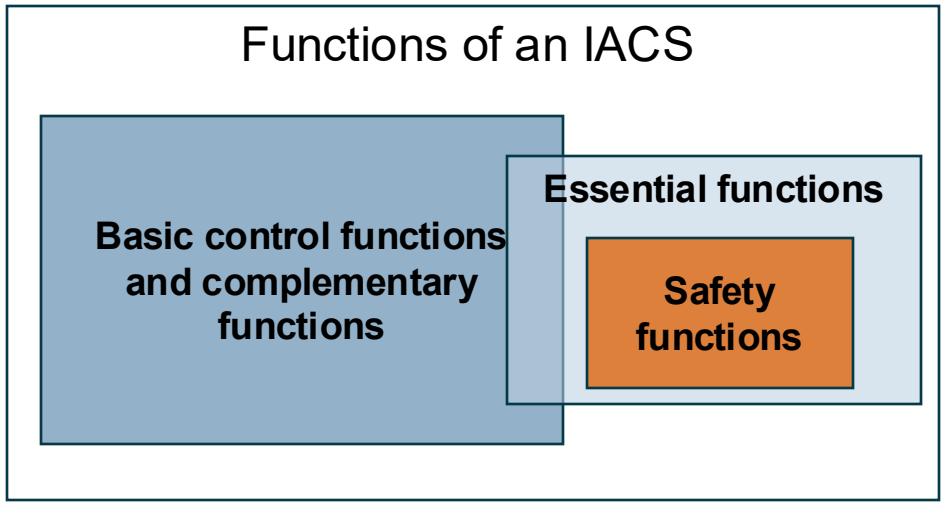
Target audience

Asset owners, system integrators, product suppliers, service providers, authorities

IEC TR 63069:2019

Industrial-process measurement, control and automation - Framework for functional safety and security

Types of functions in an IACS

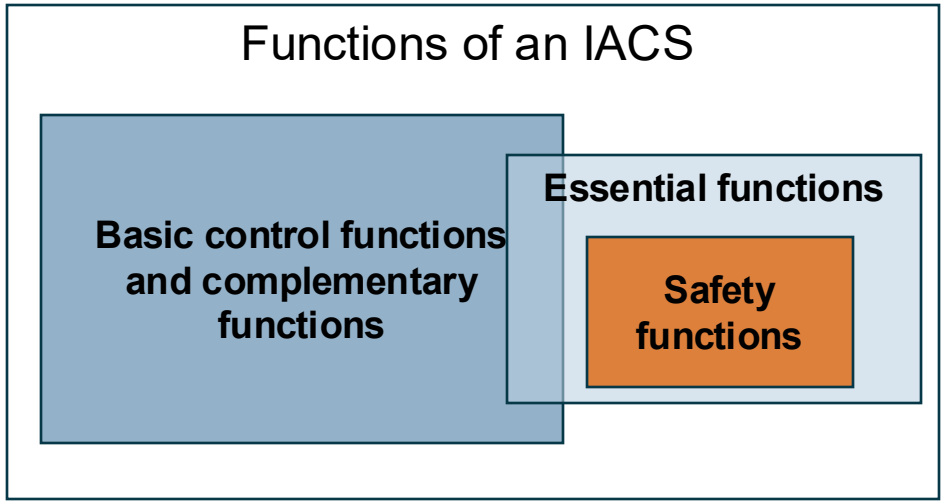


- Logging - Essential function
- Emergency stop – Safety function

IEC TR 63069:2019

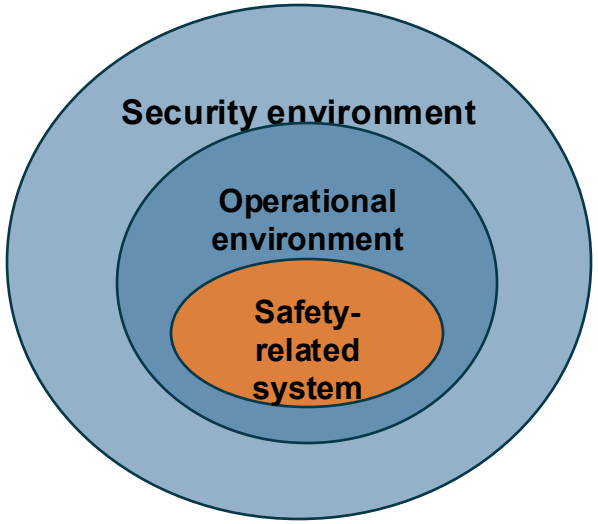
Industrial-process measurement, control and automation - Framework for functional safety and security

Types of functions in an IACS



- Logging - Essential function
- Emergency stop – Safety function

Security environment

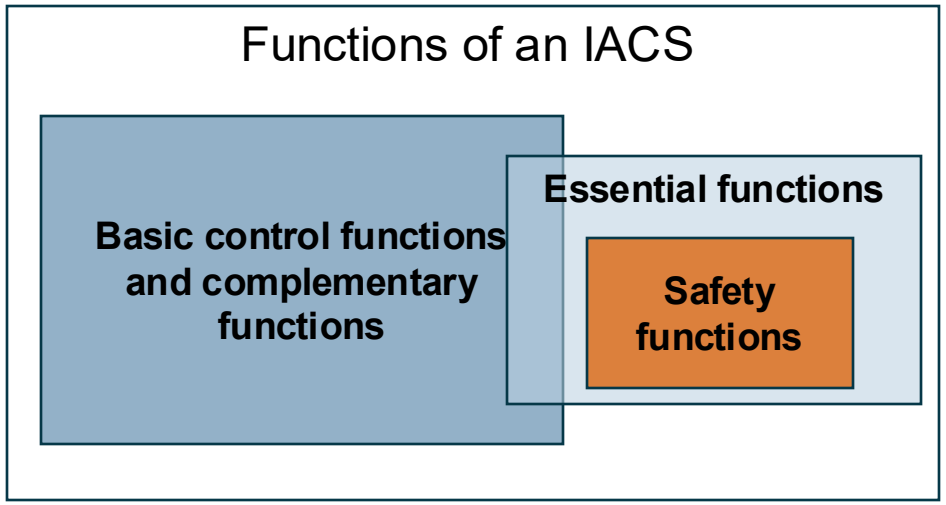


- Collection of countermeasures.
- Protects essential functions.
  - Ex: Defense in depth, security perimeter, vulnerability management

IEC TR 63069:2019

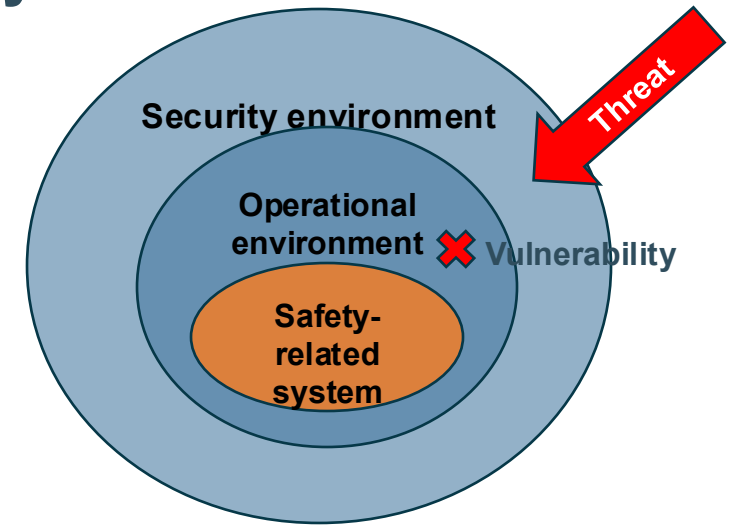
Industrial-process measurement, control and automation - Framework for functional safety and security

Types of functions in an IACS



- Logging - Essential function
- Emergency stop – Safety function

Security environment



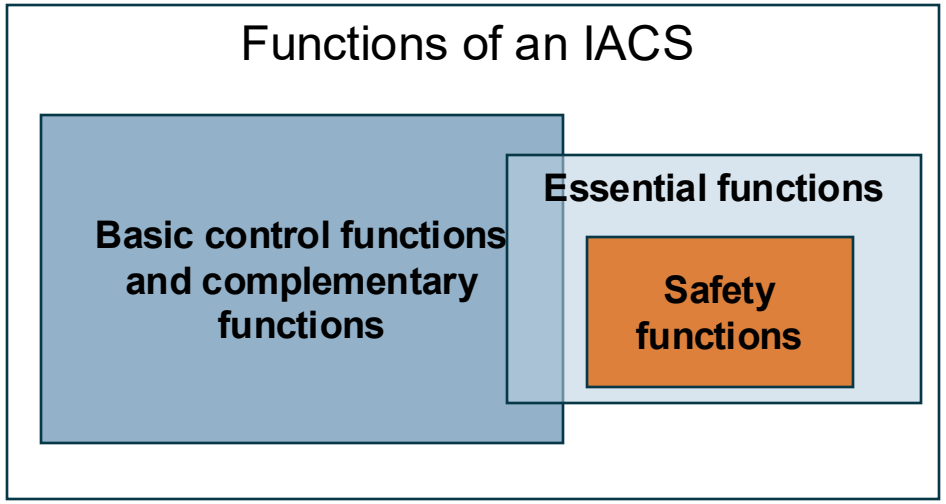
- Collection of countermeasures.
- Protects essential functions.
  - Ex: Defense in depth, security perimeter, vulnerability management

Image recreated from IEC TR 63069:2019

IEC TR 63069:2019

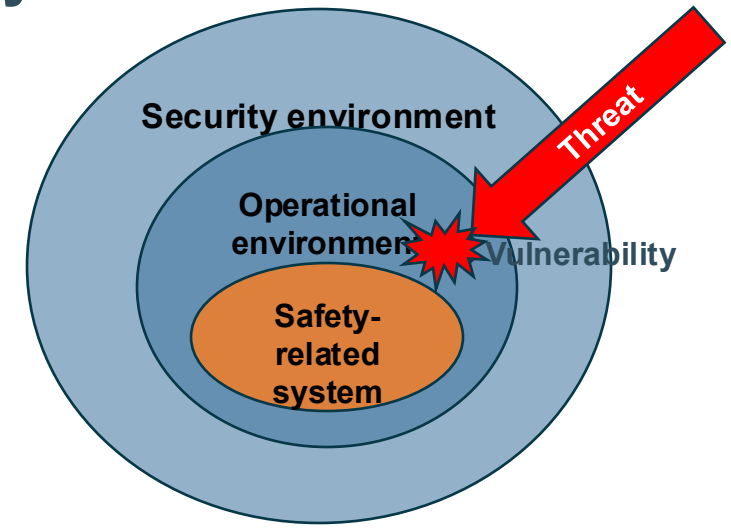
Industrial-process measurement, control and automation - Framework for functional safety and security

Types of functions in an IACS



- Logging - Essential function
- Emergency stop – Safety function

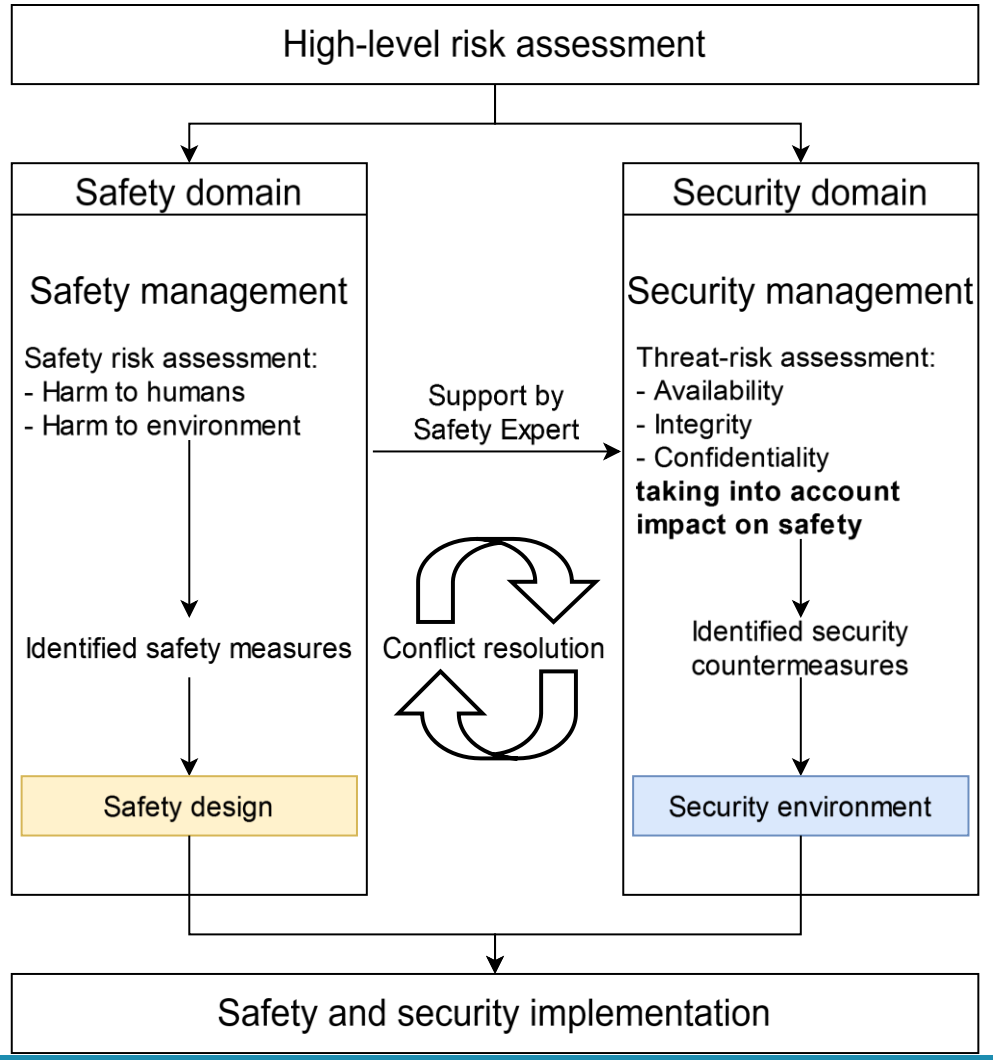
Security environment



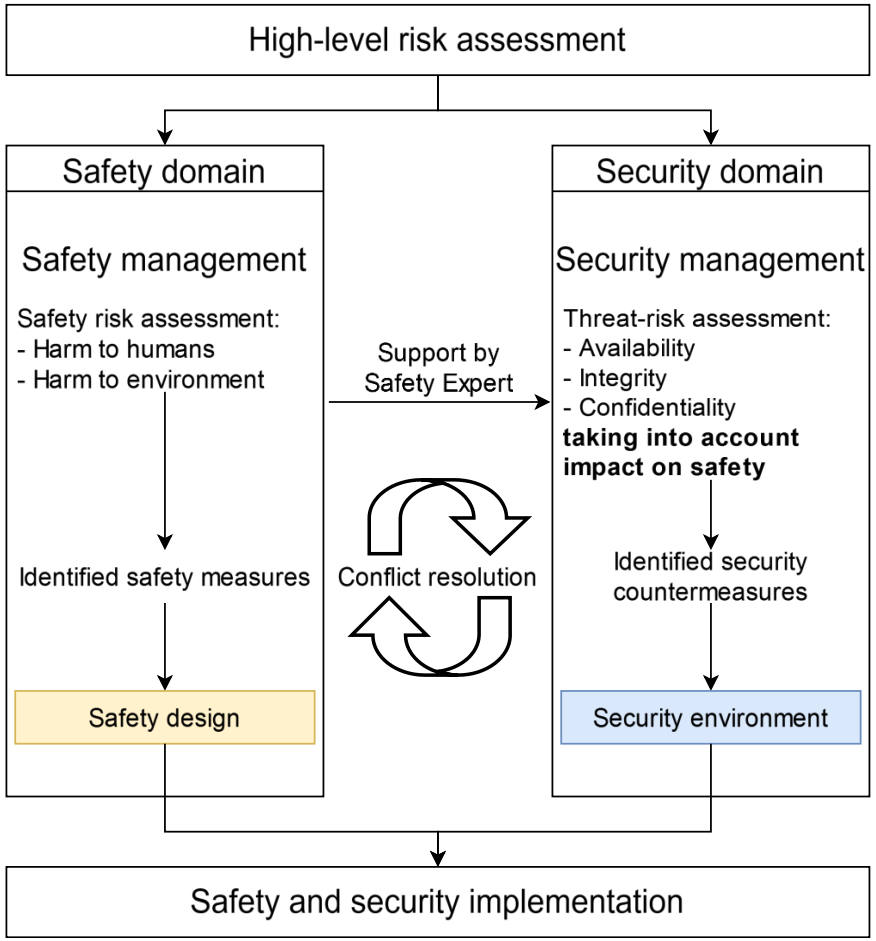
- Collection of countermeasures.
- Protects essential functions.
  - Ex: Defense in depth, security perimeter, vulnerability management

Image recreated from IEC TR 63069:2019

IEC TR 63069:2019 – Co-engineering lifecycle



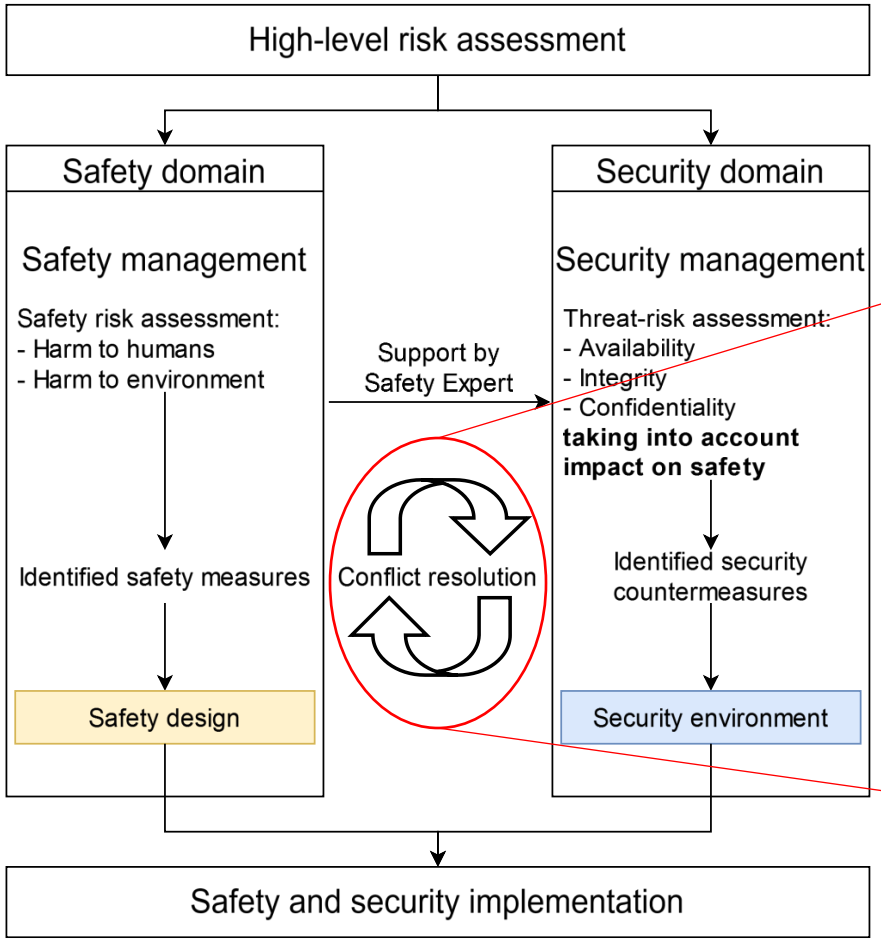
IEC TR 63069:2019 - Co-engineering lifecycle



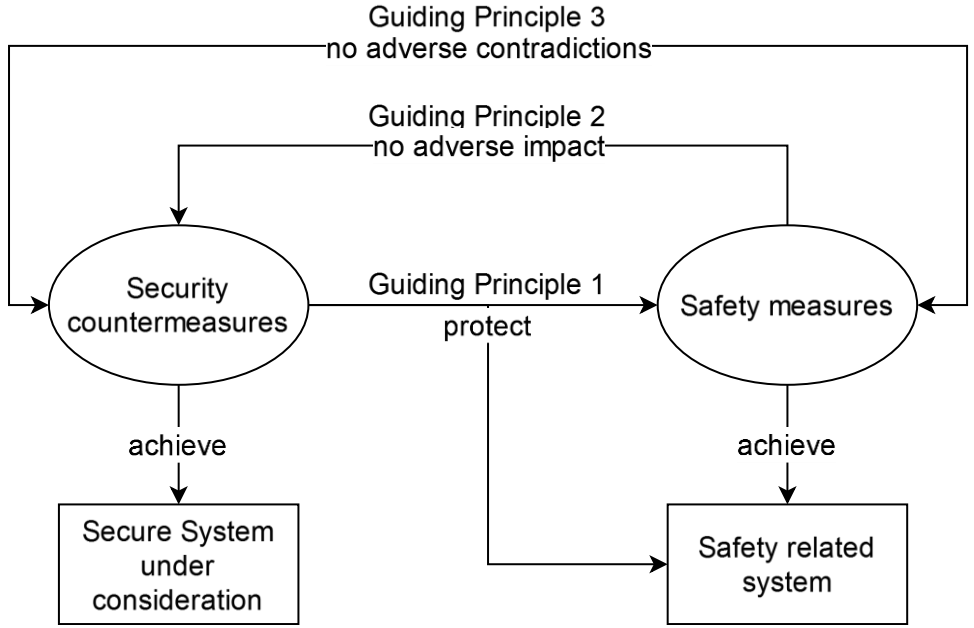
General remarks:

- Safety managed according to IEC 61508 (all parts)
- Security management according to IEC 62443 (all parts)
- Parallel development
- Security elements are not part of the safety risk assessment.
- Conflict resolution needs consensus.
  - Guiding principles apply!

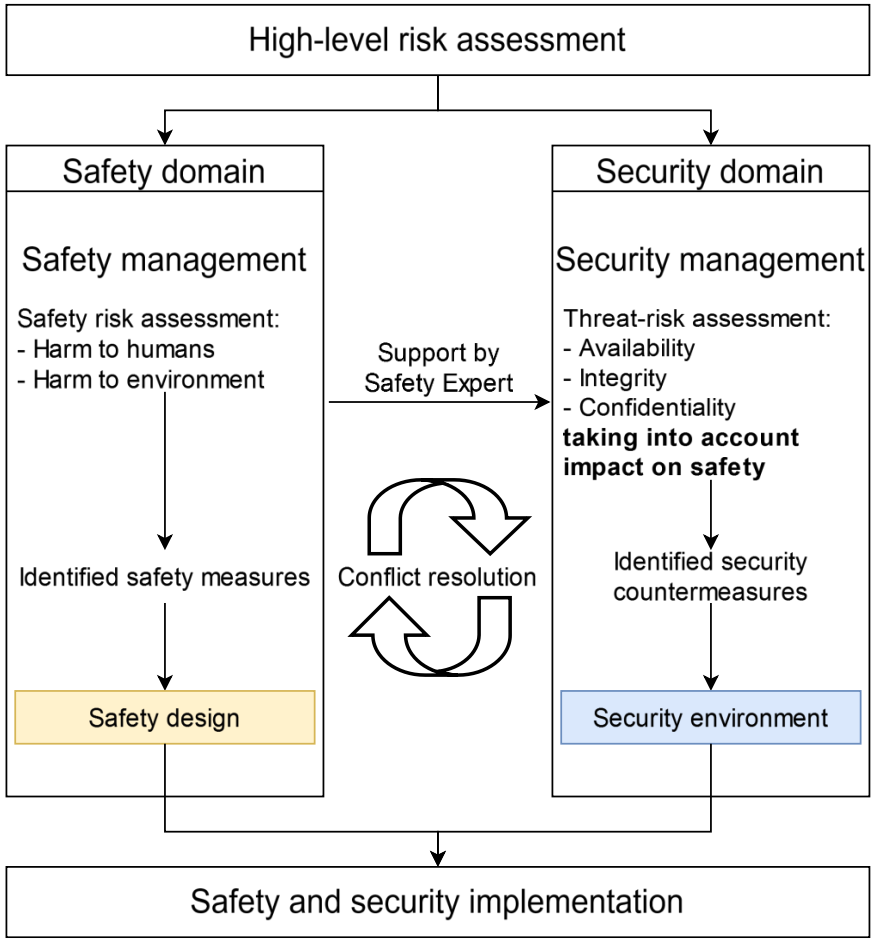
IEC TR 63069:2019 - Co-engineering lifecycle



Guiding principles:



IEC TR 63069:2019 - Co-engineering lifecycle



Safety and security management

- Safety risk assessment assumes effective (security) countermeasures.
- Security elements are not part of the safety risk assessment.
  - As it is covered in the security threat-risk assessment
  - Needs experts from both domains
- Any threat-risk to the safety function should have a countermeasure.

Conclusion

- Informative framework for the combined application of IEC 61508 & IEC 62443
  - Central idea: security environment encapsulating the *essential functions*
  - Based on a high-level risk assessment, then parallel development for the two domains
  - Suggesting 3 guiding principles to judge impact of one domain on the other
- Although written for industrial control processes, can be applied in other domains

- While it feels more concrete than the IET CoP, remains high-level and less hands-on than often desired (or needed)

Current research track

CONSENSUS: Co-Engineering Safety and Security using Ontologies

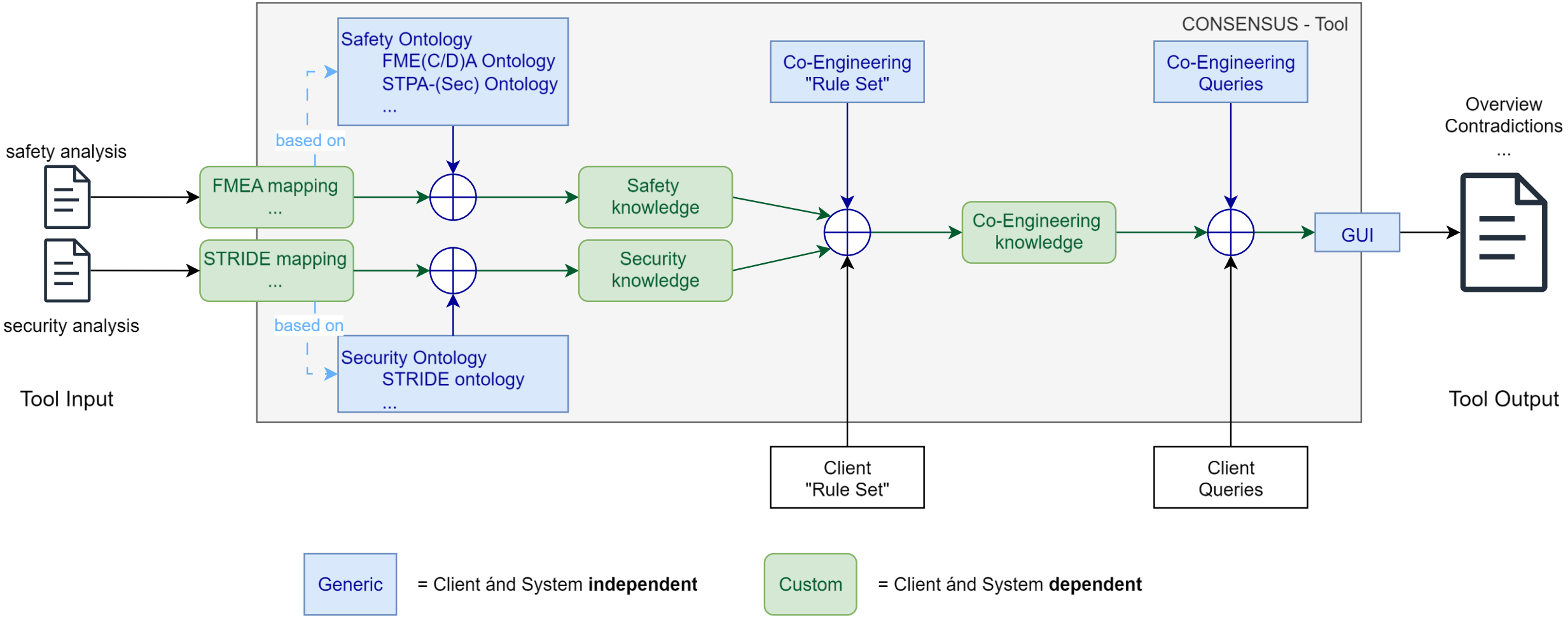
Co-engineering – Practical Challenges

- Knowledge from safety domain and security domain are not readily combinable to generate insights.
- Cross-domain influences are not adequately considered.
- Gaps in co-engineering lead to safety and security issues.
- Managing gaps relies on experience.

- Investigating tool-based solution to manage (some) of the gaps **continuously.**
  - Using ontologies and knowledge bases.

Demo:

Safety and Security Co-engineering Tool



Summary

No safety without security, and vice versa!

- Co-engineering of safety and security is needed throughout the lifecycle of a CPS.
  - Manage cross-domain risks and have adequate control measures in place.
- Separate standards for safety and security exist, but interplay is addressed to varying degrees.
  - But (safety) regulation is changing to include cyber risks.
- Some frameworks exists, more (concrete & domain-specific) guidance needed
  - E.g. IET COP and IEC 63069
- Currently exploring tool-based support
  - Next steps: expanding capabilities & industrial validation

Want to know more?
Let's connect!

Contact details

Jens Vankeirsbilck

Tel. +32 487 613 503

Jens.Vankeirsbilck@kuleuven.be

Spoorwegstraat 12 –

8200 Brugge

https://iiw.kuleuven.be/onderzoek/m-group

Contact details

Jeroen Boydens

Tel. +32 486 796 390

Jeroen.Boydens@kuleuven.be

Spoorwegstraat 12 –

8200 Brugge

https://iiw.kuleuven.be/onderzoek/m-group