

Article

Proposal for an Integrated Framework for Electronic Control Unit Design in the Automotive Industry

Aleksander Buczacki ^{1,*} and Piotr Piątek ²

¹ Faculty of Production Engineering, Warsaw University of Technology, 02-524 Warsaw, Poland

² Faculty of Electrical Engineering, Automatics, Computer Science and Biomedical Engineering, AGH University of Science and Technology, 30-059 Cracow, Poland; piatek@agh.edu.pl (PP)

* Correspondence: aleksander.buczacki@pw.edu.pl (AB); Tel.: +48-22-234-81-26

Citation: Buczacki, A.; Piątek, P. Proposal for an Integrated Framework for Electronic Control Unit Design in the Automotive Industry. *Energies* **2021**, *14*, 3816. <https://doi.org/10.3390/en14133816>

Academic Editors: Leandros Maglaras, Antonios Argyriou, Sotiris Moschoyiannis, Athanasios Maglaras, Ioanna Kantzavelou and Igor Kotenko

Received: 7 April 2021

Accepted: 21 June 2021

Published: 24 June 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

Abstract: The automotive sector is facing challenges in terms of the requirements for guaranteeing the safety and security of cars. In respect of the engineering process, it is challenging to incorporate functional safety, safety of the intended functionality, and cybersecurity requirements into electrical vehicles. All of these aspects impact not only the vehicles or ECUs produced, but also the structures of the organizations by which the products are created. Based on current standards, drafts of future standards, and an analysis of the performance of a real design process for the ECU of an electrical vehicle, we propose an integrated design framework from the perspective of cybersecurity. Therefore, a stronger emphasis is placed on correct estimations of cybersecurity activity processes. As they affect all areas of development, these estimations cannot be isolated considering the ECU's design process. More cooperation between various stages of the process is required in order to provide complete products at an early stage of design and development. The challenge is the identification of overlapping activities and the combination of design efforts in order to reduce the time and costs of an engineering project. A dedicated process entity will be proposed to an engineering division to manage cybersecurity processes.

Keywords: cybersecurity; functional safety; systems engineering; project management; gateway; automotive; V2G; electric vehicles; connected vehicles; smart charging solutions

1. Introduction

In the development of intelligent vehicles, the level of system complexity is increasing. The automotive industry is facing challenges in terms of the requirements for guaranteeing the safety and security of autonomous cars and their surroundings, under any and all circumstances. Concurrently, original equipment manufacturers (OEMs) are looking for a way to increase the efficiency and effectiveness of design processes, as well as to shorten the time and decrease the cost of the development of new products. Research on the management of big engineering programs (US space programs) has identified the following challenges in managing programs [1]:

- Reactive program execution;
- A lack of stability, clarity, and completeness of requirements;
- Insufficient alignment and coordination of the extended enterprise;
- A non-optimized value stream throughout the entire enterprise;
- Unclear roles, responsibilities, and accountability;
- Insufficient team skills and unproductive behavior and culture;
- Insufficient program planning;
- Improper metrics, metric systems, and key performance indicators;
- A lack of proactive management of program uncertainties and risks;
- Poor program acquisition and contracting practices.

The above issues also apply to the automotive industry. Currently, in order to cover all use cases for autonomous vehicles, OEMs use the ISO 26262:2018 [2] standard. However, that standard covers only the faults resulting from system malfunctions, whereas the interaction of an autonomous vehicle with an environment goes far beyond this area. The new ISO PAS 21448 [3], which defines the paradigm of Safety of the Intended Functionality (SOTIF), increases the level of safety for future intelligent vehicles. However, an entire autonomous ecosystem can coexist only in conjunction with cybersecurity. The upcoming ISO 21434 [4] will fill in this gap.

How can the safety of an electric and autonomous vehicle be increased in the design phase? The full integration of analytical methods used for vehicle design is fundamental. This has a direct impact on the cost and time needed for the development of an electronic control unit (ECU) [5]. The identification of a universal vehicle design scheme, as well as the establishment of a way of working among engineers from different fields, such as functional safety (FS) and cybersecurity, is challenging [6]. Simultaneously, the entire design process can be placed in the ASPICE [7] frames [8,9]. Market demand for environmental friendliness, safety, economic efficiency, and user friendliness necessitate increasingly complex innovations in shorter intervals. The shorter development cycles and increasing reliability requirements require the improvement of development processes.

In this paper we introduce an integrated framework for ECU design in the automotive sector. We present it from the cybersecurity perspective and include dependencies on SOTIF and FS. Section 2 describes the background of our study; we show the current general approaches to the development of new products, as well as methodologies dedicated to ECU design and development, e.g., the current standard V-model approach and the FS dependencies according to the ISO 26262 standard series [2]. Later, we introduce the ECE/TRANS/WP/20/2020/79 directive and its correlation with the cybersecurity process requirements in the upcoming ISO 21434 [4]. Section 2 concludes with an analysis of the framework for the safety of the intended functionality (SOTIF) according to ISO/PAS 21448 [3].

Section 3 presents the research methodology applied in this research and a short description of another related publication in this area. Section 4 presents the results of our study, with an indication of the dependencies between FS, cybersecurity, and SOTIF. We found that only two of the 40 security areas [4]—namely, cybersecurity responsibilities and cybersecurity cases—do not have a direct impact on the safety process in autonomous systems. We combined these into a new V-model development process.

We gathered our findings in the Analysis Coordination section, where we suggest a path for the improvement of product design phases. Additionally, we presented data from a leading Tier 1 automotive supplier planning team; we were able to gather data regarding how cybersecurity activities were planned and later re-estimated for the development of a single V2G Gateway ECU for a premium German OEM. As a result, we observed a significant increase in design activities in the cybersecurity domain. The change was from 0.02% to 4% of all project design work. Section 5, where we present our discussion, gives an overview of the necessary improvements for future development. Since the cybersecurity shift affects both OEMs and suppliers, common paths and templates must be established in the process and design areas. Furthermore, we present a potential analysis where FS, cybersecurity, and SOTIF can coexist. Section 5 also includes the limitations of this research.

2. Background

2.1. Project Management Approaches for Design and Development Processes

New product development (NPD) is usually the most complex process that companies realize. Firstly, this process involves many stakeholders—both internal and external—with different points of view, expectations, and requirements addressed to the

product and the NPD process itself. NPD processes are usually related to long-term projects—in this case, innovative products with an uncertainty factor due to the products, technologies, and/or standards incorporated into the product. A generic NPD process flow is presented in Figure 1.

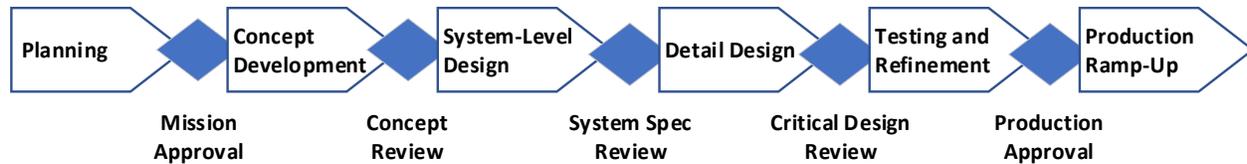


Figure 1. Product development process. Source: Authors' own, based on [10].

In practice, the process alternates between stages and gates; in the literature, this is called the stage–gate approach and it was first presented by Robert Cooper [11]. In this process, the concept phase and system-level design phase are especially critical because, in these phases, designers ensure that the right products will be designed and delivered. In the concept stage, all requirements related to the designed product should be understood and considered. To increase the effectiveness of NPD processes, companies implement the lean approach, which is well known and widely implemented in production processes. The lean approach developed from the Toyota Production System [12] and was later popularized by American researchers [13]. The first implementations of the lean approach in NPD were conducted in the early 2000s [14–16].

NPD processes should consider the following principles [17]:

- Identify value: All the process activities should focus on value generation. All activities can be classified as value-added, necessary but non-value-added, or non-value-added (pure waste) activities;
- Create value stream: The value defined in the previous step is generated as a result of the process. The opposite of the value is waste. In this step, sources of different types of waste should be identified (presented in Table 1) within the processes. This step also consists of the improvement of the process and the outcomes (products) of the process;
- Ensure process flow: Materials and information should constantly flow in the process (stream) without slowdowns, interruptions, delays, or unnecessary stoppages;
- Establish pull control: Materials and information are produced at the appropriate time and in the expected quality and amount;
- Implement perfection: All activities are performed with the expected quality and perfectly for the first time;
- Establish rules of respect for people: For engineering teams from different domains, interpersonal relations that motivate people are crucial. This stage focuses on teambuilding, trust, and involvement actions.

The first five steps are cyclic. The rules of respect have an impact on all other steps.

Table 1. Types of waste in NPD processes. Source: Authors' own, based on [18].

Type of Waste	Description/Examples
Overproduction	Creating information that will not be used (e.g., waiting for available resources). Working on unnecessary activities instead of those that are currently needed.
Waiting	Waiting for engineers, information, materials for reviews, decisions, or further actions.
Wrong process	Performing unnecessary activities or tasks. This could also relate to designing new components instead of using standards/carry-overs.

Type of Waste	Description/Examples
Transportation	Unnecessary flows of people, information, or materials, e.g., handoffs.
Motion	Unnecessary actions in the performance of tasks, such as non-productive meeting or project reviews and redundant status reports.
Inventory	Collecting information that is not currently being used. In practice, inventory waste is a result of overproduction.
Correction	All activities related to quality control but not related to quality assurance, as well as reworks.

Currently, the agile approach is widely implemented, especially for ECU design and development. In general, these two approaches (lean and agile) are similar [19].

Therefore, all stakeholders should be able to make the right decisions based on all of the necessary information. This applies not only to technical topics, but also to other topics related to the designed product, such as FS, SOTIF, or cybersecurity. The main challenges in the planning and concept development stages are the clarification and understanding of all requirements, as well as the creation of the right product concept.

2.2. Engineering Approaches for the Design of Embedded Systems

2.2.1. Standard Systems Engineering Approach in the Automotive Industry

In today's challenging environment of the modern automotive industry, where software and its quality play an important role, there is a need to quickly deploy new technologies in all aspects of businesses. The safety-critical systems of a vehicle account for a large portion of the development costs. Any failures in those systems can impact peoples' lives and can cause the OEMs to experience significant losses of income. Vehicle manufacturers take proactive action to address these issues. They focus on the following:

- The capabilities of the software for supplier assessment processes;
- Making provisions for contractual software quality requirements; and
- Assessing the software capabilities of suppliers before and during contract performance.

A common development process and monitoring framework developed by major OEMs and Tier 1 suppliers that is currently used throughout the vehicle industry is Automotive SPICE®. Version 3.1 of the ASPICE® Process Reference and Assessment Model is available and currently used as a VDA [7]. It focuses primarily on a product's software and system activities however, for version 3.1 of the standard, it is possible to add more engineering disciplines—e.g., hardware engineering and mechanical engineering—and the corresponding domain-specific processes to the scope of ASPICE depending on the product being developed.

Processes are classified by category in the process reference model, and then into process categories based on the types of operations that they discuss on a second level.

According to the VDA [7], the three process categories are as follows:

- Primary life-cycle processes;
- Organizational life-cycle processes;
- Supporting life-cycle processes.

Each process is described in the form of a purpose statement that includes the process's unique functional objectives when performed in a specific environment. There is a predefined list of outcomes for each purpose statement.

In principle, Automotive SPICE® follows generic V-model-based system development. It describes all of the activities to be performed during system development and their results. The left side of the V-model represents the project definition, whereas

the right side focuses on integration and validation. Figure 2 presents the generic engineering approach from a system development perspective.

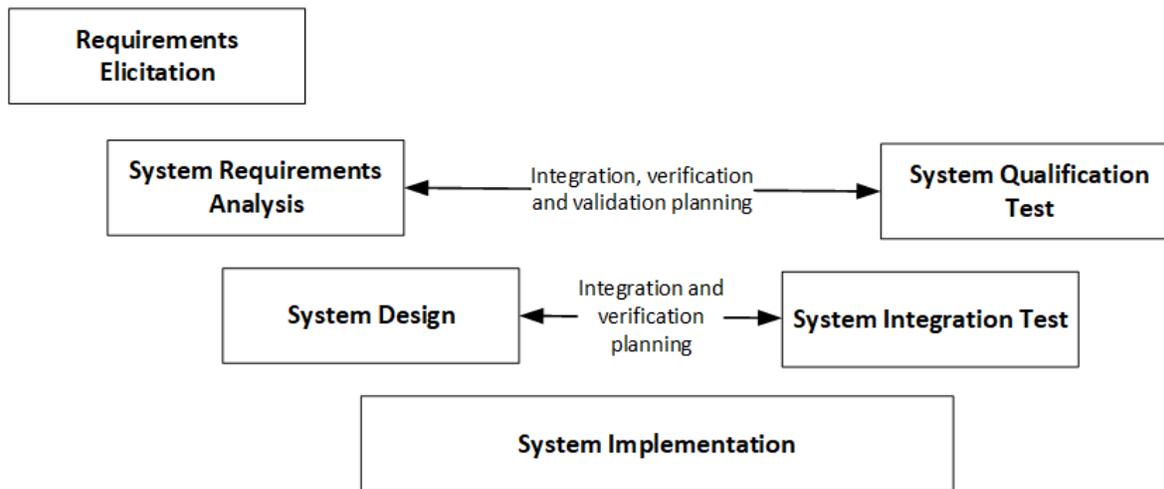


Figure 2. Generic V-model from the system development perspective. Source: Authors' own, based on [7].

2.2.2. Functional Safety

FS and reliability have become critical parts of automotive safety applications. Advanced driver assistance systems (ADASs) are paving the way for future autonomous vehicles. However, the tolerable risk level remains the fundamental challenge for engineering departments during the design of complex systems. To reduce the risk of systematic failures and incidental hardware failures, the ISO 26262 [2] series provides directions for mitigating these risks. It gives an extensive set of requirements and processes for the entire developmental life cycle [2].

Achievement of FS can be realized by the following:

- Tailoring activities for the automotive safety development cycle;
- Determining the automotive-specific integrity level, or automotive safety integrity level (ASIL);
- Using the ASIL to find which requirements of ISO 26262 should be followed to avoid unreasonable and continuing risks;
- Providing the requirements for FS management, design, implementation, verification, validation, and acceptance measures; and
- Defining the customer–supplier relationship requirements.

Safety activities are closely connected with common function- and quality-oriented activities and output products. All of them are addressed and deeply described in the ISO 26262 series.

FS, which is defined in ISO 26262 as the “absence of unreasonable risk due to hazard caused by malfunctioning behavior of Electrical/Electronic systems,” brings to product development a shift from a quality management system to a safety-oriented culture. The standard demands evidence-based safety. It enforces stricter documentation and around 130 new work packages, which undoubtedly increase the efforts required in the development of each product [20].

The basic chain of safety implications can be represented as follows: Malfunction → hazard → risk → required risk reduction.

Malfunctions are classified by the standard into two types:

- Systematic failures—these occur deterministically during the development, manufacturing, or maintenance phases;

- Random failures—incidental hardware failures that occur during a hardware component's lifetime.

In most cases, systematic failures are caused by an inadequate mechanism in the process. They can be solved by changes in the documentation, manufacturing process, operational procedures, etc. Random failures, however, are discussed during the design and verification of the HW/SW by using safety mechanisms. This enables a product's architecture to detect/correct malfunctions. This is indicated by assigning an automotive safety integrity level. The concept phase of FS is carried out by the original equipment manufacturer. The OEM is responsible for the assignment of a function to a certain system on a vehicle level. The ASIL level and the safety goals are also determined at this level. After these activities, the FS requirements are derived. The electronics provider is also involved in the FS analysis. Each piece of electronic equipment that is marked as being related to safety and will be mounted in the vehicle requires the following [21]:

- FMEDA (failure mode effect and diagnostic analysis);
- Analyses of the timing–fault-tolerant time interval (FTTI) and diagnostic test interval (DTI);
- DFA (dependent failure analysis).

In general, FS involves the implementation of active methods in order to develop the necessary level of risk mitigation. Furthermore, from the design perspective, Tier 1 suppliers are responsible for the management of safety requirements, analysis of system failures, and creation of a technical safety concept. This should be an input for the development team in order to ensure the ASIL Level. During project development, all FS activities should be verified and managed by a dedicated functional safety manager.

Even though safety management networks reduce systematic and random failures and, therefore, increase the safety and quality, they bring additional process overhead. With the increasing level of complexity of autonomous vehicles, FS analysis alone will not provide enough measures for reducing hazardous risks. Other aspects of connected vehicles, such as cybersecurity, must also be considered. Only with a holistic system approach can an adequate safety level be assured.

2.2.3. Cybersecurity

Due to the regulatory structure established by the Working Party (WP.29) of the World Forum for Harmonization of Vehicle Regulations within UNECE (the United Nations Economic Commission for Europe), innovative vehicle technologies can be introduced to the market. This framework focuses on global vehicle safety development, the reduction of environmental pollution and energy consumption, and the advancement of anti-theft capabilities [22]. WP.29 established six permanent Working Parties (GRs), which are subsidiary bodies that consider specialized tasks and consist of people with specialized knowledge. One of them is the Automated and Connected Vehicles Working Party (GRVA). The GRVA consists of several working groups, one of them being for “Cybersecurity and (OTA) software updates (CS/OTA)” [23].

The “ECE/TRANS/WP.29/2020/79 Proposal for a new UN regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management systems”, which was prepared by the CS/OTA working party, was released on 23 June 2020 [23].

The main areas of this group's interest are cybersecurity management systems (CSMSs) and vehicle security. CSMS refers to a systematic risk-based approach that defines organizational processes, responsibilities, and governance in order to reduce risks associated with cyber threats to vehicles and to protect them from cyberattacks [22]. In this case, vehicle security is the application of a CSMS to a specific type of vehicle. According to the regulation, a vehicle type is defined as one that does not differ in at least one of the following essential ways:

- The OEM's classification of the vehicle type;

- Aspects of the electric/electronic architecture and external interfaces that are critical in terms of cyber security.

The core requirements for a CSMS (Sec. 7.2) cover the entire life cycle (7.2.2.1), from development through production, to the post-production phase. The CSMS is defined as covering processes for the following (7.2.2.2.):

- Managing cybersecurity;
- Identifying risks of vehicle types;
- Assessing, categorizing, and treating identified risks;
- Confirming and checking if the identified risks are being managed properly;
- Testing the cyber security of a vehicle type;
- Keeping the risk assessment current;
- Monitoring, detecting, and responding to cyberattacks, cyber threats, and vulnerabilities of vehicle types and determining whether the cyber security measures in place are still effective considering recently identified cyber threats and vulnerabilities;
- Providing relevant data for forensic analysis.

Moreover, the CSMS must cover the entire supply chain (7.2.2.5). In summary, the aim is for an OEM to establish a certified cybersecurity management system on the enterprise level. This covers the UNECE's first discipline: "Managing vehicle cybersecurity".

The implementation timeline defined in the requirements of WP.29 is extremely challenging for the entire car industry. By 2022, the UN regulation will be applied for new vehicle types (EU and Japan), and by 2024, it will be applied for the first registrations (EU and Japan).

While ECE/TRANS/WP.29/2020/79 defined the basic requirements for automotive cybersecurity and CMSs, the upcoming ISO/SAE 21434 will give more detail on the implementation of cybersecurity in engineering processes.

Starting in 2016, the Society of Automotive Engineers (SAE) and the International Organization for Standardization (ISO) decided to work together to issue industry standards related to automotive cybersecurity.

In the past, both bodies worked on standards related to automotive safety and security. ISO 26262 [2] set the FS standards and SAE J3061 [24] set the foundation for cybersecurity standards. The ISO and SAE, together with OEMs, ECU suppliers, cybersecurity vendors, governing organizations, and automotive experts from various countries, created a working group to compose a new and complete standard for automotive cybersecurity. The ISO/SAE 21434 [4] draft was created with a focus on risk management, product development, production, operation, maintenance, decommissioning, process overview, and fostering a positive cybersecurity culture in the industry.

ISO/SAE 21434 was specifically developed to provide an extensive safety and security level for the ultimate road user/driver. It ensures that the risk levels and corresponding cybersecurity measures are set based on the impact on the final driver. Apart from a standardized cybersecurity framework, the document defines cybersecurity as an integral part of engineering throughout the entire vehicle life cycle; from the conceptual phase to the development, testing and validation, manufacturing, post-production, and decommissioning, it ensures the involvement of cybersecurity. Furthermore, the standard requires effective methods for learning lessons, training, and proper communication related to automotive cybersecurity.

ISO/SAE 21434 explicitly requires OEMs to perform an analysis of threats and risks throughout a vehicle's life cycle. This determines the extent to which the road user can be impacted by automotive cyber threats and vulnerabilities. This work product is called a threat analysis and risk assessment (TARA). The standard defines the way in which the analysis is to be performed and what it consists of.

In Annex E, the document covers the definition of cybersecurity assurance levels (CALs). The need for this classification was described in [25]. It can be used to ensure that an item's or component's assets are properly secured against relevant threat scenarios. However, the CALs do not specify the technical requirements. They are to be used as guidance for cybersecurity engineering by providing a common language for communication about cybersecurity assurance requirements among the organizations involved [4]. ISO/SAE 21434 provides example CALs with their requirements for cybersecurity assurance measures.

By analyzing the structure and content of ISO 21434, we realized that it will have a tremendous impact on vehicle engineering. Cybersecurity work deliverables are available in all process areas. Therefore, additional effort is required at each development step in order to be compliant with the ISO 21434 standard. To reduce the impacts on engineering efforts and project timing, further methods should be analyzed to smoothly incorporate the culture of cybersecurity into product development. At the same time, guidelines for cybersecurity in the automotive industry, e.g., PAS 1885 [26], have been introduced. However, they do not constitute formal requirements for placement in the market.

2.2.4. Safety of the Intended Functionality

As an outcome of vehicle development, connected and self-driving vehicles are soon expected to replace human drivers. To work flawlessly, a system of linked, cooperative automated vehicles (AVs), which is called the Cooperative Intelligent Transport System (C-ITS), will have to integrate all hazard scenarios. To consider all possibilities, a risk analysis of the system should include a safety analysis according to ISO 26262 [2], as well as other possible threat scenarios, such as cyber threats. Only by identifying the communication links between various phases of safety and cybersecurity processes can this kind of analysis be prepared. It can include, e.g., cyber threats, which cause safety losses, or an integrated requirement analysis [27].

However, in order to assess the complete range of risks for systems that rely on sensing the external or internal environment, as well as the hazard behavior caused by the intended functionality or performance limitations of a fault-free system in the ISO 26262 series, ISO/PAS 21448 [3] must be considered.

Examples of limitations given by the standard include the following:

- The function's inability to correctly comprehend the situation and operate safely, which includes functions that employ machine learning algorithms;
- Inadequate function robustness in the face of sensor input variations or varying environmental conditions [3].

Furthermore, the absence of unreasonable hazard risks resulting from functional weaknesses of the intended functionality or reasonably foreseeable misuse by people is referred to as the safety of the intended functionality (SOTIF).

The SOTIF primarily applies to emergency intervention systems (e.g., emergency braking systems) and advanced driver assistance systems (ADASs) with automation levels of 1 or 2 according to the OICA/SAE standard J3016 [28]. It can be considered for higher levels of automation systems as well, although additional measures may be required.

The activities of the SOTIF are implemented during the design, verification, and validation phases. Nonetheless, the entire analysis should be followed by an extensive system analysis in order to understand the user functions, the behaviors, and the limitations (ISO/PAS 21448) [29].

For the SOTIF analysis, the relevant hazardous use cases are classified into four areas:

- 1—known safe scenarios;
- 2—known unsafe scenarios;
- 3—unknown unsafe scenarios;
- 4—unknown safe scenarios.

The primary goal of the implementation of the standard is to shrink Areas 2 and 3 while expanding Area 1. Area 4 is included for completeness only and is not considered in the analysis. In summary, the analysis tries to identify the unknown and unsafe areas of operation and contain them within an acceptable level of risk. It adds, however, another level of processes that should be considered for the project development into the standard V-model. In order to lower a project's risks and timing, the SOTIF must be assessed together with the cybersecurity and safety measures. To complete the safety ecosystem, the vehicle and environmental factors must also be considered. This requires interdisciplinary engineering cooperation in order to include all possible hazardous events. The study should be expanded to define how the vehicle and environmental factors can be treated together, which will complete the AV safety ecosystem.

3. Materials and Methods

The NPD process, especially in the case of the development of ECUs for modern vehicles, is a complex management activity that involves many engineering competencies and domains. The background of the main challenges and the approaches generally used in NPD are presented in Section 2.1. The primary purpose of this paper is the exploration of the cybersecurity area of designed and developed ECUs and the discovery of connections with the FS and SOTIF domains. A brief description of engineering standards and standards related to FS, SOTIF, and cybersecurity is presented in Section 2.2.

Based on our background analysis, we proposed the following research questions:

RQ1: How can the design and development process of an ECU with a cybersecurity component be improved with respect to timing and costs?

RQ2: What is the impact of incorporating the cybersecurity component into the organization and management of the engineering process?

We started from a literature review that covered publications related to the FS and cybersecurity topics. We decided not to consider SOTIF separately because, in some papers, it is considered a part of FS. Figure 3 presents the numbers of publications in the Scopus database for the following queries (article title, abstract, and keywords):

1. Functional Safety AND Automotive (FS AND Auto);
2. Cybersecurity AND Automotive (Cyber AND Auto);
3. Functional Safety AND Cybersecurity AND Automotive (FS AND Cyber AND Auto).

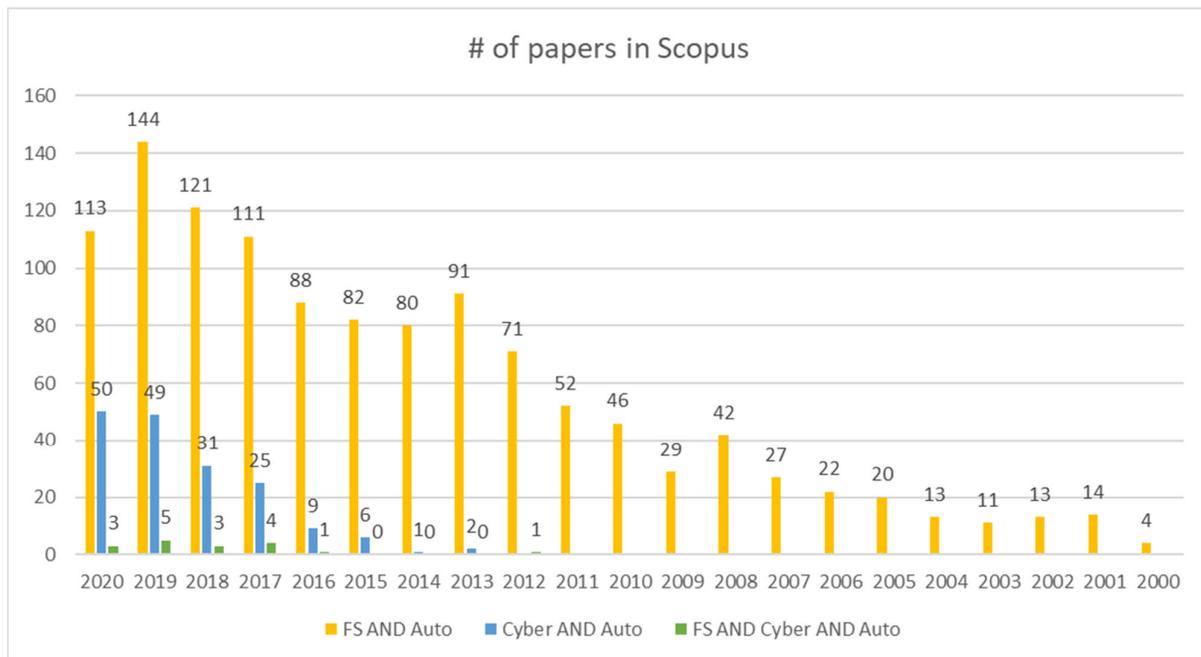


Figure 3. Numbers of publications in the Scopus database.

Due to fact that the FS topic is more mature than cybersecurity, we observed that there were more publications on the FS topic. However, we still observed an increasing trend of publications related to cybersecurity. Furthermore, we decided to analyze more deeply the publications on FS and cybersecurity in the automotive industry from the Scopus and Web of Science (WoS) databases. The papers are listed in Table 2.

Table 2. Summary of the literature review in WoS and Scopus databases.

Reference	Paper Characteristics	Year of Publication	WoS	Scopus	Type of Paper
[30]	Paper focused on artificial intelligence and machine learning topics. Not related to engineering management.	2020	X	X	Conference Paper
[31]	Proposed a method for integrating security and safety engineering in the ASPICE context.	2020		X	Technical Paper
[32]	Paper focused on the technical aspects related to FlexRay/Ethernet communication.	2020	X	X	Article
[33]	A case study (integrated pattern for FS and cybersecurity) of one automotive function. Briefly considered not only the OEM perspective, but also that of the supplier.	2019		X	Conference Paper
[34]	Paper focused on FS for critical automotive systems and CAVS (cooperation automated vehicles).	2019		X	Conference Paper
[35]	Trends in automotive system architecture design based especially on high-performance computation platforms, as well as the impacts of safety and cybersecurity requirements for future systems.	2019	X	X	Article
[36]	Focused on technical topics. Not related to engineering management.	2019	X	X	Conference Paper
[37]	General description of three cases, rather focused on system issues, not how such a system could/should be designed.	2019	X	X	Conference Paper

[8]	A couple of European initiatives were presented that mainly focused on FS. The article also focuses on the mutual dependencies of FS and ASPICE 3.0.	2018	X	X	Article
[38]	Synergies of FS and cybersecurity in engineering processes. Some qualitative effects of co-engineering approaches (FS and cybersecurity) are presented.	2018	X	X	Conference Paper
[39]	Results of static code analysis performed on automotive production software source code using reference coding standards.	2017		X	Conference Paper
[40]	Set on jointly addressing system safety and cybersecurity topics.	2017		X	Conference Paper
[41]	Training materials and best practices for ISO 26262 in the context of the EU SafeUR project.	2017		X	Lecture Notes
[42]	General framework for integration of FS and cybersecurity in the ADAS context.	2017	X	X	Conference Paper
[43]	Proposition of how cybersecurity topics could be supported by the FS standard (ISO-26262) and incorporated into hardware–software interface definitions.	2016	X	X	Conference Paper

Additionally, we ran the following query: “Autonomous vehicle*” AND Cybersecurity. As a result, 66 items were filtered in the WoS database, while 113 items were filtered in the Scopus database. Some publications did not concern the automotive industry. There were also publications that generally dealt with cybersecurity in autonomous vehicles, while most of the publications dealt with the technical issues of autonomous systems. Few papers concentrated on the device design and development process. Aside from the publications listed in Table 2, there were few that focused on both FS and cybersecurity.

To summarize the literature review, we can state that the use of cybersecurity in the development of modern vehicles is not mature. Additionally, appropriate standards are still in the phase of being detailed. There are not many papers related to the topics of both FS and cybersecurity in the automotive industry. Existing papers focus on the impacts of FS and cybersecurity on the ECUs that are designed. However, there is a lack of papers about the impact of the NPD process on the organization and management topics.

Based on this initial study, we decided to analyze more deeply a case of ECU development with a focus on the management of the engineering process. This also included an analysis of the scope of the deliverables provided during the project—especially from the cybersecurity perspective. Data for the analysis were obtained through in-depth interviews with cybersecurity and FS managers, project managers, systems engineers, software managers, software developers, and electrical and manufacturing engineers. Quantitative data on the project’s realization were also considered; these included work effort, timing, design, and an analysis of the reworking of development. In the next step of our research, an integrated framework was proposed and verified during a focus group interview (FGI). The focus group consisted of the project manager and representatives of the engineering team who were directly involved in the analyzed project, including those working on the FS and cybersecurity components. In addition, the focus group consisted of engineers with experience in implementing cybersecurity in ECUs, as well as representatives of the engineering staff and project managers from other multinational automotive companies (Tier 1 suppliers). One of the main conclusions of the FGI was the specification of the processes that support the implementation of cybersecurity mechanisms in ECUs, which must be supported in the post-production phases. The overall research methodology is presented in Figure 4.

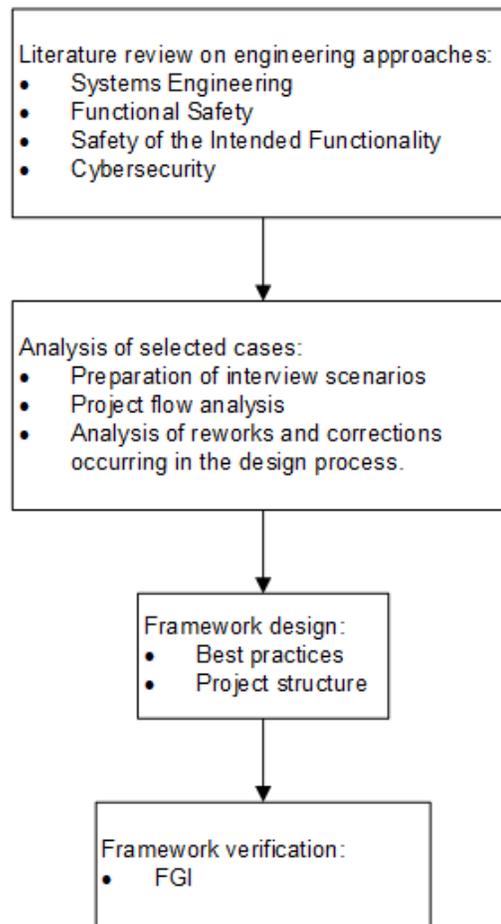


Figure 4. Research methodology.

The topic discussed in the present paper is important from the project management perspective, especially in the phases of the development and design of units in which FS and cybersecurity aspects should be included. There are several papers related to FS and cybersecurity in the automotive industry, but relatively few have considered both of these topics.

4. Results

4.1. Cybersecurity's Impact on the Project Development Process

Establishing the area of cybersecurity in the product development process for electric vehicles introduces completely new challenges. Due to its dynamic nature (new threats appearing throughout the entire product life cycle), the standard product development process must be extended. This goes beyond the production ramp-up and it reaches the post-production and decommissioning areas. These processes are paramount for product cybersecurity in order to establish the mechanisms of a cybersecurity incident response and introduce software updates once vulnerabilities have been detected. Moreover, once a product is withdrawn from the market or cybersecurity support ends, established procedures are applied to run these processes safely and responsibly. The changes in the project development process are presented in Figure 5.

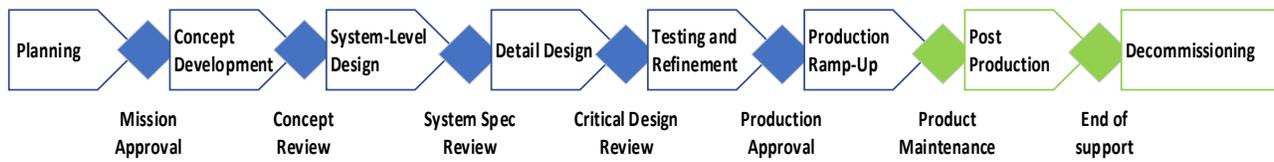


Figure 5. Updated project development process.

However, cybersecurity also has an impact on other areas. It goes hand in hand with FS processes, which are also further extended to autonomous systems. Table 3 includes mapping between cybersecurity and product development processes for electric vehicles, and Table 4 includes mapping between cybersecurity and supporting processes. It also shows which cybersecurity processes have an impact on functional/autonomous system safety processes.

Table 3. Cybersecurity processes impacting the product development processes of electric vehicles.

Electric Vehicle Product Development Process	Cybersecurity Area	Cybersecurity Areas that Impact Functional/Autonomous System Safety Processes
Planning	1. Cybersecurity Responsibilities	2; 3; 4; 5; 7; 8; 10; 11;12,13
	2. Cybersecurity Planning	
	3. Cybersecurity Tailoring	
	4. Cybersecurity Reuse	
	5. Off-the-Shelf Cybersecurity Component	
	6. Cybersecurity Case	
	7. Cybersecurity Assessment	
	8. Release for Post-Development	
	9. Adjustment of Responsibilities	
	10. Cybersecurity Monitoring	
	11. Vulnerability Monitoring	
	12. Penetration Testing Assessment	
	13. Key Management Processes	
Concept Development	1. Cybersecurity Item Definition	1; 2; 3; 4
	2. Cybersecurity Goal Definition	
	3. Threat and Risk Analysis	
	4. Cybersecurity Concept	
System Design	1. Cybersecurity Architectural Design	1; 2
	2. System Vulnerability Analysis	
Detailed Design	1. Software Cybersecurity Architecture Design	1; 2; 3; 4
	2. Detailed Software Design Requirements	
	3. Hardware Cybersecurity Architecture Design	
	4. Detailed Hardware Cybersecurity Design Requirements	
Testing and Refinement	1. Integration and Verification Specifications	1; 2; 3; 4; 5
	2. Integration and Verification Reports	
	3. Software Vulnerability Analysis Report	
	4. Hardware Vulnerability Analysis Report	
	5. Cybersecurity Validation Report	
Production and Ramp-Up	1. Production Control Plan	1
Post-Production	1. Software Update	1; 2
	2. Cybersecurity Incident Response	

Decommissioning	1.	End of Cybersecurity Support	1; 2
	2.	Decommissioning	

Table 4. The impact of cybersecurity on the supporting process group for product development.

Supporting Process Group	Cybersecurity Area	Cybersecurity Areas that Impact Functional/Autonomous System Safety Processes
Organizational Cybersecurity Management	1.	Cybersecurity Governance
	2.	Cybersecurity Culture
	3.	Cybersecurity Information Sharing
	4.	Cybersecurity Management Systems
	5.	Tool Management
	6.	Information Security
	7.	Organization Security Audits
		1; 2; 3; 4; 5; 6; 7

Appropriate planning is an essential component of a successful project. In this area, project leaders prepare timelines for all engineering disciplines based on state-of-the-art knowledge, lessons learned, and internal company standards. Another layer of abstraction is added to this part by cybersecurity. New areas that were not previously considered must be incorporated into the overall project planning. As a result, a new managerial position, that of the Cybersecurity Manager, is required in order to handle all required objectives and ensure the cybersecurity process's correctness throughout the entire life cycle of the designed system. The Cybersecurity Manager is, e.g., responsible for working with the penetration assessment team on the scheduling and execution of penetration assessments. During the execution of tests, the vulnerabilities of system safety/autonomous features should be verified. The evaluation should, therefore, be planned in coordination with a Functional Safety Manager in order to coordinate a mitigation plan for the safety/autonomous feature vulnerabilities.

Key management also creates a new complexity layer. In order to handle security artefacts, the entire IT infrastructure must be established. This includes, for instance, a Public Key Infrastructure that is used for the creation of digital certificates and the management of public key encryption. There must be procedures for the distribution of key materials to vehicles during production and maintenance. Any vulnerabilities found in these fields could lead to safety losses if, for instance, an attacker compromises the binary in safety-critical/autonomous ECUs.

The cybersecurity areas mentioned in the third column of Table 3 have an impact on functional/autonomous system safety processes because they necessitate the additional consideration of safety-critical systems in order to cover all system use cases.

The foundation of a system design is known as the concept development. For cybersecurity, an extensive analysis of potential threats to defined cybersecurity items, as well as risk assessment and mitigation plans, is required. This concludes with a definition of the cybersecurity concept. This section encapsulates the essence of holistic engineering. All possible hazard scenarios due to unreasonable risk or autonomous use cases should be considered in order to obtain a complete security concept. As a result, all of these areas have an impact on the functional/autonomous system safety processes.

To complete the design activities, a system design is needed, which consists of the system boundaries, actors, and use cases. Only after all safety, security, and autonomous functions have been considered can the overall system architecture be created.

According to the V-model, the detail design activities come next. They include the definition of the developed solution's hardware (HW) and software (SW) architectures. To fit the cybersecurity concept, appropriate hardware measures must first be considered, for example, the microcontroller selection, choosing secure hardware elements (hardware

security module—HSM; trusted platform module—TPM), obscuring electronic paths, or physically preventing the product's cover from being opened. From a software standpoint, the selection of secure libraries, memory and memory process isolation, and secure coding must be ensured. To complete the analysis, all of these activities must be considered for the sake of safety and autonomy. All potential vulnerabilities must be investigated from both a cybersecurity and a safety standpoint, especially in vehicles with a high level of autonomy. The selection of appropriate electronic components has a direct impact on both safety and cybersecurity.

The final step is to double-check the solution that has been implemented. Cybersecurity requirements must be validated at all levels, including software testing, integration testing, and system testing. This includes both hardware and software testing. In this case, all cybersecurity testing and refinement must be performed concurrently with safety and autonomous functions. These cannot be treated in isolation because, if a specific cybersecurity function (e.g., security of a safety-critical signal) that is supposed to protect the safety function (e.g., emergency braking) is not implemented correctly, this has an impact on the end user's safety.

Finally, the product must be manufactured. Cybersecurity is also involved when it comes to generating/providing security artefacts (such as symmetric/asymmetric keys, certificates, etc.) in the ECU, as well as exchanging confidential information between OEMs and Tier 1 suppliers. If an ASIL product is considered, extensive testing during the manufacturing process is required in order to ensure that each produced unit is correctly assembled. The challenge is to carry out security functions while ensuring that they do not interfere with the final product's functionality.

Post-production and decommissioning are two additional product development processes that were not previously extensively considered. If a severe malfunction is detected after production, a software update is required. This can be performed in a workshop or, if possible, over the air (OTA). This poses a new threat to vehicles, necessitating the implementation of proper cybersecurity measures, such as digital software signing. Furthermore, adequate safety measures must be implemented to avoid potentially hazardous situations during and after software updates. An extensive rollback scenario must be considered for a safety-critical autonomous system.

Starting with the managers and moving on to the IT system, information security, and, finally, external audits, the functional/autonomous system safety process is also impacted because these components must work in a secure environment, which is provided by cybersecurity measures.

By analyzing the impact of cybersecurity on electric vehicle product development and the supporting processes in Table 3 and 4, we can see that only two of the 40 security areas mentioned—cybersecurity responsibilities and cybersecurity cases—do not have a direct impact on the safety process for autonomous systems.

Furthermore, cybersecurity affects areas such as post-production and decommissioning, which have previously received little attention. As a result, collaboration between cybersecurity and other areas must be established at each process level. This is especially critical during the concept phase, in which decisions that affect the entire product development strategy are made.

Risk assessment is a key aspect of the development of new products therefore, we analyzed risk assessments more closely. However, the processes of cybersecurity and functional/autonomous system safety approach this activity from different perspectives.

With cybersecurity, the process of TARA is performed once the items of cybersecurity are defined. According to ISO 21434 [4], the process consists of an asset definition, threat scenario identification, impact rating, attack path analysis, attack feasibility rating, risk value determination, and risk treatment decision. The impact rating is evaluated for each identified asset; it is used to assess if a particular threat scenario can lead to financial, confidential, operational, or safety damages. Afterwards, the analysis goes through the

next steps, which lead to the assignment of a cybersecurity assurance level (CAL), the definition of the cybersecurity goals, and to the definition of the security requirements.

Similarly, functional/autonomous system safety processes start with the definition of an item; then, a hazard analysis and risk assessment are performed, which lead to the assignment of an automotive safety integrity level (ASIL). After this activity, the safety goals are defined and the safety requirements are prepared. Annex F of ISO 21434 [4] offers guidance on how damage to safety can be rated. However, the given example does not cover multiple road users in a single damage scenario. This provides an area that can be improved for better ratings of damage that impacts more road users. Based on the guidelines, as an example, we propose a more detailed rating system, which is presented in Table 5. These ratings should be specific to organizations and systems. They differentiate between a single road user and multiple road users who are affected by damage to safety due to a potential cybersecurity threat. The values assigned to safety damage can be adjusted depending on the organization's specific approach.

Table 5. Example safety impact rating criteria for TARA analysis.

Safety Impact	Description	Value
Road traffic accident	The threat may cause a life-threatening injury to multiple car operators and road participants (survival uncertain).	V8
Life threatening—multiple users	The threat may cause a life-threatening injury to a vehicle operator or more than one road participant (survival uncertain).	V7
Life-threatening—single user	The threat may be life threatening to a vehicle operator or a road participant (survival uncertain).	V6
Severe injury—multiple users	The threat may cause a severe injury to a vehicle operator or more than one road participant (survival probable).	V5
Severe injury—single user	The threat may cause a severe injury to a vehicle operator or a road participant (survival probable).	V4
Light injury—multiple users	The threat may cause a light injury to a vehicle operator or more than one road participant.	V3
Light injury—single user	The threat may cause a light injury to a vehicle operator or a road participant.	V2
No injury	The threat cannot cause injury to a vehicle operator or a road participant.	V1

This results in a connection between TARA and HARA, which is shown in Figure 6. Once an impact rating is defined in TARA for safety damage in a threat scenario, the hazard identification during the HARA analysis must be refined. The hazard taken from the possible system vulnerability must be considered (Green Arrow 2). However, this is not a one-way connection. For safety-critical/autonomous systems, the safety cannot be guaranteed without cybersecurity measures. Therefore, all identified hazards must be considered during threat scenario identification (Blue Arrow 1). In Figure 6 we do not describe HARA in detail for our analysis because we would like to concentrate on TARA due to its dependency on particular ECU use cases. The entire process results in a combination of cybersecurity and safety goals after incorporating the impacts of TARA and HARA. In consequence, the FS/autonomous and cybersecurity requirements better reflect the system's needs.

For a V2G gateway, an example of the cooperation between TARA and HARA is an inlet temperature sensor, which monitors a vehicle's inlet temperature during charging. The temperature sensor is a safety-critical item because a malfunction in this sensor may lead to the vehicle catching fire. Therefore, FS measures are taken to protect the user when a defect in occurs in the sensor (e.g., a signal plausibility check, sensor redundancy, end-to-end protection, or safe state). However, this is not enough. Information from the temperature sensor is sent to a battery management system. The ECU must be protected by cybersecurity measures against manipulation (e.g., spoofing, tampering, etc.). Any vulnerabilities found in this case can cause the same risks as those in the FS case. This type of analysis must be carried out at an early stage of product development. Any deficiencies found later in development can lead to significant architectural modifications, which can not only include software, but also hardware changes. The time and development costs thus increase.

In addition, if any vulnerabilities are identified in the field, the consequences may be even greater if the entire fleet is updated. The ADAS system of a U.S. OEM was, as described in [44], not prepared for phantom attacks (where fake objects are considered as real). While the OEM refused to accept the error, the software responsible for data identification was deleted shortly after publication, and this actually required additional costs and time for a redesign and reimplementation.

We were able to gather information regarding how cybersecurity activities were planned for the development of a single V2G (vehicle-to-grid) gateway ECU for a premium German OEM after interviewing the planning teams of one of the leading Tier 1 automotive suppliers. The specifications for the ECU included approximately 8000 requirements, in addition to more than 1000 requirements related to the cybersecurity component. The project is still in the development phase. The V2G ECU will be mounted in an electric vehicle. For the needs of this paper, we examined only the design process.

For the project analyzed here, the initial planning assumed that the cybersecurity design activities would be taken over by the systems engineering (SE) department (a total of four or five systems engineers, including one required engineer, were involved in the project). The effort was estimated to require half of the systems engineering resources until the pre-production phase, which, in total, would last six quarters, i.e., quarters 1, 2, 3, 4 of the first year of the product's development and quarters 1 and 2 of the second year of the product's development. Moreover, the support of a fraction of 0.2 of the systems engineering resources was planned for the next three quarters until the start of production. No estimates were made for the maintenance or decommissioning phases. The overall effort needed for the cybersecurity design was calculated as 0.02% of the estimate of the effort required for the entire project. The initial project resource estimates are presented in Table 6, where a system engineering effort is presented as man-effort.

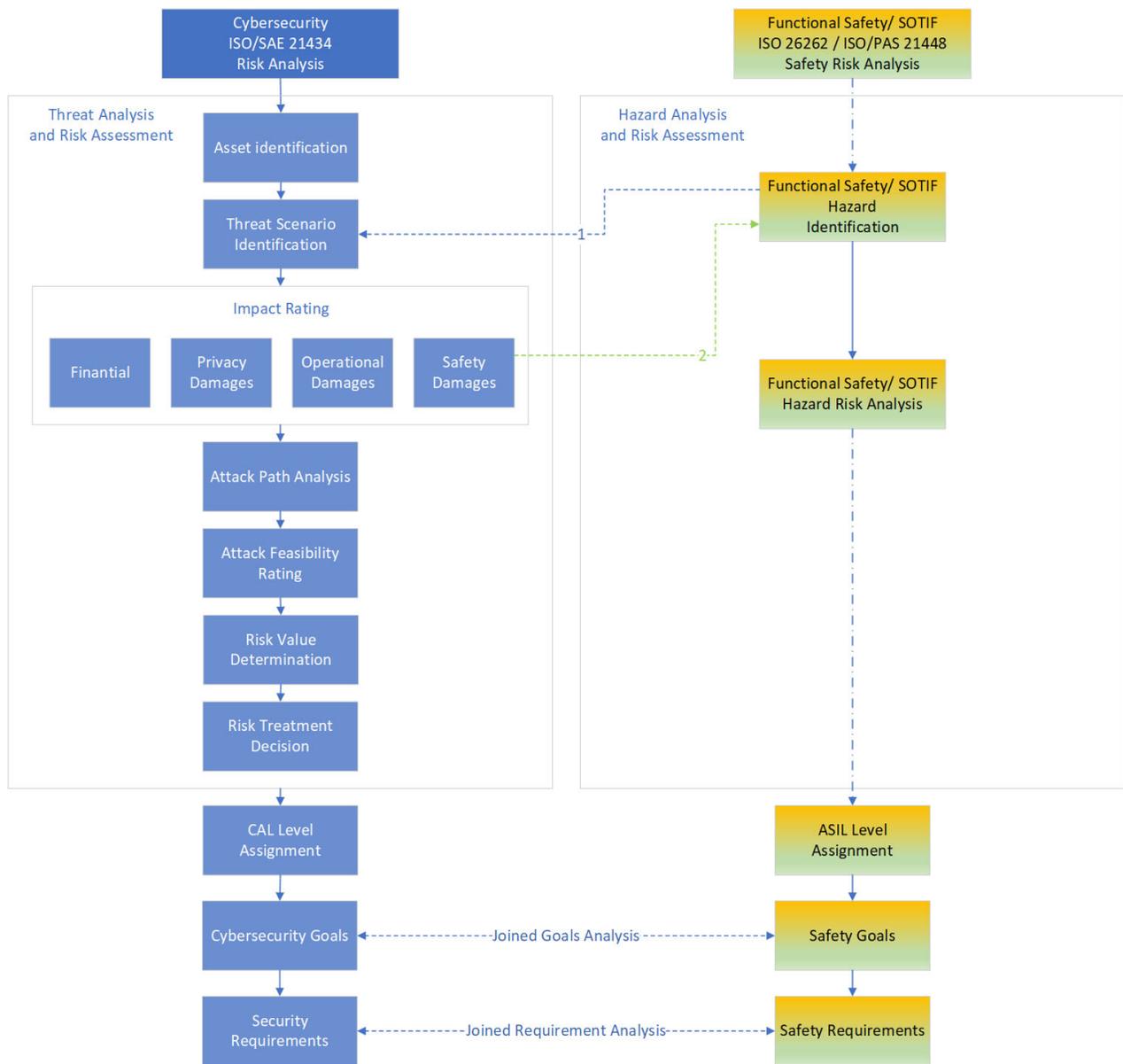


Figure 6. The impact of cybersecurity risk analysis on functional safety/SOTIF risk analysis.

Table 6. Initially estimated systems engineering effort for the cybersecurity design of the V2G gateway ECU.

Year	Quarter	Systems Engineering Effort
1	Q1	0.5
1	Q2	0.5
1	Q3	0.5
1	Q4	0.5
2	Q1	0.5
2	Q2	0.5
2	Q3	0.2
2	Q4	0.2
3	Q1	0.2
3	Q2	0.2
3	Q3 ¹	0
3	Q4	0

¹ Start of production.

After only one year of development, the hours reported for the cybersecurity activities reached 4% of the hours of the overall project design activities. Moreover, in total, two resources were involved in the cybersecurity design—one from the systems engineering team and the other from the software team (SW). The effort reported by the systems engineering team reached 1.5% of the entire project effort, and from the software engineering side, it reached 2.5%. The activities are not yet finished (the project has advanced to approximately 70% completion). The current assumption is that one more resource should be added for each competency, i.e., SYS and SW, due to the new regulations and customer requirements. Table 7 presents the re-estimated engineering effort for the cybersecurity design, and it includes the forecasted effort for the growth of features. Just as in Table 6, Table 7 systems engineering effort is presented as man-effort.

Table 7. Re-estimated engineering effort for the cybersecurity design of the V2G gateway ECU after 1 year of development.

Year	Year 1	Systems Engineering Effort	Software Engineering Effort
1	Q1	1	1
1	Q2	1	1
1	Q3	1	1
1	Q4	1	1
2	Q1	2	2
2	Q2	2	2
2	Q3	2	2
2	Q4	2	2
3	Q1	2	2
3	Q2	2	2
3	Q3 ¹	1	2
3	Q4	1	2

¹ Start of production.

4.2. Combined V-Model for Autonomous Cyber-Physical Systems

4.2.1. Cybersecurity, Functional Safety, and Autonomous Engineering Impact the Development Cycle of the Standard V-Model

New areas of automotive engineering, such as cybersecurity and SOTIF, have introduced another work product into the well-known V-model for the development of safety-critical systems.

An example of the workflow for cybersecurity product development is available in the ISO 21434 draft document [4]. The left side of the V-model includes the following:

- Item definitions;
- Cybersecurity goals;
- Cybersecurity requirements;
- Cybersecurity concept;
- System cybersecurity requirements;
- System architectural design;
- Hardware cybersecurity requirements;
- Hardware architectural design;
- Software cybersecurity requirements; and
- Software architectural design.

The right side of the V-model includes the following:

- Cybersecurity validation;
- Item integration verification;
- System integration verification;
- Hardware integration verification; and
- Software integration verification.

There is an overlap in the systems engineering approaches used for cybersecurity and safety processes. The process dependencies are shown in Figure 7.

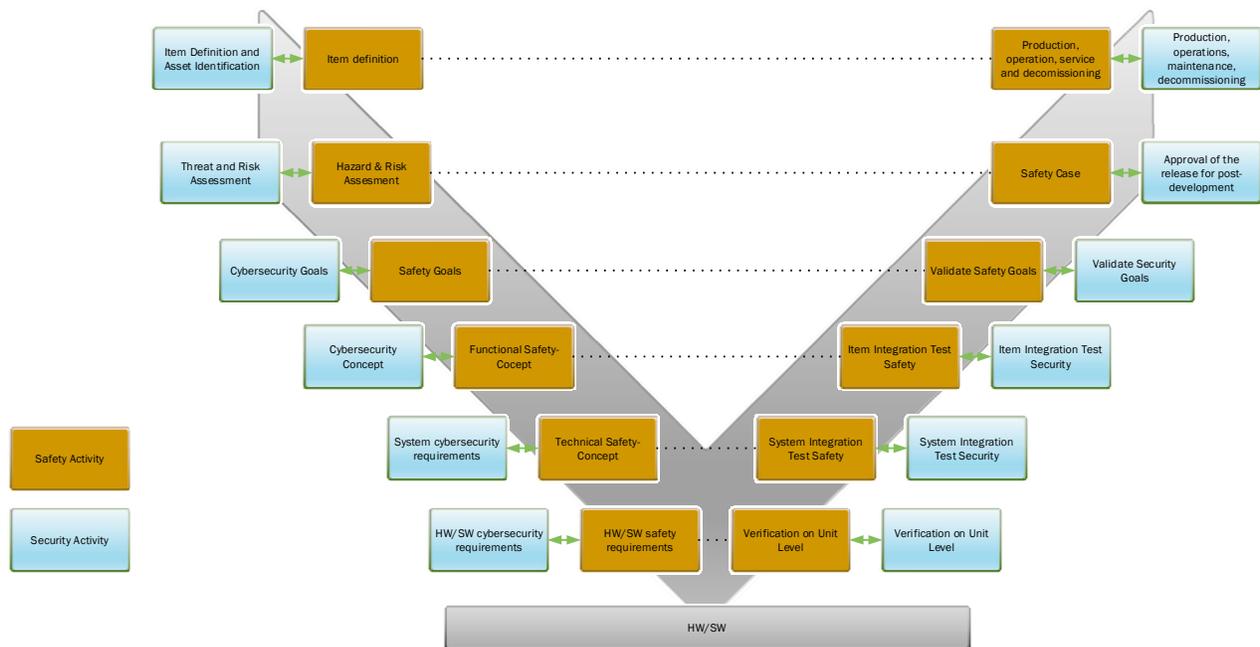


Figure 7. V-model for safety and cybersecurity activities according to the ISO 26262 and ISO/SAE 21434 standards.

Similarly, ISO/PASS 21448 [3] defines the possible interactions of product development activities with the processes of the ISO 26262 series. The left side of the v-model, which is responsible for the project’s definition, is covered by the following:

- Clause 5—Functional and System Specification;
- Clause 6—SOTIF-related Hazard Identification and Risk Evaluation;
- Clause 7—Identification and Evaluation of Triggering Events; and

- Clause 8—Functional Modification to Reduce SOTIF risks.

The right side of the v-model, which is responsible for the testing and integration of the project, is covered by the following:

- Clause 9—Definition of the Verification and Validation Strategy;
- Clause 10—Verification of the SOTIF: Evaluation of Known Scenarios;
- Clause 11—Validation of the SOTIF: Evaluation of Unknown Scenarios; and
- Clause 12—Methodology and Criteria for SOTIF Release.

Considering the relations between all of the processes, a combined V-model for autonomous cyber–physical systems is proposed in Figure 8.

Each process on the left side of the combined V-model is verified and validated by the corresponding process on the right side; these relationships are represented by the dotted lines in Figure 8. The verification and validation activities are not performed in a single run. These are added to the loop, along with project development milestones.

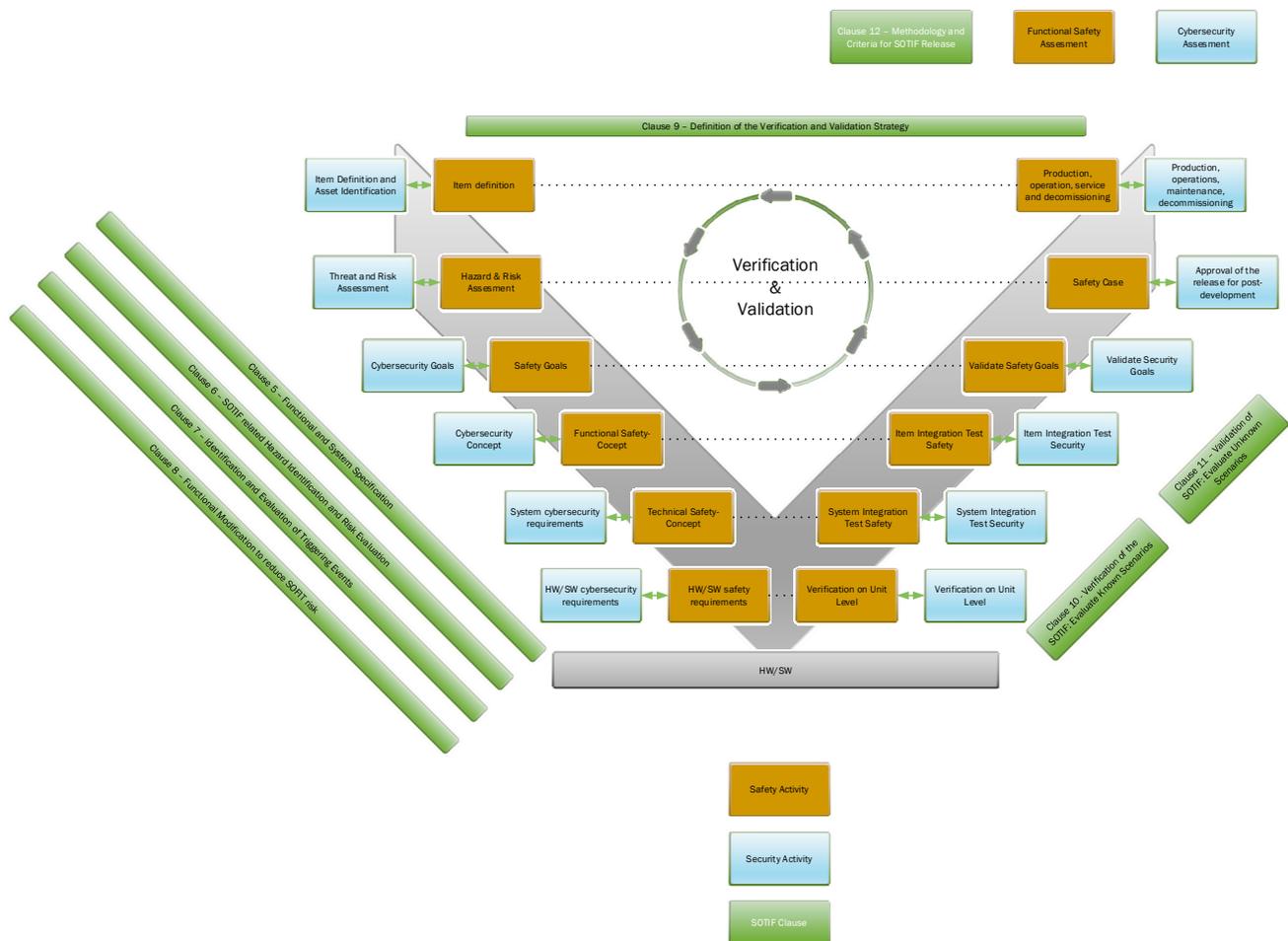


Figure 8. Combined V-model for autonomous cyber–physical systems.

4.2.2. Analysis Coordination

During the design of a complex ECU for an electric vehicle, the number of analytical work products needed is substantial. These products require early cooperation between engineering teams during the concept phase, shared system understanding, and mutual awareness in order to achieve a complete analysis.

Currently, for systems that require FS, cybersecurity, and autonomous driving (AD) work products, the analysis is performed with insufficient coordination. Early on, the work is not organized, and knowledge is not shared among the engineers involved.

The present state is shown in Figure 9. The green portion represents the systems engineering (SE) workflow and shows the requirements of the involved competencies. FS, cybersecurity, and AD engineering activities are represented in yellow, and finally, the regulations that they must consider are shown in blue. The light blue color signifies future market regulations.

The SE team is responsible for the definition of the entire system, as well as its boundaries, use cases, and requirements. If the system requires FS, cybersecurity, or AD analyses, the systems engineer passes the information to the responsible team and waits for the results. Therefore, the analyses are performed in later product development stages, leading to incomplete work products. Moreover, at this design phase, it is challenging to incorporate any analysis outcomes into the system design. As a result of this, the system is not optimally designed, and it is not robust enough.

In order to improve the design of ECUs for electric vehicles, we propose an integrated approach based on the processes of systems engineering; this approach includes activities related to FS, cybersecurity, and AD in the early stages of concept development. The systems engineer is still responsible for the definition of the system however, the feedback from the engaged competencies is collected before the final system design is completed. The FS, cybersecurity, and autonomous systems engineers work iteratively on small portions of the requirements provided by the SE team. The systems engineer is responsible for the coordination of analyses between engineers. Each iteration of the work products is jointly reviewed by the involved competencies, and the results of the reviews are stored in the project's repository. The numbers of iterations and requirement portions are adjusted according to the project's scope and available resources.

The engineering cooperation is shown in Figure 10. The green solid line represents the flow of information between the involved engineering competencies, i.e., FS, cybersecurity, AD, and SE—level 1. In practice, this coordinating role can be played by the lead systems engineer. The yellow dotted line represents the flow of information on the second level, i.e., only FS, cybersecurity, and AD. Finally, the blue dotted lines on level 3 represent the dependencies between engineering activities. The last level shows the regulations that should be considered for each competency during the creation of a work product. The possible future regulations are represented in light blue below the already available regulations.

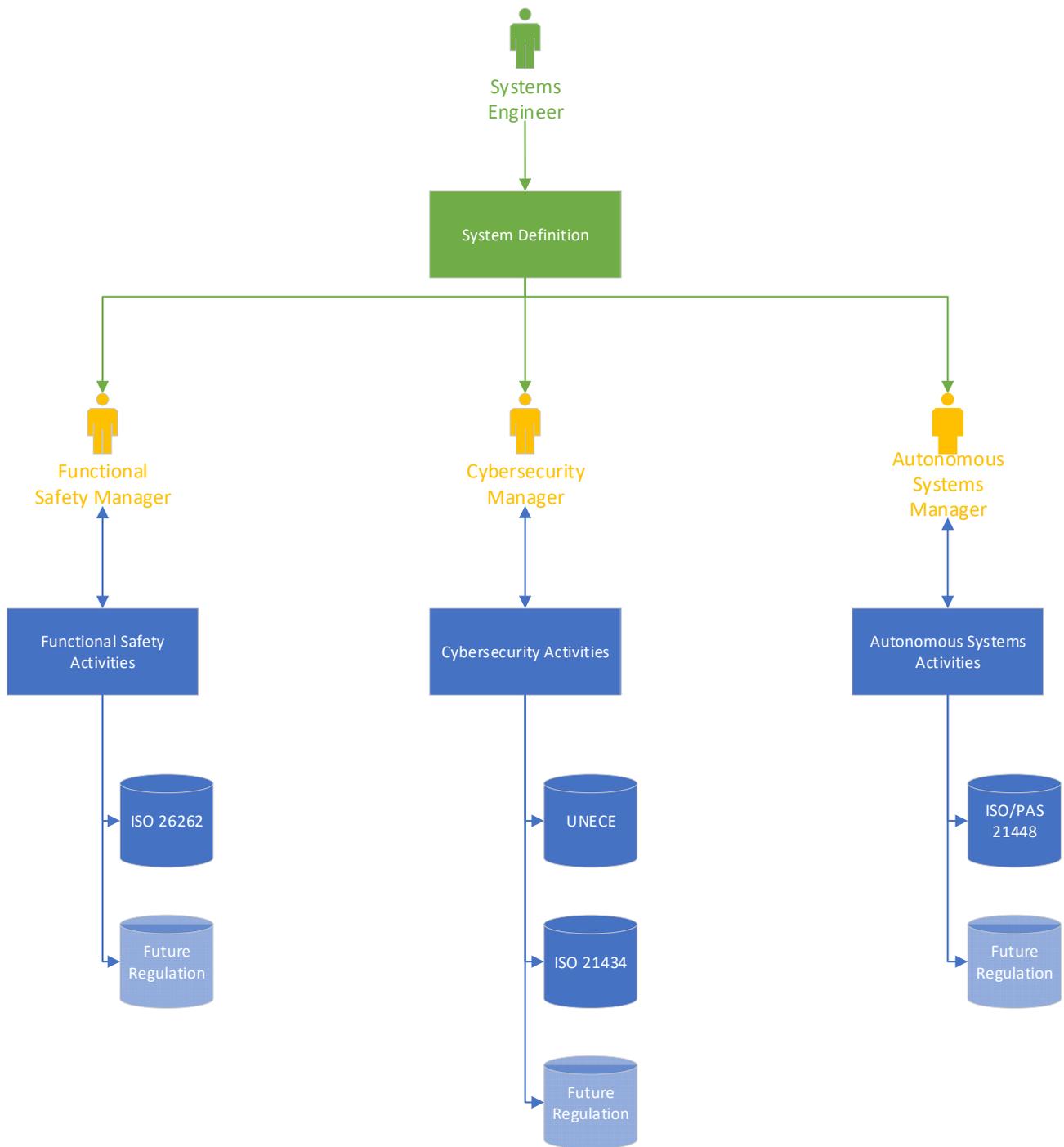


Figure 9. Current flow of information during the design of an ECU.

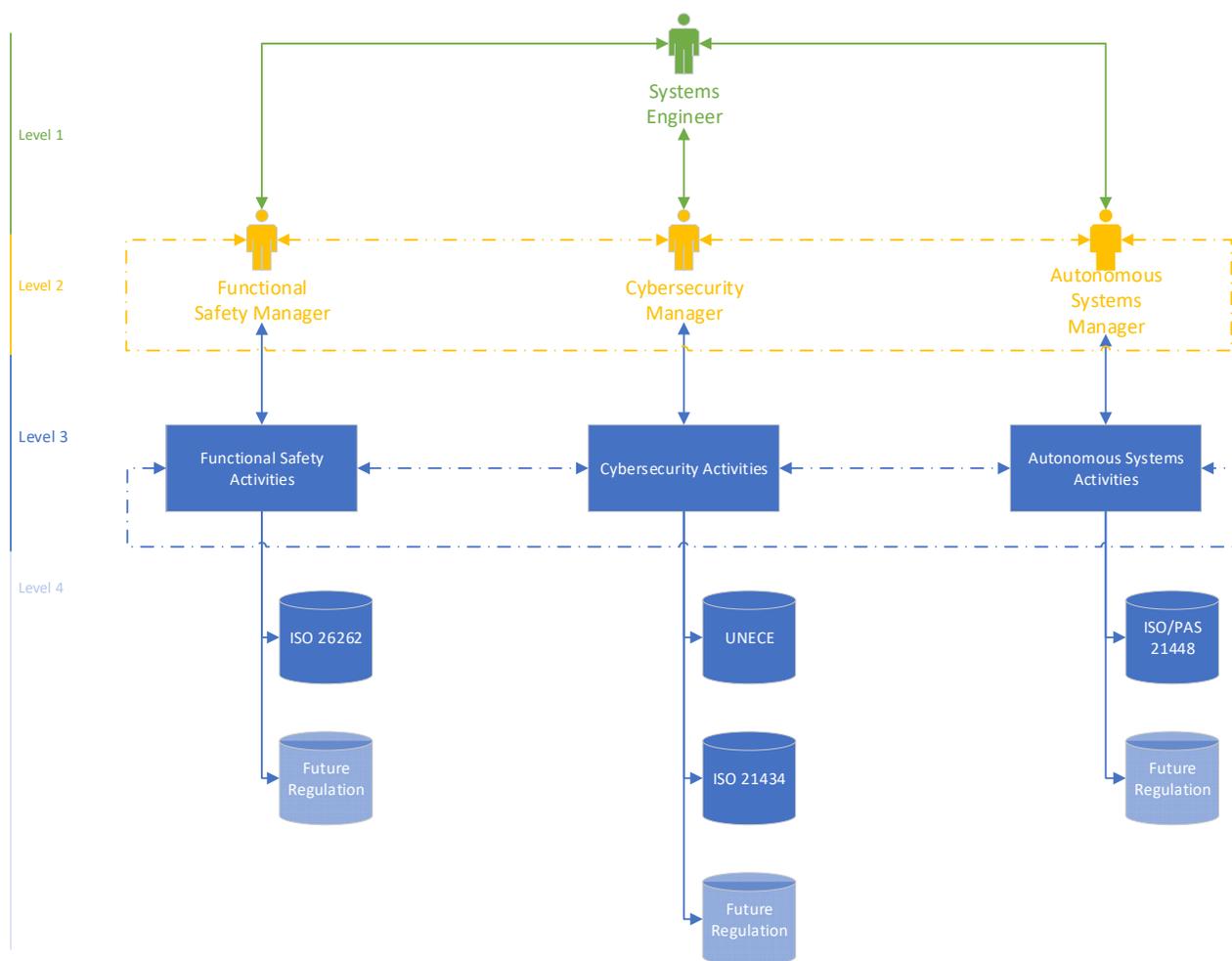


Figure 10. Coordination of ECU analyses.

5. Discussion

The new EC/TRANS/WP.29/2020/79 regulation and the ISO 21434 standard has caused a shift towards cybersecurity for all vehicle engineering and management processes. OEMs must establish CMSMs to manage and improve cybersecurity. Similarly to FS, this means that additional analyses should be used to choose the functions that should be protected. Moreover, this will result in the assignment of cybersecurity assurance levels. The CAL informs the supplier of the level of security that must be implemented in order to protect a certain functionality. However, the CAL analysis in ISO 21434 is only a guideline. Each OEM must establish its own definition of the CAL. This problem will be further analyzed and, eventually, standardized in ISO 21434 in order to have a common understanding, similarly to the ASIL levels for FS.

Suppliers are also affected by the cyber shift. They must establish similar processes throughout the entire development cycle on their side in order to fulfill the requirements of ISO 21434. Furthermore, each supplier must prove its processes with proper certification of the results. This adds to the project's costs, but in order to maintain the market position and release the vehicle, suppliers and customers must collaborate closely to meet the demands of the modern industry.

In the analysis of the estimates of the effort in the example of the cybersecurity design for a V2G Gateway ECU from a leading Tier 1 supplier, an underestimation of the related effort could be observed. The cybersecurity activities were not properly quoted, while new regulations and customer requirements emerged. At this point in time where not all

standards were officially released, the costs of the cybersecurity design project reached 12% of the costs of all design processes, considering the average three-year development period. Therefore, proper estimations of cybersecurity activity processes should be more in focus. Since cybersecurity affects all development areas, it cannot be isolated. More cooperation between various process areas is required in order to provide complete work products. The challenge is to identify overlapping activities and combine design efforts in order to reduce the time and costs needed for engineering tasks. Moreover, a separate process entity should be established inside engineering divisions to manage cybersecurity processes. The culture of cybersecurity is not yet well established in engineering groups involved in the processes of developing new products. With the introduction of ISO 21434 and other cybersecurity regulations, e.g., ECE/TRANC/WP/29/2020/79, this kind of process expertise will be required.

Together with the new process areas, which should increase vehicles' overall safety, the standard V-model proposed by the ASPICE® must be updated. It must include all recent areas defined in ISO 21434 and ISO/PAS 21448. For this purpose, we introduced the combined V-model for autonomous cyber-physical systems. Nevertheless, a more detailed analysis will be performed for all process areas in order to identify overlapping processes and define similarities. This will include project management, planning, team coordination, requirement management, system design, coding, test reports, assessment reports, etc. This will reduce time and costs and will help manage the risks involved in the development of new autonomous cyber-physical systems.

A work product that can be used for all newly identified areas is the failure mode and effect analysis (FMEA). This type of operation usually consists of a design failure mode and effect analysis (DFMEA) and process failure mode and effect analysis (PFMEA). Since these analyses are already known to the industry, adding new items to them from the cybersecurity and AD areas might create a solid background for further project design phases. However, cybersecurity and vehicle autonomy bring a dynamic factor to well-known analytical schemas. In this case, risk analysis is no longer finite work. As a matter of fact, the real risks start when a vehicle is delivered to an end customer. It then becomes part of a connected ecosystem that is vulnerable to threats. Each vulnerability can be used to capture sensitive data, take control of, or steal the vehicle. Therefore, over-the-air (OTA) updates play a significant role in the creation of a safe environment.

TARA determines the extent to which a road user can be impacted by a threat scenario. There are several steps to be performed during this analysis, such as asset identification, threat scenario identification, determination of the impact rating, identification of the attractive paths for identified threat scenarios, determination of the easiness of exploitations, derivation of the risk values, and selection of the appropriate risk treatments for mitigating the threat scenarios. This analysis is performed at the design phase of project development. Currently, the level of detail of TARA has not been determined. Therefore, it is mainly limited to a system-level view. However, because cybersecurity impacts electrical engineering, software engineering, and other factors, it is necessary to add more detailed analyses. One suggestion is to create separate TARA work products for each involved competency, i.e., to perform TARA on the system, hardware, and software levels to cover all possible threats. This approach is also common for DFMEA analyses, where engineers from different fields add their input from the areas in which they are experts. Undoubtedly, this activity must be managed by a cybersecurity project's representative, who will guide engineers from different fields in the cybersecurity domain.

Our integrated framework for electronic control unit design based on a system engineering approach will improve cooperation among engineers in the automotive sector during the design of a system concept. One of the work products that is affected by this approach is the system architecture document. Currently, system architectures for ECUs are designed prior to the FS, cybersecurity, and AD analyses. Therefore, any changes introduced during further analyses are not considered. Our framework allows

for cooperation among engineers during the product design phase in order to achieve more flexibility. In the case of system architecture, this implies more interactions among engineers—which are coordinated by the systems engineer—in order to complete the entire system design and introduce changes in early design phases. Further regulations will be examined to determine if they can also be considered during the vehicle design phases. One candidate is the ISO 15118 [45] series, which describes vehicle-to-grid communication.

Apart from the standard processes for autonomous cyber–physical systems, there is also a need for a standard template that can be used during the design of systems to mitigate known cyber risks. The widely-used concepts for, e.g., enterprise systems, networking systems, etc., are design patterns, which support the understanding of problems and their solutions. Therefore, the given problem can be solved in the most optimal way.

Moreover, for the automotive industry, similarly to ICT (information and communications technology), the concept of security by design will be followed. At present, in software development, the features of cybersecurity are treated as add-on functionalities for an already working solution. This may lead to the introduction of vulnerabilities because the solutions are verified at the very end. Hence, further research will need to be undertaken to embed the cybersecurity analysis into the early stage of software development together with verification and validation techniques.

6. Conclusions

In the automotive industry, the complexity of the systems that are designed is increasing dramatically. In addition to their high technical performance, modern vehicles must have a high level of safety and security. In terms of FS standards, such as ISO 26262, the requirements and processes have been well defined and are widely used by OEMs and their suppliers. Cybersecurity standards, on the other hand, are not yet at the same maturity level. As a result, engineering teams that design ECUs with cybersecurity components use not only mandatory standards, which are required for the products to be admitted to the market, but also non-obligatory standards, such as PAS 1885, which consist of guidelines and the best practices.

Incorporating both the FS and cybersecurity domains into the development and implementation process of an ECU is extremely difficult and necessitates changes not only in the design and development processes, but also in the entire organization, particularly in the processes that support cybersecurity mechanisms (e.g., key handling). The example presented in this paper demonstrates that companies have issues with the incorporation of cybersecurity into ECU design processes. It has a negative impact on the management of such projects, particularly in terms of costs and timeliness. The proposed framework is one of the threads of discussion in the automotive industry about incorporating the cybersecurity domain into the design process for ECUs with FS and cybersecurity components.

The presented framework is based on the analysis of the V2G design project. It will need to be verified on other types of designed system, especially on autonomous driving systems.

Author Contributions: Conceptualization, A.B. and P.P.; methodology, A.B. and P.P.; validation, A.B. and P.P.; formal analysis, P.P.; investigation, P.P.; resources, A.B. and P.P.; data curation, P.P.; writing—original draft preparation, A.B. and P.P.; writing—review and editing, A.B. and P.P.; visualization, A.B. and P.P.; supervision, A.B.; project administration, P.P.; funding acquisition, A.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Council of Scientific Discipline Management and Quality Sciences of the Warsaw University of Technology.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data could be obtained upon request from authors.

Conflicts of Interest: The authors declare no conflicts of interest.

References

- Oehmen, J. *The Guide to Lean Enablers for Managing Engineering Programs*; MIT-PMI-INCOSE: 2012. Available online: <https://dspace.mit.edu/handle/1721.1/70495> (accessed on 31 March 2021).
- ISO. INTERNATIONAL STANDARD 26262 Road Vehicles—Functional Safety. 2018; Volume 2018. Available online: <https://www.iso.org/standard/68383.html> (accessed on 31 March 2021).
- ISO/PAS. ISO/PAS 21448 Road Vehicles—SAFETY of the Intended Functionality. 2019. Available online: <https://www.iso.org/standard/70939.html> (accessed on 31 March 2021).
- ISO/SAE. ISO/SAE DIS 21434 Road Vehicles—Cybersecurity Engineering—Draft. 2020. Available online: <https://www.iso.org/standard/70918.html> (accessed on 31 March 2021).
- Axelrod, C.W. Cybersecurity challenges of systems-of-systems for fully-autonomous road vehicles, In Proceedings of the 2017 13th International Conference and Expo on Emerging Technologies for a Smarter World (CEWIT), Stony Brook, NY, USA, 7 November 2017; pp. 1–6, doi:10.1109/CEWIT.2017.8263141.2017.
- Martin, H.; Ma, Z.; Schmittner, C.; Winkler, B.; Krammer, M.; Schneider, D.; Amorim, T.; Macher, G.; Kreiner, C. Combined automotive safety and security pattern engineering approach. *Reliab. Eng. Syst. Saf.* **2020**, *198*, doi:10.1016/j.ress.2019.106773.
- VDA QMC. Working Group 13/Automotive SIG. Automotive SPICE Process Assessment/Reference Model. 2017. Available online: http://www.automotivespice.com/fileadmin/software-download/AutomotiveSPICE_PAM_31.pdf (accessed on 31 March 2021).
- Messnarz, R.; Kreiner, C.; Macher, G.; Walker, A. Extending Automotive SPICE 3.0 for the use in ADAS and future self-driving service architectures. *J. Softw. Evol. Process.* **2018**, *30*, 1–14, doi:10.1002/smr.1948.
- Walker, A. Cybersecurity in safety-critical systems. *J. Softw. Evol. Process.* **2018**, *30*, 4–9, doi:10.1002/smr.1956.
- Ulrich, K.; Eppinger, S.; Yang, M. *Product Design and Development*, 7th ed.; McGraw-Hill Education: 2020.
- Cooper, R. Stage-Gate Systems: A New Tool for Managing New Products. *Bus. Horiz.* **1990**, 44–54.
- Ohno, T. *Toyota Production System: Beyond Large-Scale Production*; CRC Press: Portland, OR, USA, 1988.
- Womack, J.; Jones, D.; Ross, D. *The Machine That Changed the World*; Free Press: New York, NY, USA, 1990.
- Oppenheim, B. Lean Product Development Flow. *Syst. Eng.* **2004**, *7*, 352–376.
- Ward, P. *Lean Product and Process Development*; Lean Enterprises Inst. Inc.: Cambridge, MA, USA, 2007.
- Morgan, J.; Liker, J. *The Toyota Product Development System*; Productivity Press: New York, NY, USA, 2007.
- Oppenheim, B. *Lean for Systems Engineering with Lean Enablers for Systems Engineering*; Wiley: Hoboken, NJ, USA, 2011.
- Oehmen, J.; Rebertsch, E. *Waste in Lean Product Development*; Initiative LAI-MIT: 2010, Available online: <https://dspace.mit.edu/handle/1721.1/79838> (accessed on 31 March 2021)
- Pernalst, J.; Feldt, R.; Gorschek, T.; Floren, D. FLEX-RCA: A lean-based method for root cause analysis in software process improvement. *Softw. Qual. J.* **2019**, *27*, 389–428, <https://doi.org/10.1007/s11219-018-9408-8>.
- Stirgwort, P. Effective management of functional safety for ISO 26262 standard. *Proc. Annu. Reliab. Maintainab. Symp.* **2013**, doi:10.1109/RAMS.2013.6517758.
- ISO/TS. ISO/TS 16949:2009 Quality Management Systems—Particular Requirements for the Application of ISO 9001:2008 for Automotive Production and Relevant Service Part Organizations. 2009. Available online: <https://www.iso.org/standard/52844.html> (accessed on 31 March 2021).
- UNECE. UNECE, 2020. Available online: <https://unece.org/> (accessed on 31 March 2021).
- United Nations Economic and Social Council. Proposal for a New UN Regulation on Uniform Provisions Concerning the Approval of Vehicles with Regards to Cyber Security and Cyber Security Management System. 2020. Available online: <http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf> (accessed on 31 March 2021).
- SAE. Cybersecurity Guidebook for Cyber-Physical Vehicle Systems J3061_201601. 2016. Available online: https://www.sae.org/standards/content/j3061_201601/ (accessed on 31 March 2021).
- Torok, A.; Szalay, Z.; Saghi, B. New Aspects of Integrity Levels in Automotive Industry—Cybersecurity of Automated Vehicles, *IEEE Trans. Intell. Transp. Syst.* **2020**, 1–9, doi:10.1109/TITS.2020.3011523.
- BSI. BS PAS 1885:2018 The Fundamental Principles of Automotive Cyber Security. Specification. 2018. Available online: <https://www.bsibadge.com/productdetails/BSI/BSI30365446/pas1885> (accessed on 12 May 2021).
- Sabaliauskaite, G.; Cui, J.; Liew, L.S.; Zhou, F. Integrated safety and cybersecurity risk analysis of cooperative intelligent transport systems. In Proceedings of the 2018 Joint 10th International Conference on Soft Computing and Intelligent Systems (SCIS-ISIS 2018) and 19th International Symposium on Advanced Intelligent Systems, 5 December 2018, Toyama, Japan; pp. 723–728, doi:10.1109/SCIS-ISIS.2018.00120.
- SAE. Surface Vehicle Recommended Practice J3016. 2018. Available online: https://www.sae.org/standards/content/j3016_201806/ (accessed on 31 March 2021).
- Zhang, X.; Zhou, M.; Shao, W.; Luo, T.; Li, J. The architecture of the intended safety system for intelligent driving. In Proceedings of the 2019 IEEE International Symposium on Circuits and Systems (ISCAS), Sapporo, Japan, 26–29 May 2019; p. 3, doi:10.1109/ISCAS.2019.8702580.

29. Kyrkou, C.; Papchristodoulou, A.; Theocharides, T.; Kloukiniotis, A.; Papandreou, A.; Lalos, A.S.; Moustakas, K. Towards artificial-intelligence-based cybersecurity for robustifying automated driving systems against camera sensor attacks. In Proceedings of the 2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 6–8 July 2020, Limassol, Cyprus; pp. 476–481, doi:10.1109/ISVLSI49217.2020.00-11.
30. Macher, G.; Schmittner, C.; Dobaj, J.; Armengaud, E.; Messnarz, R. An Integrated View on Automotive SPICE, Functional Safety and Cyber-Security. *SAE Tech. Pap.* **2020**,, doi: 10.4271/2020-01-0145.
31. Lee, T.Y.; Lin, I.A.; Liao, R.H. Design of a Flex Ray/Ethernet Gateway and Security Mechanism for In-Vehicle Networks. *Sensors* **2020**, *20*, 3.
32. Warg, F.; Skoglund, M. Argument patterns for multi-concern assurance of connected automated driving systems. In Proceedings of the 4th International Workshop on Security and Dependability of Critical Embedded Real-Time Systems, CERTS, 9 July 2019, Stuttgart, Germany; volume 73, , doi:10.4230/OASlcs.CERTS.2019.3.
33. Appel, M.A.; Ahmed, Q. Intelligent vehicle monitoring for safety and security. SAE Technical Paper 2019-01-0129, 2019, doi:10.4271/2019-01-0129.
34. Lo Bello, L.; Mariani, R.; Mubeen, S.; Saponara, S. Recent Advanced and Trends in On-Board Embedded and Networked Automotive Systems. *IEEE Trans. Ind. Inform.* **2019**, *15*, 1038–1051.
35. Pisoni, F.; Avellone, G.; Grazia, D.D.; Silverio, A.; Durand, J.; Garcia, J.; Tijero, E.D.; Falletti, E. GNSS functional safety for the autonomous vehicle. In Proceedings of the 32nd International Technical Meeting of the Satellite Division of the Institute of Navigation, ION GNSS+2019, Miami, FL, USA, 16–20 September 2019; pp. 1696–1706.
36. Messnarz, R.; Macher, G.; Stolfa, J.; Stolfa, S. Highly Autonomous Vehicle (System) Design Patterns—Achieving Fail Operational and High Level of Safety and Security. In Proceedings of the Systems, Software and Services Process Improvement: 26th European Conference, EuroSPL, 18–20 September, 2019, Edinburgh, UK; Walker, A., O'Connor, R.V., Messnarz, R., Eds.; 2019; pp. 465–480.
37. Skoglund, M.; Warg, F.; Sangchoolie, B. In Search of Synergies in a Multi-concern Development Lifecycle: Safety and Cybersecurity. In Computer Safety, Reliability, and Security SAFECOMP 2018; Gallina, B., Skavhaug, A., Schoitsch, E., Bitsch, F., (eds); vol 11094, pp. 302–313, doi:10.1007/978-3-319-99229-7_26.
38. Edwards, J.; Kashani, A.; Iyer, G. Evaluation of Software Vulnerabilities in Vehicle Electronic Control Units, In Proceedings of the 2017 IEEE Cybersecurity Development Conference, Cambridge, UK, 24–26 September 2017; 2017; pp. 83–84.
39. Macher, G.; Messnarz, R.; Armengaud, E.; Riel, A.; Brenner, E.; Kreiner, C. Integrated Safety and Security Development in the Automotive Domain, SAE Technical Paper 2017-01-1661, 2017, doi:10.4271/2017-01-1661.
40. Macher, G.; Much, A.; Riel, A.; Messnarz, R.; Kreiner, C. Automotive SPICE, safety and cybersecurity integration. In Computer Safety, Reliability and Security, SAFECOMP 2017; Tonetta S.; Schoitsch E.; Bitsch F. (eds.); vol. 104489, pp. 273–285, doi:10.1007/978-3-319-66284-8_23.
41. Messnarz, R.; Much, A.; Kreiner, C.; Biro, M.; Gorner, J. Need for the Continuous Evolution of Systems Engineering Practices for Modern Vehicle Engineering. In Proceedings of the Systems Software and Services Process Improvement: 24th European Conference,; Stolfa, J., Stolfa, S., O'Connor, R., Messnarz, R., Eds.; 2017; pp. 439–452.
42. Macher, G.; Sporer, H.; Brenner, E.; Kreiner, C. Supporting Cyber-Security Based on Hardware-Software Interface Definition. In Proceedings of the Systems Software and Services Process Improvement: 23rd European Conference,; Kreiner, C., O'Connor, R., Poth, A., Messnarz, R., Eds.; 2016; pp. 148–159.
43. Nassi, B.; Nassi, D.; Ben-Netanel, R.; Mirsky, Y.; Drokin, O.; Elovivi, Y. Phantom of the ADAS: Phantom Attacks on Driver-Assistance Systems. IACR, 2020. Available online: <https://eprint.iacr.org/2020/085> (accessed on 30 May 2021).
44. ISO 15118, Road Vehicles—Vehicle to Grid Communication Interface. 2019. Available online: <https://www.iso.org/standard/69113.html> (accessed on 31 March 2021).