The 13th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2023
13-15 October, 2023, Athens, Greece

# Towards Effective Safety and Cybersecurity Co-engineering in Critical Domains

Ievgen Babeshko
*National Aerospace University "KhAI"*
Kharkiv, Ukraine
e.babeshko@csn.khai.edu
*Istituto di Scienza e Tecnologie dell'Informazione "Alessandro Faedo" ISTI-CNR*
Pisa, Italy
ievgen.babeshko@isti.cnr.it

Oleg Illiashenko
*National Aerospace University "KhAI"*
Kharkiv, Ukraine
o.illiashenko@khai.edu
*Istituto di Scienza e Tecnologie dell'Informazione "Alessandro Faedo" ISTI-CNR*
Pisa, Italy
oleg.illiashenko@isti.cnr.it

Felicita Di Giandomenico
*Istituto di Scienza e Tecnologie dell'Informazione "Alessandro Faedo" ISTI-CNR*
Pisa, Italy
felicita.digiandomenico@isti.cnr.it

***Abstract*—The primary objective of functional safety and cybersecurity co-engineering is to streamline assessment processes and enhance efficiency by implementing integrated approaches, therefore reducing overall effort and bringing several consequential advantages. Although this concept is not new, and there have already been successful attempts at its utilization in different critical domains such as nuclear, railway, and automotive, no mature approach could be easily adopted and applied during the assessment. Another challenge is that the understanding of co-engineering is essentially different, depending on domain specifics and priorities. Moreover, issues are still related to measuring efficiency achieved by co-engineering utilization. This paper addresses the current state of safety and cybersecurity co-engineering in critical domains. With a focus on nuclear, automotive, and railway domains, it proposes directions toward developing effective co-engineering frameworks for them.**

***Keywords—Safety; Cybersecurity; Assessment Techniques; Co-engineering***

## I. INTRODUCTION

A unified, efficient, and verifiable approach is the primary target of the safety and cybersecurity co-engineering concept. Its primary purpose is to reduce duplication of assessment efforts and obtain more precise and trustworthy results. Besides that, co-engineering also presents a range of attendant benefits. Among them are the following ones:

- Identification of safety and cybersecurity interdependencies: joint safety and cybersecurity methodologies facilitate the revealing of interconnections and interdependencies that exist between these two areas, providing a holistic view of overall safety;
- Harmonized safety and cybersecurity measures: safety and cybersecurity measures are coordinated and complement each other;
- Adaptive response strategies: integrated understanding of safety and cybersecurity allows swift adjustment of tactics in response to dynamic threats;
- Enhanced communication with stakeholders: a unified strategy encompassing safety and cybersecurity is more comprehensive to licensing and regulatory bodies, clients, and partners;
- Efficient resource utilization: by combining functional safety and cybersecurity efforts, manufacturers can optimize the use of resources, including time and personnel. Cross-functional teams can collaborate effectively, reducing duplication of work and streamlining processes. This efficiency can lead to cost savings and faster time-to-market for vehicles;
- Improved resilience: co-engineering helps create products more resilient to emerging safety and cybersecurity challenges. It allows for proactive measures to protect against potential threats and vulnerabilities. As new threats arise, vehicles designed with co-engineering principles can adapt and evolve to maintain their safety and security features.

At the same time, the following challenges exist that prevent safety and cybersecurity co-engineering from widespread utilization:

- Differing expertise and mindsets: safety and cybersecurity require distinct expertise and often have different organizational structures within the companies;
- Lack of a comprehensive approach: there is a clear need for frameworks that facilitate safety and cybersecurity integration seamlessly;
- Shortcomings of the normative documents: existing safety and cybersecurity international standards and regulations are usually confined to guidance on safety and cybersecurity coordination points within the lifecycle while

not providing detailed methodologies for such coordination;

- Rapid technological evolution: different industries are undergoing rapid technological advancements, particularly with the introduction of artificial intelligence and interconnectivity of the devices produced by original equipment manufacturers (OEMs). This fast-paced environment makes it challenging to establish comprehensive safety and cybersecurity standards to keep up with emerging threats and vulnerabilities.
- Lack of effectiveness confirmation: there are no practical confirmations for the claims that approaches targeting safety and cybersecurity co-engineering help reduce effort and costs;
- Complexity and cost: integrating safety and cybersecurity measures from the early stages of product development can add complexity and cost to the process. It may involve additional testing, validation, and security measures that increase development expenses and time-to-market;
- Lack of methods for assessing efficiency: there are no practical guidelines on how to measure the efficiency of existing practices and processes to adapt them and make them more effective;

Triggered by the abovementioned challenges, in this work, we focus on safety and cybersecurity co-engineering in different critical domains, striving to develop a unified framework able to effectively respond to the needs of nowadays dependability and resilience requirements. The paper describes research results obtained within the framework of a grant from the Ministry of Education and Science of Ukraine[1].

The rest of the paper is structured as follows. Section II presents the state of the art, providing information on the most relevant studies in the field and normative documents. Section III provides the results of the functional safety and cybersecurity co-engineering development and assessment approaches for several critical domains: nuclear, automotive, and railway. Section IV briefly summarizes the main results obtained, proposes directions toward developing an effective general safety and cybersecurity co-engineering framework for critical domains, and highlights the further research steps domains.

## II. STATE OF THE ART

### A. *Primary studies*

We have performed a mapping study on safety and cybersecurity assessment for critical domains [1], and it has shown significant interest in safety and cybersecurity co-engineering. Yet, many questions are still open and require further investigation.

We have focused on studies that address both safety and cybersecurity to provide details on how exactly safety and cybersecurity co-engineering is implemented in research studies.

In [2], authors utilize fault tree analysis (FTA) for safety assessment, while cybersecurity is used as one of the contributors to safety (Fig. 1), along with reliability and human error issues.

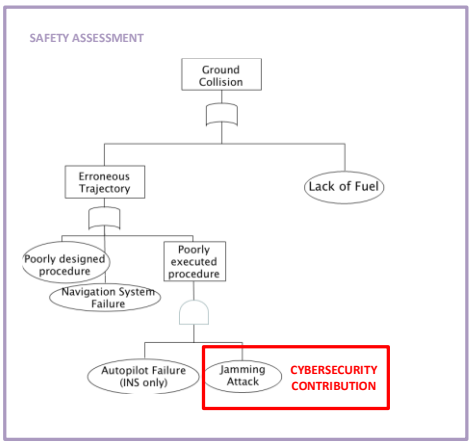


Fig. 1. An example of FTA assessment from [2] with safety and cybersecurity relation shown

In [3], the generic framework is provided (Fig. 2), suggesting choosing the most appropriate safety and/or cybersecurity technique based on requirements.

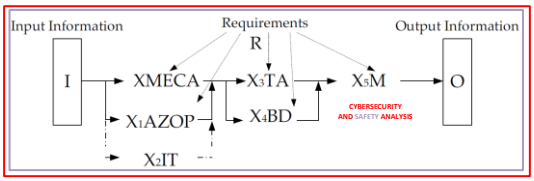


Fig. 2. An example of XMECA concept from [3] with safety and cybersecurity relations shown

In [4], cybersecurity is also integrated into the safety assessment process (Fig. 3).

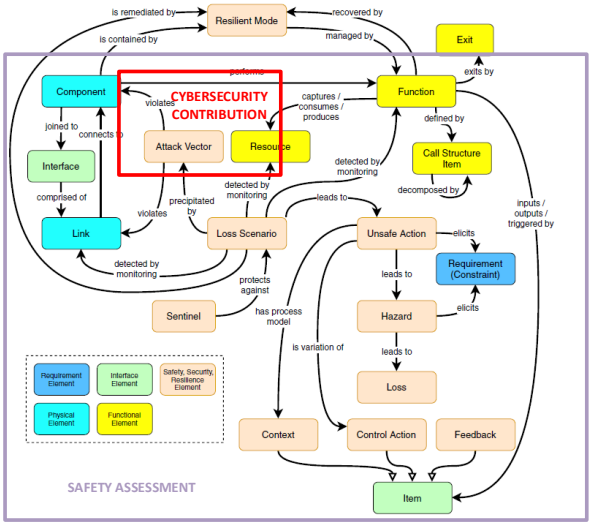


Fig. 3. An example of the ontological model from [4] with safety and cybersecurity relations shown

[1] This research was partially funded by the Ministry of Education and Science of Ukraine, state grant registration number 0123U102106, project title "Methods and case technologies of evidence-based cybersecurity assessment of programmable systems to ensure the protection of critical IT infrastructure". This publication reflects the views of the authors only, and the Ministry of Education and Science of Ukraine cannot be held responsible for any use of the information contained therein.

In [5], consequence-based analysis is described, where cybersecurity assessment is included as a necessary step, with further focus on potential safety impact (Fig. 4).

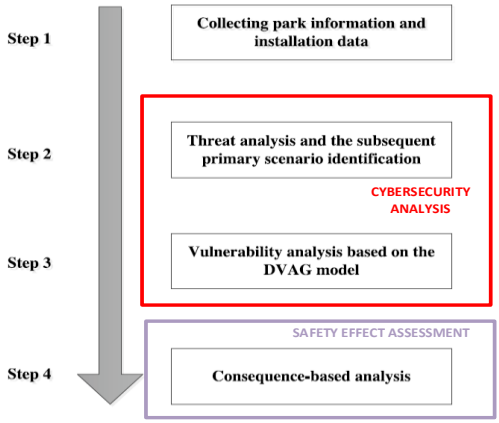


Fig. 4. An example of a consequences-based method from [5] with safety and cybersecurity relations shown

In [6], cybersecurity and safety risks are defined separately, further evolving to a global definition of industrial risk that combines both entities (Fig. 5).

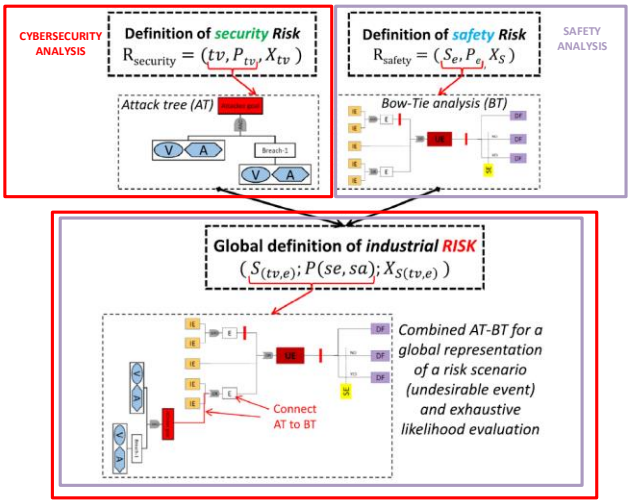


Fig. 5. An example of the approach based on global (cybersecurity and safety) industrial risk definition from [6]

In [7], scenario-based threat analysis focused on cybersecurity includes potential impact on safety and relevant safety assets (Fig. 6).

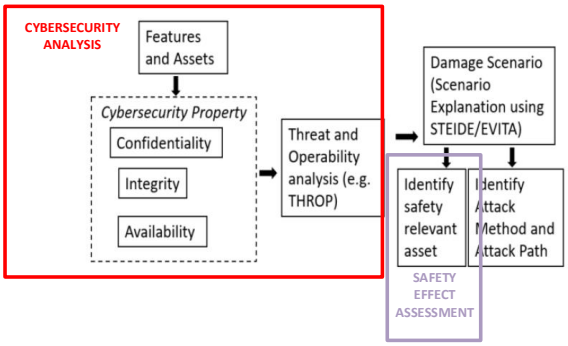


Fig. 6. An example of a threat analysis approach from [7] with safety and cybersecurity relations

From this short overview of existing studies, it can be concluded that there is relevant interest in conducting joint safety and cybersecurity development and assessment. Therefore, methodological supports to promote more effective and widely adoptable assessment approaches based on safety and cybersecurity co-engineering are certainly appropriate and of practical utility.

### *B. Normative documents*

Safety and cybersecurity co-engineering issues are also addressed in several normative documents.

For example, in [8], safety and cybersecurity co-engineering guidelines are provided, with references to the relevant field normative documents (Fig. 7).

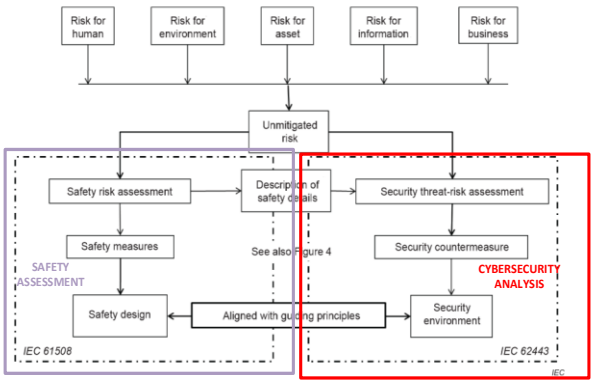


Fig. 7. An example of cybersecurity and safety co-engineering guidelines in a normative document [8]

[9] highlights the importance of addressing cybersecurity during safety analysis (Fig. 8).

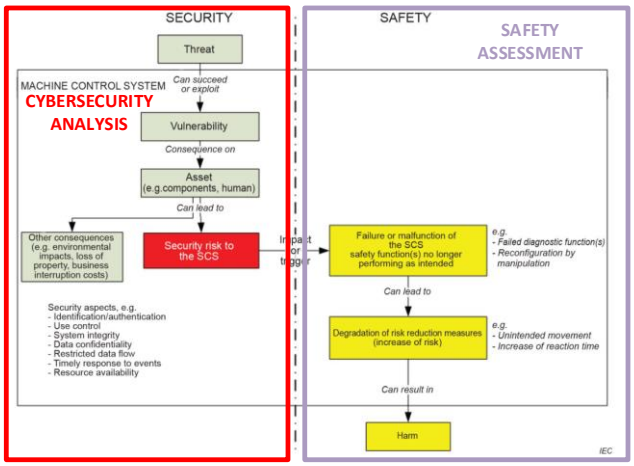


Fig. 8. An example of cybersecurity importance for safety in a normative document [9]

[10] analyzes safety and cybersecurity integrally as dependability attributes. According to the proposed requirements consistency (Fig. 9), cybersecurity requirements should be analyzed after the safety requirements are understood adequately. However, it is mentioned that this is one of many possible flows, but rather, an example. Nevertheless, needs in safety and cybersecurity co-engineering are well defined.

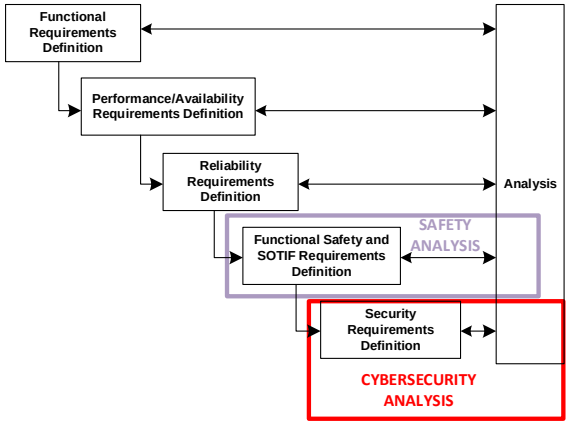


Fig. 9. An example of cybersecurity and safety integral analysis as part of dependability analysis in a normative document [10]

Based on the normative documents analyzed above, the following directions for joint consideration of safety and cybersecurity are available:

- Cybersecurity contributes to (supports) existing safety assessment methods;
- Cybersecurity is integrated into safety/resilience models;
- Generic approach is applied for safety and cybersecurity assessment, tuned according to the requirements;
- Cybersecurity is analyzed only in terms of its effects on safety;
- Cybersecurity and safety are analyzed integrally as dependability attributes.

## III. TOWARDS SAFETY AND CYBERSECURITY CO-ENGINEERING FRAMEWORK

We developed the safety and cybersecurity co-engineering ontology presented in Fig.10 based on safety, cybersecurity, and safety and cybersecurity co-engineering normative documents available now.

The following critical domains were covered: aerospace [19-20], automotive [12-14], nuclear [15-18], health [30], smart grid [31], cyber-physical vehicles [32], instrumentation and control [8-9],[27],[29], railway [23],[28], and robots [33]. Generic (multi-domain) normative documents were also considered [10],[34].

It was observed that time-proved critical domains like aerospace, nuclear, railway, and automotive have well-established normative documents on safety. However, there is a clear trend in the advent of normative documents on cybersecurity also. More recent critical domains like the smart grid and cyber-physical vehicles have normative documents on cybersecurity from the outset.

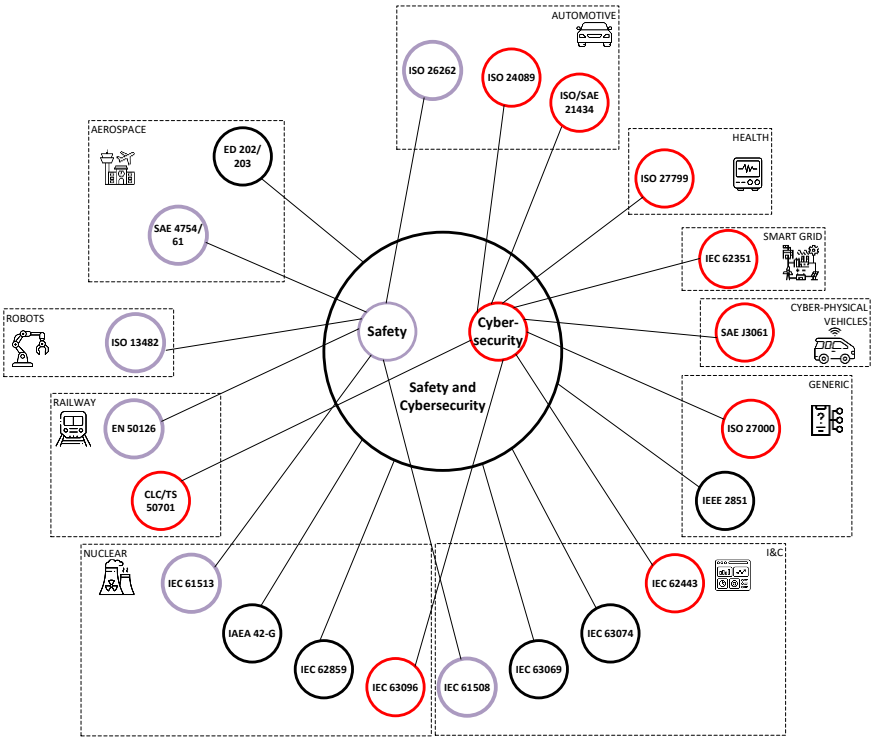


Fig. 10. Cybersecurity and safety co-engineering ontology based on relevant normative documents

It should be emphasized that normative documents covering safety and cybersecurity co-engineering are still not mature since some are in the draft form, technical report, or technical specification stage.

The developed ontology is exploited in the following to revisit the processes devoted to account for safety and cybersecurity requirements during design and assessment in representative critical sectors, proposing a co-engineering solution.

### A. *Automotive domain*

The United Nations Economic Commission for Europe (UNECE) established WP.29 [11] to regulate motor vehicles and equipment. This subsidiary Working Party (GRVA) is dedicated to automated/autonomous and

connected vehicles and proposes uniform provisions for the approval of vehicles concerning:

- Safety and environmental performance of wheeled vehicles, their subsystems and parts;
- Cybersecurity and cybersecurity management systems;
- Software and management system updates.

ISO/SAE 21434 [12] is aimed at the protection of assets against the environment (i.e. to identify assets of the item whereby compromising their cybersecurity properties could lead to damage scenarios) is built on the family of twelve functional risk-based safety standards ISO 26262 [13], which in its turn, is aimed at protecting the environment against malfunctions (i.e. to identify functionalities of the item whereby compromising their properties of correctness could lead to harm), providing a similar framework for the entire life cycle of road vehicles. Overall, ISO/SAE 21434 gives "what" shall be done and limits information on "how" it shall be done. Cybersecurity is less consolidated than safety. Risk assessment is still relatively controversial. It includes cybersecurity risk management requirements for:

- Road vehicles with electrical and electronic systems;
- Components, interfaces and communications;
- Engineering through concept, design, development, production, operation, maintenance, and decommissioning.

ISO 24089 [14] provides technical requirements related to software updates and cybersecurity throughout the vehicle lifecycle and organizational and procedural requirements for the entire automotive supply chain. In short, it aims to ensure that:

- Vehicle software updates are secure and come from verified sources;
- Processes and continuous improvements for software updates are implemented;
- The shared awareness of safety and cybersecurity is created along the automotive supply chain.

Figure 11 depicts a developed conceptual diagram of the safety and cybersecurity co-engineering in the automotive domain based on integrating ISO 26262 and ISO/SAE 21434. The proposed diagram illustrates ISO 26262 and ISO/SAE 21434 activities separately but interconnected within the overall vehicle development lifecycle. Combining functional safety artifacts with cybersecurity artifacts at different stages of the automotive development lifecycle is essential for ensuring overall safety and cybersecurity.

The integration and alignment of safety and cybersecurity processes are represented in the lower section of the diagram, emphasizing the need for cross-domain collaboration and coordination to ensure the overall safety and cybersecurity of the vehicle.

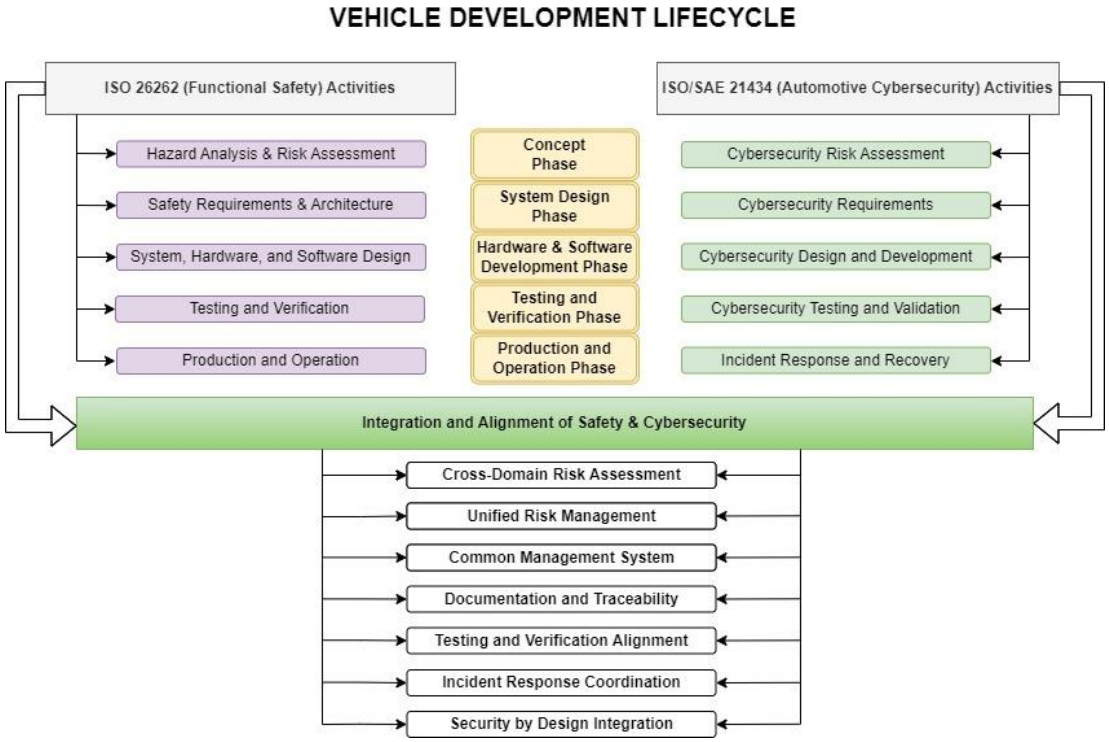


Fig. 11. Conceptual diagram of co-engineering in integration of ISO 26262 and ISO/SAE 21434

During the Concept Phase, hazard analysis and risk assessment inform safety and cybersecurity. The Hazard Analysis Report identifies potential hazards, some of which may have cybersecurity implications.

In the System Design Phase, safety requirements are specified. These requirements should also consider cybersecurity aspects, such as secure communication protocols or intrusion detection systems. The Safety Requirements Specification needs to account for both safety and cybersecurity requirements.

The Hardware & Software Development Phase includes the development of system architecture and design specifications. This phase should also involve the

creation of cybersecurity design specifications, which can be integrated into the overall design.

During the Testing and Verification Phase, verification activities must encompass both safety and cybersecurity. A Verification Test Plan should outline safety and cybersecurity verification testing procedures, with corresponding test cases for each domain.

In the Production and Operation Phase, incident response planning is essential. An Incident Response Plan should address safety incidents as well as cybersecurity incidents, ensuring a coordinated approach to handling both types of issues.

This integration ensures that safety and cybersecurity are considered throughout the development lifecycle and that relevant artifacts are created and managed to maintain the vehicle's overall safety and cybersecurity. These artifacts and processes are often more detailed and extensive in practice, but this representation provides a high-level overview of their integration.

### *B. Nuclear domain*

Recent normative documents and guides in the nuclear field have a trend for safety and cybersecurity co-engineering.

In particular, 3.22 of IAEA 42-G [15] states that "computer security should be implemented as an integral part of the life cycle processes of computer-based systems used for nuclear safety, to ensure that computer security and nuclear safety requirements are considered together."

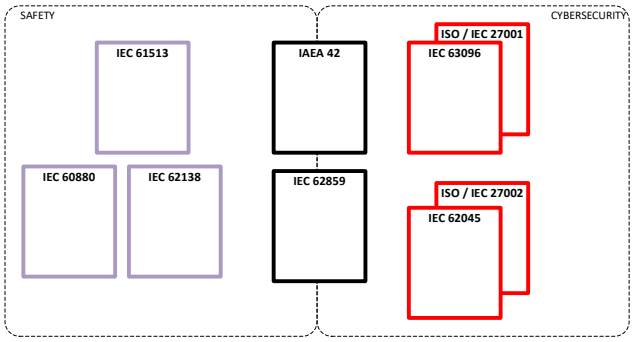


Fig. 12. Diagram of safety and cybersecurity normative documents in the nuclear field

IEC 61513 [16] focuses on safety but incorporates requirements for cybersecurity planning.

IEC 63096 [17] adapts information security, including cybersecurity and management system from ISO/IEC 27001 for the nuclear field, focusing on cybersecurity controls and risk management framework. Interactions between safety and cybersecurity for nuclear power plant (NPP) systems are covered in the framework provided in IEC 62859 [18]. The diagram of relevant normative documents is shown in Fig. 11. Discussion of co-engineering approaches from these documents is presented below.

During the Requirements and Planning phase, potential dependencies, safety requirements, and cybersecurity requirements should be identified and considered to ensure the definition of an integrated solution meeting both the safety and security goals.

During the Design phase, any system features initially designed for safety reasons that have a potential value as a cybersecurity counter-measure should be examined considering threats and cyberattacks to confirm cybersecurity effectiveness.

As for the Implementation phase, no specific requirements or recommendations related to the safety and cybersecurity co-engineering are provided in existing normative documents.

During the Verification and Validation phase, integrating safety-oriented code review, analysis, and other techniques with the relevant cybersecurity-oriented ones depends highly on the context. Therefore, no universal co-engineering approach has been provided so far.

During the Operation and Maintenance phase, it is stated that periodic testing of safety functions shall not affect cybersecurity and that cybersecurity verifications may also be considered for integration in safety periodic testing.

### *C. Railway domain*

In the railway domain, functional safety and cybersecurity are intertwined. Railway systems often rely on complex electronic and software components, making them susceptible to functional safety and cybersecurity risks. Therefore, railway operators and manufacturers must adhere to relevant international and regional standards to ensure the safety and security of their systems [21-22]. Additionally, they should stay updated on the evolving threat landscape and adapt their safety and cybersecurity measures accordingly.

In the railway domain, there is a group of European standards specifically address the railway sector's functional safety EN 50126 [23] (provides guidelines for the management of reliability, availability, maintainability, and safety in railway systems), EN 50128 [24] (focuses on software aspects, including software development, verification, and validation in railway control and protection systems), and EN 50129 [25] (addresses the safety-related aspects of electronic systems used in railway signaling) as well as the international standards IEC 62279 [26] (specifies the process and technical requirements for the development of software for programmable electronic systems for use in railway control and protection applications. Applied with ISO/IEC 61508-2 [27]) and the updated version of the CLC/TS 50701 [28] (which offers numerous benefits for organizations in the railway industry. Applied with EN 50126-1 RAMS [23] lifecycle process and is consistent with the application of security management requirements contained within the IEC 62443-2-1 [29]).

As a general co-engineering safety and cybersecurity framework in railway systems, the following steps and respective actions are proposed to be implemented:

1. Comprehensive risk assessment:
   - Integrate safety and cybersecurity risk assessment;
   - Utilize EN 50126 and IEC 62279 for RAMS analysis;
   - Consider CLC/TS 50701 for cybersecurity threats;

2. Unified safety and cybersecurity requirements:
- Define unified safety and security requirements;
- Align with EN 50128 and IEC 62279;

3. Secure development practices:
- Implement secure coding practices from EN 50128
- Incorporate security early in design based on CLC/TS 50701 and IEC 62279
- Implement secure coding practices (EN 50128);
- Include security features in system design (CLC/TS 50701);

4. Security testing and verification:
- Conduct integrated testing for safety and security;
- Follow cyber-physical testing guidelines (IEC 62279, IEC 62433);

5. Continuous monitoring:
- Apply continuous monitoring per IEC 62443;
- Deploy intrusion detection systems (IEC 62443);

6. Regulatory compliance:
- Ensure compliance with safety and cybersecurity regulations;
- Adhere to standards and guidelines (EN 50126, IEC 62279, CLC/TS 50701, etc.).

Figure 13 illustrates how safety and cybersecurity considerations are integrated throughout the entire railway systems development lifecycle, ensuring comprehensive protection against both safety-related failures and cybersecurity threats.

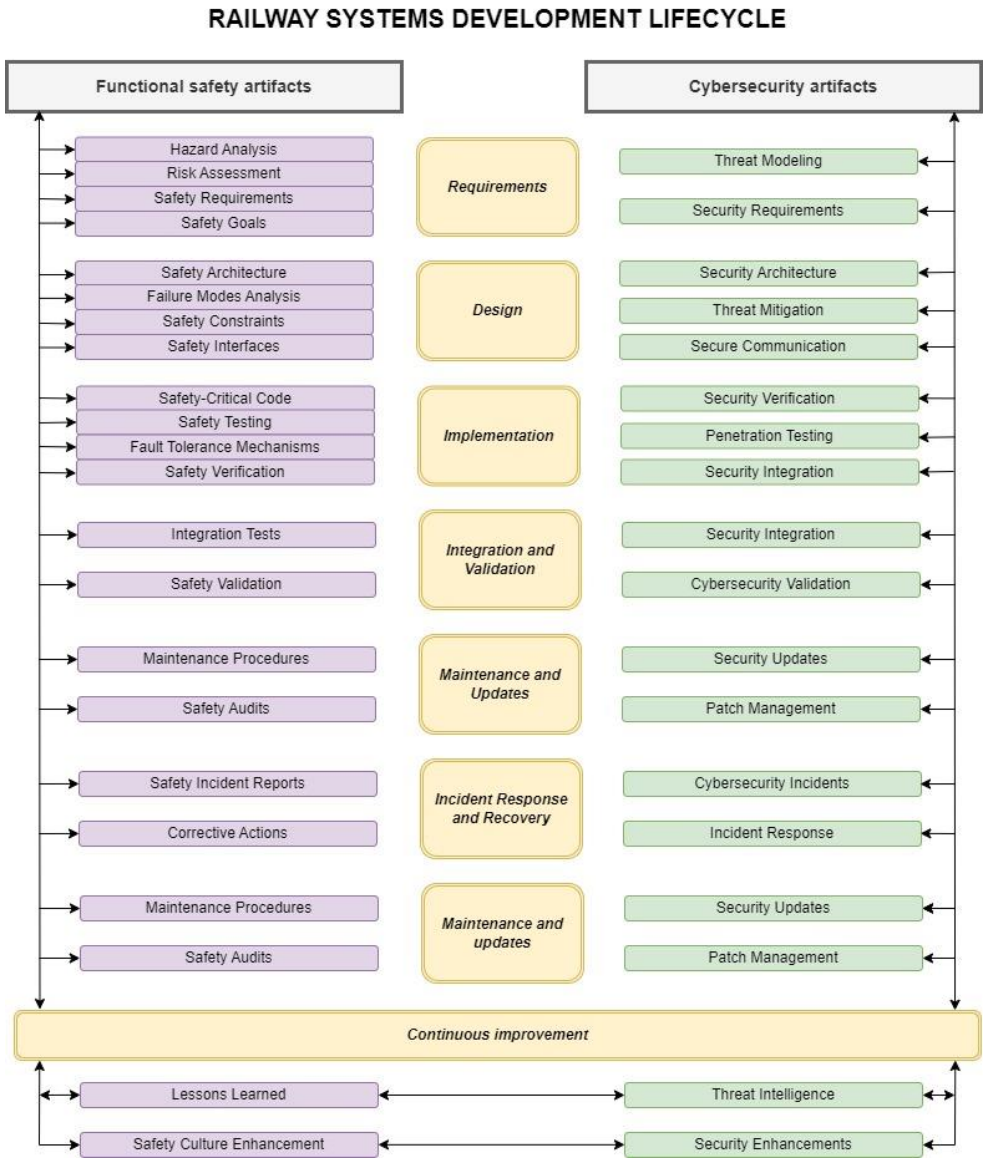


Fig. 13. Conceptual diagram of co-engineering in the integration of EN 50126, EN 50129, IEC 62279, CLC/TS 50701

The evolution of safety and cybersecurity co-engineering in the railway domain is seen as the research and development in the following directions: quantitative risk assessment models (models for assessing combined risks, consideration of passenger safety, and financial implications), formal verification for railway systems (enhancing of formal methods for correctness verification, ensuring safety and security requirements), predictive maintenance with security (integration of predictive maintenance, early detection of vulnerabilities), secure train-to-ground communication

(strengthening security for train-ground communications, prevention of unauthorized access). This list needs to be completed, and additional directions are to be clarified by the domain experts.

## IV. Conclusion

Safety and security co-engineering is a relatively novel field in terms of real practical implementation, and it is expected to mature significantly shortly. Although there are attempts to integrate concepts, processes, and specific engineering techniques in different domains, the absence of the universal co-engineering approach will likely persist for some time due to the unique characteristics of each field. Research has shown that a unified safety-cybersecurity co-engineering development cycle is feasible, but its implementation and adoption still need to be revised. There is a clear need for additional methodological and tool support to assist communities dealing with these challenges.

As overall recommendations, the following ones appear to be of utmost relevance to address the safety and cybersecurity issues adequately during development, assessment, maintenance, and commissioning:

- Artifact traceability: i) establish traceability between safety and cybersecurity artifacts, ii) use traceability matrices to manage relationships;
- Cross-sector collaboration: i) collaborate with experts from both safety and cybersecurity domains; ii) foster cooperation among original equipment manufacturers, original design manufacturers, tier (1,2,3+) companies, safety and cybersecurity experts, and technology providers;
- Incident response and recovery: i) develop coordinated incident response plans; ii) address safety and cybersecurity incidents promptly and effectively;
- Training and awareness: i) train staff to recognize and respond to safety and cybersecurity threats; ii) promote a culture of security and safety awareness;
- Documentation and reporting: i) maintain comprehensive documentation of safety and cybersecurity measures; ii) establish precise reporting mechanisms for incidents and vulnerabilities.

## References


[1] I. Babeshko and F. D. Giandomenico, "Safety and Cybersecurity Assessment Techniques for Critical Industries: A Mapping Study," in *IEEE Access*, vol. 11, pp. 83781-83793, 2023, doi: 10.1109/ACCESS.2023.3297446.

[2] R. B. Ferreira et al., "A Risk Analysis of Unmanned Aircraft Systems (UAS) Integration into non-Segregate Airspace," *2018 International Conference on Unmanned Aircraft Systems (ICUAS)*, Dallas, TX, USA, 2018, pp. 42-51, DOI: 10.1109/ICUAS.2018.8453455.

[3] I. Babeshko, O. Illiashenko, V. Kharchenko, K. Leontiev, "Towards Trustworthy Safety Assessment by Providing Expert and Tool-Based XMECA Techniques," *Mathematics*, 2022, 10, 2297. DOI: 10.3390/math10132297.

[4] G. Bakirtzis, T. Sherburne, S. Adams et al, "An ontological metamodel for cyber-physical system safety, security, and resilience coengineering," *Softw. Syst. Model.*, 2022, 21, pp. 113–137. DOI: 10.1007/s10270-021-00892-z.

[5] C. Chen, G. Reniers, N. Khakzad, "Integrating safety and security resources to protect chemical industrial parks from man-made domino effects: A dynamic graph approach," *Reliab. Eng. Syst. Saf.*, 2019, 191, 106470.

[6] H. Abdo, M. Kaouk, J.-M. Flaus, F. Masse, "A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie – Combining new version of attack tree with bowtie analysis," *Comput. Secur.*, 2018, 72, pp. 175–195.

[7] M. Khatun, M. Glaß and R. Jung, "An Approach of Scenario-Based Threat Analysis and Risk Assessment Over-the-Air updates for an Autonomous Vehicle," *2021 7th International Conference on Automation, Robotics and Applications (ICARA)*, Prague, Czech Republic, 2021, pp. 122-127, DOI: 10.1109/ICARA51699.2021.9376542.

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

[9] IEC TS 63074:2023. Safety of machinery - Security aspects related to functional safety of safety-related control systems

[10] IEEE P2851/D4.0, July 2023. IEEE Draft Standard for Functional Safety Data Format for Interoperability within the Dependability Lifecycle, 26 July 2023, pp.1-253.

[11] The United Nations Economic Commission for Europe UNECE World Forum for Harmonization of Vehicle Regulations WP.29 – https://unece.org/wp29-introduction

[12] ISO/SAE 21434:2021 Road vehicles – Cybersecurity.

[13] ISO 26262:2018 Road vehicles – Functional safety standards.

[14] ISO 24089:2023 Road vehicles – Software update engineering.

[15] IAEA Nuclear Security Series No. 42-G. Computer Security for Nuclear Security. Implementing Guide https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1918_web.pdf

[16] IEC 61513:2011. Nuclear power plants – Instrumentation and control important to safety – General requirements for systems

[17] IEC 63096:2020. Nuclear power plants – Instrumentation, control and electrical power systems - Security controls

[18] IEC 62859:2016. Nuclear power plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity

[19] ED-202A – Airworthiness Security Process Specification https://eshop.eurocae.net/eurocae-documents-and-reports/ed-202a/

[20] ED-203A – Airworthiness Security Methods and Considerations https://eshop.eurocae.net/eurocae-documents-and-reports/ed-203a/

[21] S. Soderi, D. Masti and Y. Z. Lun, "Railway Cyber-Security in the Era of Interconnected Systems: A Survey," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 7, pp. 6764-6779, July 2023, doi: 10.1109/TITS.2023.3254442.

[22] S. Soderi, D. Masti, M. Hämäläinen and J. Iinatti, "Cybersecurity Considerations for Communication Based Train Control," in *IEEE Access*, vol. 11, pp. 92312-92321, 2023, doi: 10.1109/ACCESS.2023.3309005.

[23] EN 50126:2017 Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability, and Safety (RAMS)

[24] EN 50128:2020 Railway Applications – Communications, Signalling, and Processing Systems – Software for Railway Control and Protection Systems

[25] EN 50129:2018 Railway Applications - Communications, Signalling, and Processing Systems – Safety-Related Electronic Systems for Signalling.

[26] IEC 62279:2015 Railway applications - Communication, signalling and processing systems – Software for railway control and protection systems.

[27] IEC 61508-2:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems.

[28] CLC/TS 50701:2023 Railway applications – Cybersecurity.

[29] IEC 62443-2-1:2010 Industrial communication networks - Network and system security – Part 2-1: Establishing an industrial automation and control system security program.

[30] Health informatics – Information security management in health using ISO/IEC 27002.

[31] IEC 62351:2023. Power systems management and associated information exchange – Data and communications security – All parts.

[32] SAE J3061. Cybersecurity Guidebook for Cyber-Physical Vehicle Systems.

[33] ISO 13482:2014. Robots and robotic devices – Safety requirements for personal care robots.

[34] ISO/IEC 27000:2018. Information technology – Security techniques – Information security management systems – Overview and vocabulary.