INCOSE

ASIA-OCEANIA SYSTEMS ENGINEERING CONFERENCE

Integrated Approach of ISO15288, 26262 and 21434 in Technical Processes

INCOSE AOSEC · 2025

AUTHORS

Takatsugu Adachi, Seiji Honda, Midori Daida, Takeshi Ejima, Akiyuki Takoshima, Akinori Kamiya, Ken Kawamura, Kao Ito, Takahiro Osada, Shota Matsumoto, and Seiichi Takahashi

PUBLICATION DATE

July, 2026

SUBMISSION #

26

INCOSE PUBLICATIONS

Integrated approach of ISO15288, 26262 and 21434 in technical processes

Takatsugu Adachi
Fujitsu Limited
Nagoya, Aichi, Japan
takatsuguadachi@fujitsu.com

Seiji Honda
Toyota Motor Corporation
Toyota, Aichi, Japan
seiji_honda_aa@mail.toyota.co.jp

Midori Daida
Change Vision, Inc.
Fukui, Japan
midori.daida@incose.net

Takeshi Ejima
Yamaha Motor Co., Ltd.
Shizuoka, Japan
ejimat@yamaha-motor.co.jp

Akiyuki Takoshima
Business Cube & Partners
Tokyo, Japan
takoshima@biz3.co.jp

Akinori Kamiya
Siemens
Yokohama, Kanagawa, Japan
akinori.kamiya@siemens.com

Ken Kawamura
Dassault Systèmes
Tokyo, Japan
ken.kawamura@3ds.com

Kao Ito
Nissan Motor Corporation
Kanagawa, Japan
kao_ito@mail.nissan.co.jp

Takahiro Osada
Fujitsu Limited
Kawasaki, Kanagawa, Japan
author.six@email.com

Shota Matsumoto
DENTSU SOKEN INC.
Toyota, Aichi, Japan
matsu-moto.shota@dentsusoken.com

Seiichi Takahashi
ST Research
Shizuoka, Japan
smtnr-t@ruby.plala.or.jp

Abstract

This paper proposes a process approach for the integrated application of three major ISO standards—ISO/IEC/IEEE 15288 (systems and software engineering), ISO 26262 (functional safety), and ISO/SAE 21434 (cybersecurity) across the entire system lifecycle to ensure safety and security in automotive system development. Specifically, based on the technical processes of ISO/IEC/IEEE 15288, the functional safety processes of ISO 26262 and the cybersecurity processes of ISO/SAE 21434 were systematically mapped to design an integrated process framework that eliminates duplication and inefficiency.

The proposed approach integrates the processes and deliverables of the three standards hierarchically, from the system context level down to subsystem and component levels. It derives safety and security goals and requirements through stakeholder requirements, functional definitions based on Nominal Scenarios, and risk analysis (HARA/TARA) for Off-Nominal Scenarios, thereby forming an integrated architecture. This systematic method aims to reduce development process duplication, shorten lead times, lower development costs, and improve product quality compared to conventional separate approaches.

Using an Electric Parking Brake (EPB) system as a concrete example, we conducted an investigated following the proposed integrated process. This demonstrated a design that integrates safety and security functions into the architecture, consider-

ing the EPB's main functions and external communication capabilities, achieving both reduced risk of unintended brake release and countermeasures against cyberattacks.

This approach contributes to establishing a development process that ensures high reliability and safety for increasingly complex vehicle systems. It does so by integrating functional requirements, safety and security measures previously considered separately based on systems engineering principles. This provides an effective means to build safe and secure vehicle systems while maintaining compliance with international standards.

Keywords

Automotive, Process Integration, Functional safety, Cybersecurity, Vee model

Introduction

The automotive industry is undergoing a major transformation due to advances in CASE (Connected, Autonomous, Shared, and Electric) technologies. As a result, vehicle systems are becoming increasingly complex and require rigorous engineering practices to ensure safety, security and reliability. Therefore, standards such as ISO/IEC/IEEE15288 (systems and software engineering), ISO26262 (functional safety) and ISO/SAE21434 (cybersecurity) have emerged as important frameworks. However, applying these standards individually can lead to duplication and inefficiencies throughout the development process, resulting in issues such as increased lead times, redundant documentation, prolonged development periods, and increased development effort. Existing studies have attempted to bridge ISO/IEC/IEEE15288 and automotive safety standards with Model-Based Systems Engineering (Nolte & Maurer, 2025) and to extract safety and security requirements simultaneously using SysML models (Nolte, Stein & Vietor, 2025). Nevertheless, many of these studies have focused on the alignment of specific phases and deliverables (Macher, Messnarz & Armengaud,2017), lacking a comprehensively integrated process structure across the life cycle and not showing specific examples of application of the approach.

In this paper, we propose an integrated approach that systematically maps ISO26262 and ISO/SAE21434 to the systems engineering process of ISO/IEC/IEEE15288 as an activity for providing value to users, which is the purpose of system development. Therefore, based on the principles of the system life cycle described in ISO/IEC/IEEE15288, we adopt a process approach for integration activities and deliverables across the entire set of technical processes and demonstrate the validity of this approach through a specific case.

Integration of ISO standards based on Vee model process Format

Details and features of the integrated approach:

In this paper, the technical process of ISO/IEC/IEEE15288 is adopted as the foundational framework to integrate the three ISO standards. This standard provides a high-level abstraction process of system design processes that encompasses the entire product development life cycle.

Within the framework of this process, functional safety from ISO26262 and cybersecurity from ISO/SAE21434 are incorporated into the technical process. Since both standards are essentially based on a systems engineering approach, it is reasonable to consider them as integrated processes based on ISO/IEC/IEEE 15288. Reference is made to the INCOSE Systems Engineering Handbook v5 to complement the foundational framework, and the overall map of the process organized in this paper is shown in Figure 1. Automotive-SPICE (Macher, Schmittner, Dobaj, Armengaud, & Messnarz, 2020) was considered in the drafting of Figure 1.

Figure 1 is structured into three levels: system context level, system/subsystem/component level, and hardware/software component level. At each level, the processes defined by ISO/IEC/IEEE 15288 — such as requirements definition, system analysis, architecture design, and verification — are shown in blue. On this foundation, the processes defined by ISO 26262 for functional safety

(green) and ISO/SAE 21434 for cybersecurity (purple) are mapped. For example, the system analysis process in ISO/IEC/IEEE 15288 significantly overlaps with the HARA process in ISO 26262 and the TARA process in ISO/SAE 21434. Integrating these processes reduces redundant work. Furthermore, the safety goals, security goals, requirements definition, design, and verification activities from each standard are hierarchically linked, ensuring consistency throughout the entire development process. When creating the diagram, practical application was considered and Automotive- SPICE was also referenced. Consequently, it is an integrated process map that considers not only theoretical integration but also applicability in development environments. This provides a framework that supports efficient automotive system development while achieving both safety and security.

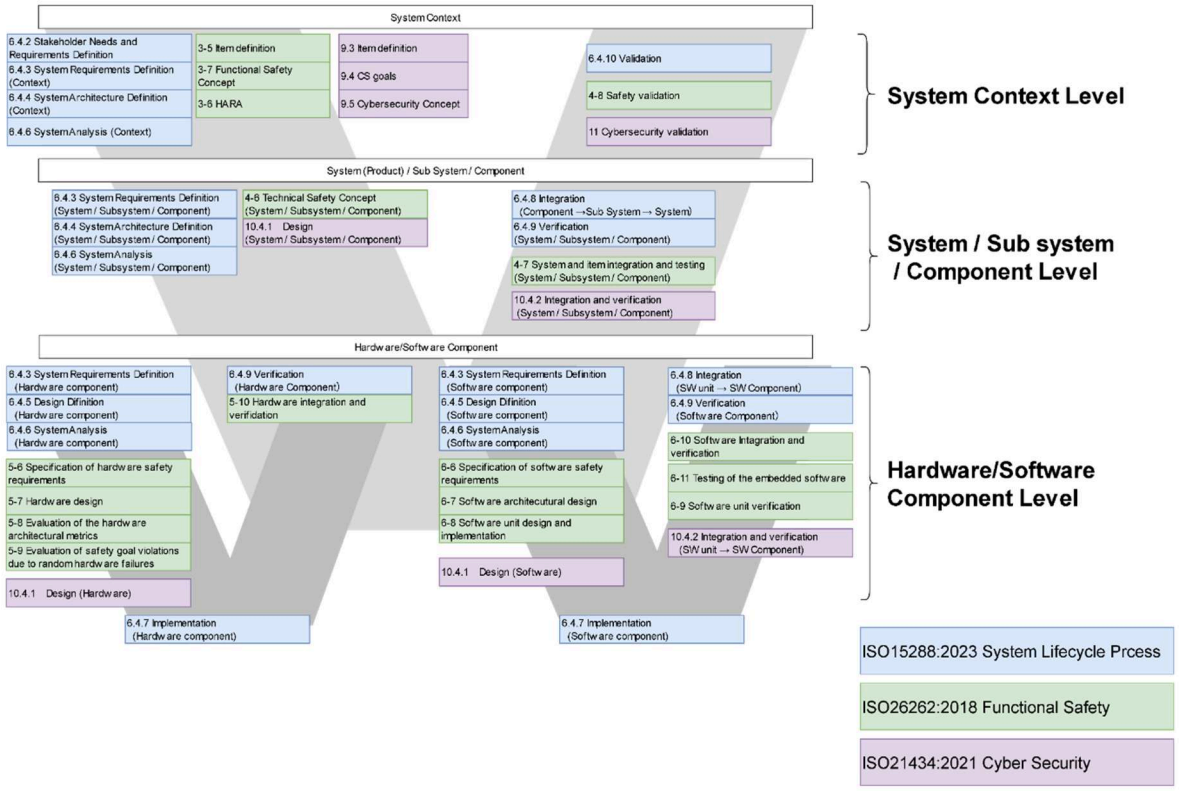

Figure 1. Overall Process Map

Basic Process (ISO/IEC/IEEE 15288).

This standard is an international standard for systems life cycle processes, provides best practices in systems engineering and defines development activities across all life cycle phases. This paper covers Section 6.4: Technical process.

Functional Safety (ISO26262).

These standard outlines safety management measures throughout the vehicle life cycle of an E/E system, defines safety goals and safety requirements at the system, hardware and software levels based on risks identified through hazard analysis and risk assessment (HARA), and details appropriate development processes, verification methods and evaluation criteria. This paper focuses on the analysis of the process defined in ISO26262 Clause 3, which aligns with the scope of the Technical Processes defined in ISO/IEC/IEEE 15288. By comparing the inputs and outputs of Clause3 with those of ISO/IEC/IEEE15288, it was clarified that the processes in Clause 3 of ISO26262 are included within ISO/IEC/IEEE15288. For example, the inputs and outputs of ISO 26262 Clause 3-5 are included in those of ISO/IEC/IEEE 15288 Section 6.4.4, system architecture definition process. Similarly, some of the processes of 3-6 Hazard analysis and risk assessment in ISO26262 were included in the inputs and outputs of the 6.4.6 systems analysis process in ISO/IEC/IEEE15288.

Cybersecurity (ISO/SAE21434).

Given the growing threat of cyber attacks in the automotive industry, this standard provides a framework for cybersecurity risk management across the entire vehicle life cycle, and defines and details the requirements, including policies, structures, responsibilities, and resource allocation, required for an organization's cybersecurity management. This paper focuses on the analysis of the process defined in Article 9 of ISO/SAE21434, which is in the same scope as the process defined in the Technical Process of ISO/IEC/IEEE15288. Comparing the inputs and outputs of Article 9 with those of ISO/IEC/IEEE15288, it was clarified that the processes contained in Article 9 of ISO/SAE21434 are contained in ISO/IEC/IEEE15288. For example, functions, internal operations, and cybersecurity requirements required for cybersecurity goals, which are the outputs of the 9-5 cybersecurity Concept in ISO/SAE21434, are included in the output of the 6.4.3 System Requirements Definition Process in ISO/IEC/IEEE15288. Similarly, the implementation of risk analysis and the determination of risk response options based on the item definition of Cybersecurity goals for items 9-4 in ISO/SAE21434 are considered to correspond to the 6.4.6 system analysis process in ISO/IEC/IEEE15288.

Proposed integrated approach

This paper describes the details and features of the integrated approach, which organizes the relationship between process and deliverables from the viewpoint of 3 standards, focusing on ISO/IEC/IEEE15288.

System Context Level.

Figure 2 shows the process at the system context level. Vehicle systems are defined through the stakeholder needs and requirements definition, system requirements definition, and architecture definition processes of ISO/IEC/IEEE15288. In product development, functions are initially defined based on nominal scenarios that address stakeholder needs. Among the functions or logical system elements defined in this context to realize these functions, those related to functional safety of electronic components and software can be defined as items in ISO26262, and those related to cybersecurity can be defined as items in ISO/SAE21434. (①).

Next, risk analysis for an unintended off-nominal scenario in the operational environment for the items defined here is conducted as part of the ISO/IEC/IEEE15288 6.4.6 System Analysis process. This corresponds to Hazard Analysis and Risk Assessment (HARA) for functional safety and Threat Analysis and Risk Assessment (TARA) for cybersecurity, resulting in the definition of safety goals and cybersecurity goals as stakeholder requirements. (②)

Through the system requirements definition process again to address the additional stakeholder requirements (Safety Goal/cybersecurity Goal), the functional safety requirements of 3-7.4. 2 of ISO26262 and the cybersecurity requirements of 9.5 of ISO/SAE21434 are defined as the vehicle-level system requirements of ISO/IEC/IEEE15288 (③). And the architecture definition processes of the three standards are integrated to define the vehicle-level architecture that satisfies the additional system requirements (functional safety and cybersecurity requirements). (④)

System/Subsystem/Component Level.

Figure 3 illustrates the process at the system, subsystem, and component levels. Similar to the system context level, system requirements for nominal scenarios are received, and functions of subsystems, components, or logical system elements are defined through the system requirements definition and architecture definition processes of ISO/IEC/IEEE 15288 (⑤). Risk analysis for the off-nominal scenarios is performed from both functional safety and cybersecurity viewpoints through the 6.4.6System Analysis process. The 4-6Technical Safety Concept for functional safety and the 10.4.1 design for cybersecurity standards correspond to the system requirements definition, architecture

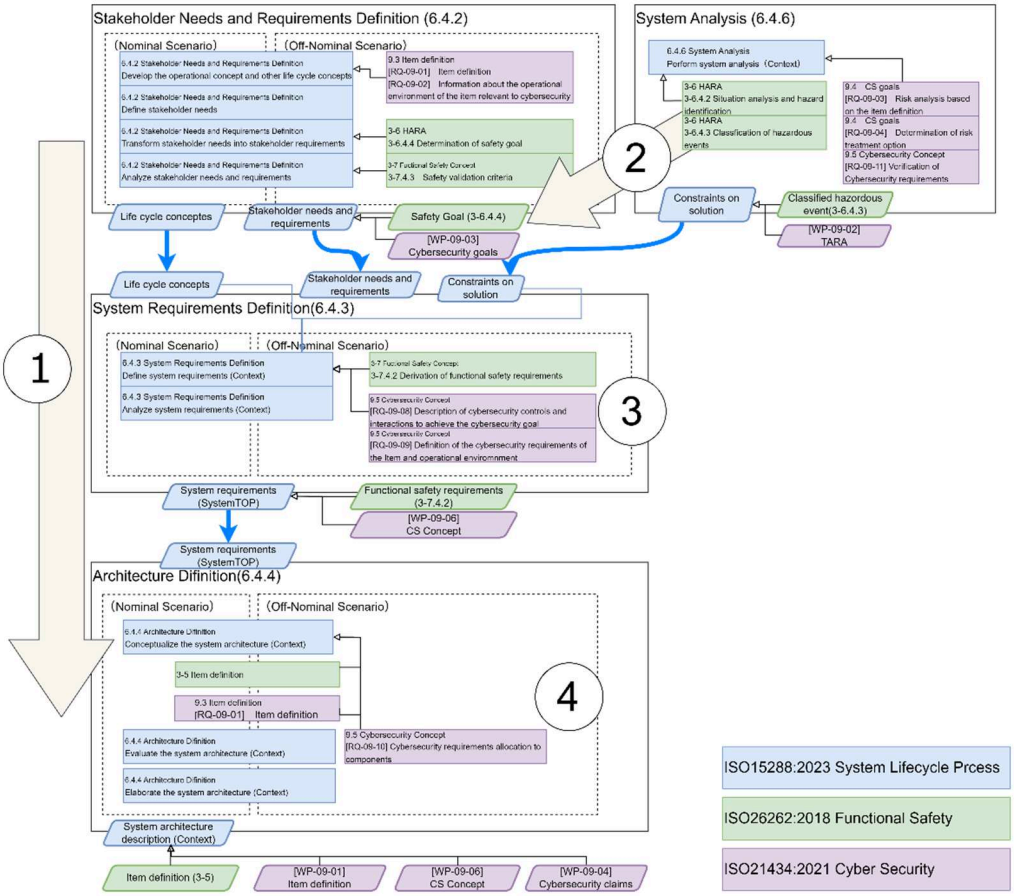

Figure 2. Correspondence Relationship of the Three Processes

- System Context Level

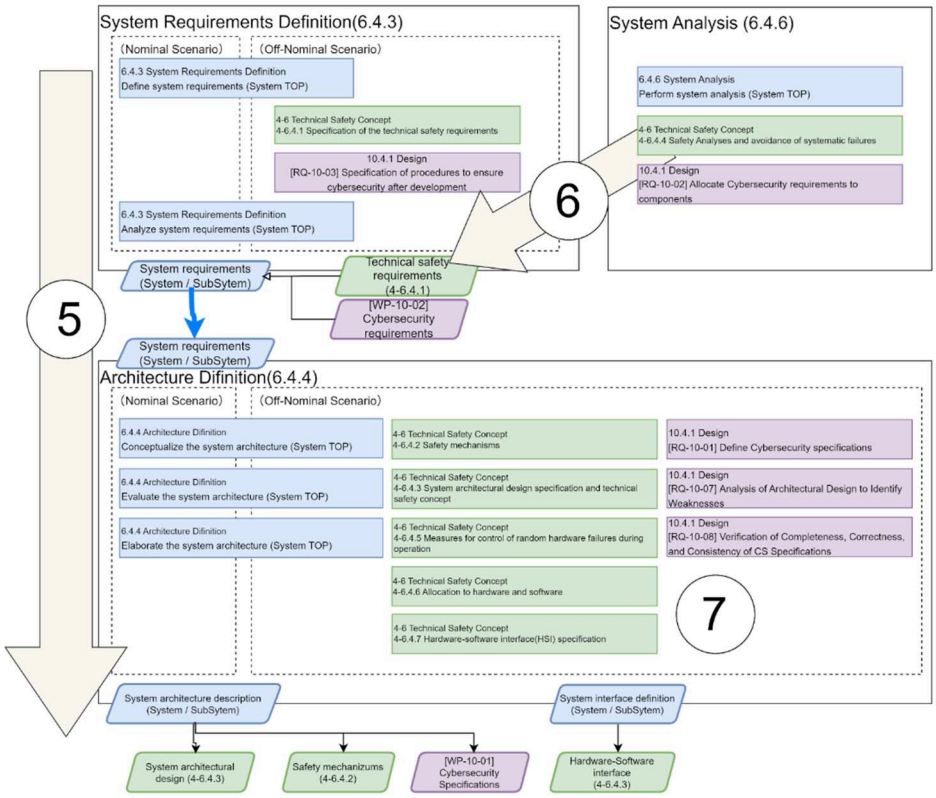

Figure 3. Correspondence Relationship of the Three Processes
- System/Sub system/Component Level

definition, and system analysis at the subsystem/component level. And the technical safety requirements for functional safety and the cybersecurity requirements for cybersecurity are defined as subsystem-level system requirements. (⑥).

The architecture definition processes of the three standards are integrated to define the subsystem-level architecture that satisfies these additional system requirements (Technical Safety Requirements/Cybersecurity Requirements). (⑦)

Based on the above, the technical advantages of this integrated approach include the ability to handle Nominal/Off-Nominal scenarios within a common analytical framework. This enables the extraction of functional safety (HARA) and cybersecurity (TARA) requirements through a single process, allowing for architecture design that comprehensively captures requirements. Consequently, design consistency and quality are enhanced.

Application of this approach

In this section, we examine the validity of our approach by using a typical EPB system as a case study. In this case, the EPB system electronically controls the parking brake of the vehicle, and the driver can hold or release the brake by, for example, pushing a button, removing the need to continuously depress the brake pedal, reducing the risk of the vehicle moving unintentionally, especially on a slope or at a traffic stop, thereby improving safety and convenience. When the driver turns on the EPB system, the control unit activates the electric motor based on various inputs and forces the brake caliper to press the brake pad against the brake disc to hold the vehicle stationary. When the driver depresses the accelerator pedal while the EPB is in operation, the stop holding state of the vehicle is released.

Basic architecture of the EPB system

This paper is an integrated approach covering ISO/IEC/IEEE15288 Section 6.4: Technical Processes and their corresponding ISO26262 and ISO/SAE21434, starting with defining the basic architecture of the EPB system through ISO/IEC/IEEE15288 Section 6.4: Technical Process Stakeholder Needs and Requirements Definition, System Requirements Definition, and Architecture Definition processes. Kono and Nishimura also refer to the integrated approach of basic architecture (ISO/IEC/IEEE15288) and functional safety (ISO26262) based on the EPB systems (Kono & Nishimura, 2021). In this paper, we will present specific examples that further include cybersecurity (ISO/SAE 21434). However, for the sections on basic architecture and functional safety, we will refer to the contents of the paper by Kono and Nishimura.

Based on the use cases and system requirements of the EPB system, Figure 4 shows the result of arranging the basic architecture of the EPB system from the viewpoint of static structure, and Figure 5 shows the intended flow of operation of each function from the viewpoint of behavior. In this case, Vehicle fixation system in Figure 4 (blue block in the figure) is the main function element of the EPB system and Generate brake torque of parking brake in Figure 5 is the main function derived from the system requirements, as indicated by the red blocks in the figure. There is also a Fixation release function and an Anti-sliding down function as secondary functions to the Vehicle fixation system and the FixSysIF function, which accepts actions at the timing intended by the driver. Furthermore, since the anti-sliding down function requires a driving force to move the vehicle, interaction with the Powertrain system is considered. In addition, other system is also arranged assuming that there is a system to monitor the fixed state of the vehicle and receive notification. In addition, although not directly derived from the system requirements, Telecommunication Equipment/Server, which interfaces with the vehicle as an external communication device (e.g., smartphone) or server (e.g., data center) as part of the external context, is added from the viewpoint of considering cybersecurity. These figures are modified from those of Kono and Nishimura.

In this case, the scope of the functional architecture shown in Figures 4 and 5 correspond to the item definition in ISO26262 Section 3-5.

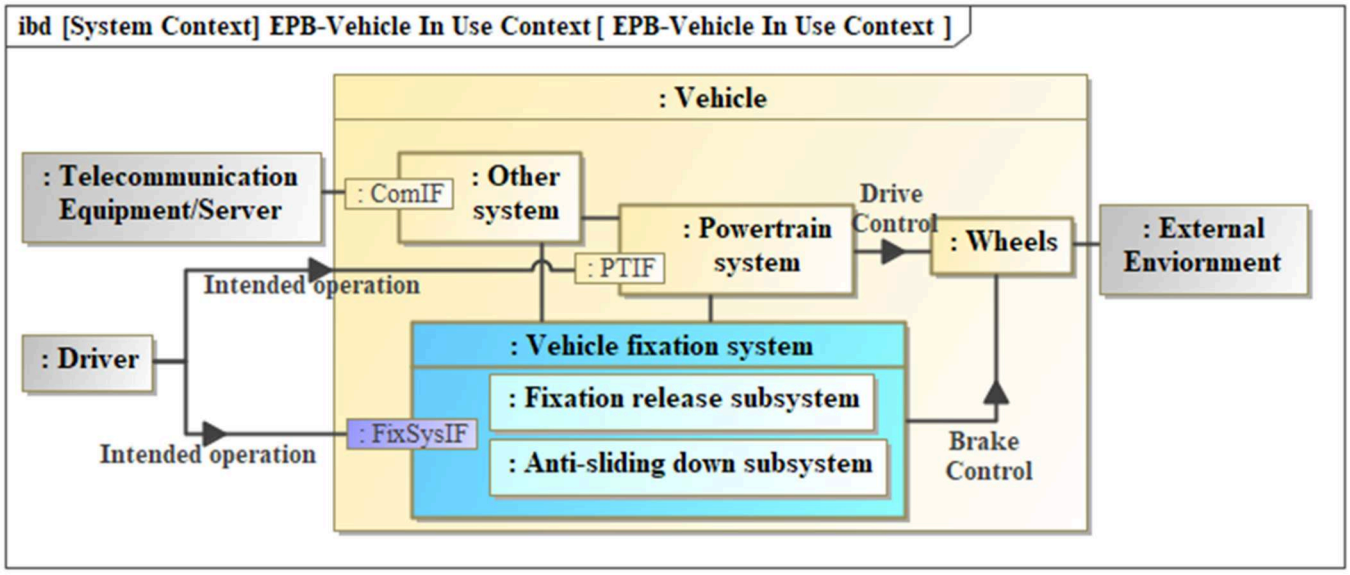

Figure 4. Basic Functional Architecture of the EPB System (Static Structure)

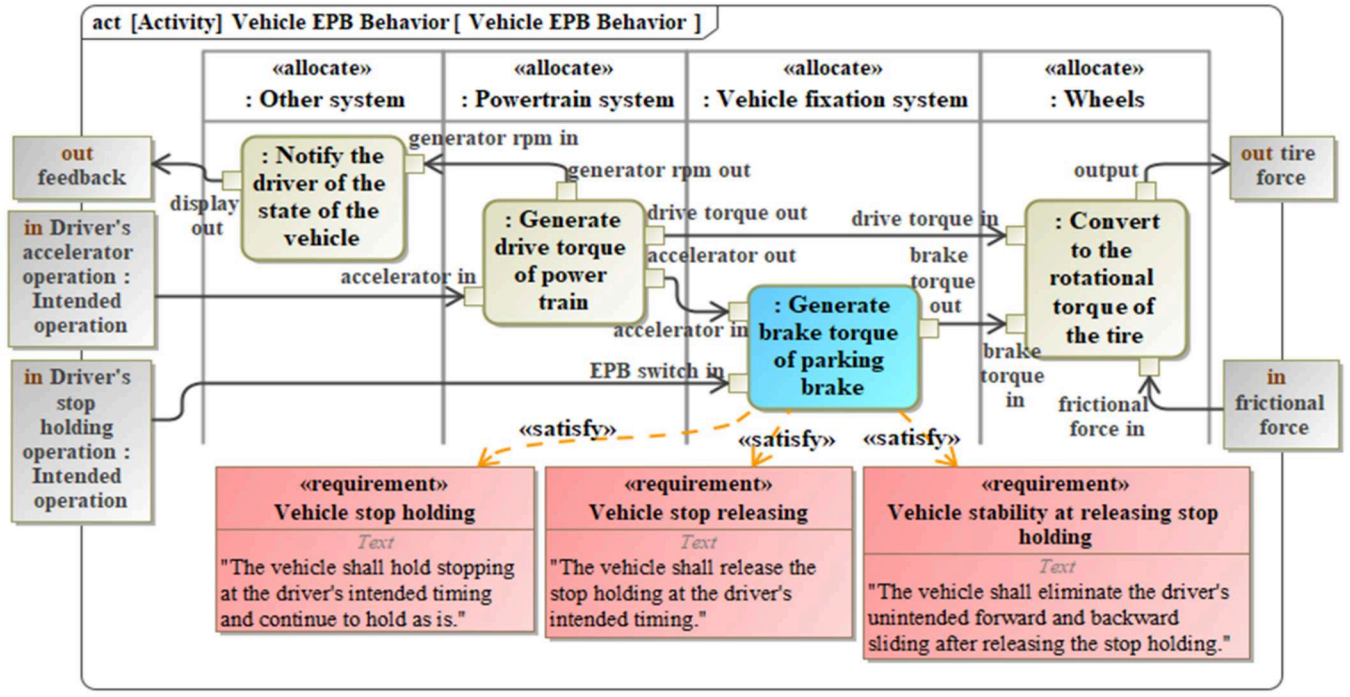

Figure 5. Basic Functional Architecture of the EPB System (Behavior)

Functional safety of the EPB system

Based on the aforementioned basic architecture with ISO/IEC/IEEE15288, functional safety analysis is conducted according to ISO26262. The functions already defined correspond to ISO26262: 3-5, and the function brake torque generation of parking brake is used as an example, referencing the hazard analysis by Kono and Nishimura. A scenario is considered in which the parking brake is released when the vehicle is attempting to accelerate with high drive torque. If the release operation of the parking brake is longer than expected due to a failure, the vehicle may suddenly start to move due to the high driving torque. And it causes a hazardous situation that such unintended sudden acceleration can cause collisions with other vehicles and persons/objects (corresponding to ISO26262: 3-6.4.2). The safety goal is then set to prevent unintended sudden acceleration (corresponding to ISO26262: 3-6.4. 4). To achieve the safety goal, the difference between the actual

driving torque and brake torque should be detected, and the functional safety requirements are derived to either advance the timing of brake release or limit the driving torque (corresponding to ISO26262: 3-7.4. 2). The safety mechanisms to satisfy the functional safety requirements are discussed in the later integrated architecture section.

Cybersecurity of the EPB System

Based on the aforementioned definition with ISO/IEC/IEEE15288 and ISO26262, the cybersecurity analysis is conducted according to ISO/SAE21434. The same scenario as the functional safety analysis is reused and analyzed from the cybersecurity perspective. As mentioned above, the vehicles interface with external communication devices and servers, which can expose them to threats. The assets involved as the Vehicle fixation system and Powertrain system are defined, and the damage scenarios are analyzed (corresponding to ISO/SAE21434: RQ-09-01). Threat scenarios include data falsification of the driver's intended operation through the communication interface and impersonation of control of the powertrain system through the communication interface. If there is a sudden loss of brake torque due to such a threat and high driving torque exists, as in the functional safety analysis results, there is a possibility of causing some kind of collision due to unintended sudden acceleration. To mitigate these risks, the cybersecurity goals are defined (corresponding to ISO/SAE21434: RQ- 09-03/04), and the functional cybersecurity requirements to detect input data tampering and control impersonation are derived (corresponding to ISO/SAE21434: RQ-09-08). The cybersecurity mechanisms to satisfy the functional cybersecurity requirements are also discussed in the later integrated architecture section.

Integrated Architecture of the EPB System

The architecture that integrates functional elements to meet functional safety and cybersecurity requirements is shown in Figure 6. A key feature of this diagram is the visual representation of how the various components within the EPB system collaborate to fulfill both functional safety and cybersecurity requirements.

Specifically, the risk of unintended acceleration under high levels of drive torque and prolonged parking brake release due to a failure is identified from a functional safety perspective, and the functional safety requirements for detecting the difference between drive torque and brake torque and implementing feedback control are shown in green blocks. This function is placed on the Vehicle fixation system to monitor and control the vehicle's fixed state during brake release. In addition, cybersecurity requirements to prevent data tampering and falsification are shown in purple blocks, and this feature is located close to the input of the powertrain system and the Vehicle fixation system to ensure early detection of external tampered data and commands and make the system more secure. By considering functional safety and cybersecurity requirements within the same structural framework based on the basic architecture, it is possible to reduce redundancy in separate processes and improve the efficiency of the development process. Traditionally, the definition of functional requirements and the implementation of safety and security measures have been pursued separately, posing challenges to achieving optimal system configurations. This approach ensures the safety and security of increasingly complex vehicle systems, while simultaneously reducing development costs, improving product quality, and enhancing compliance with standards. In other words, it enables the improvement of development process efficiency.

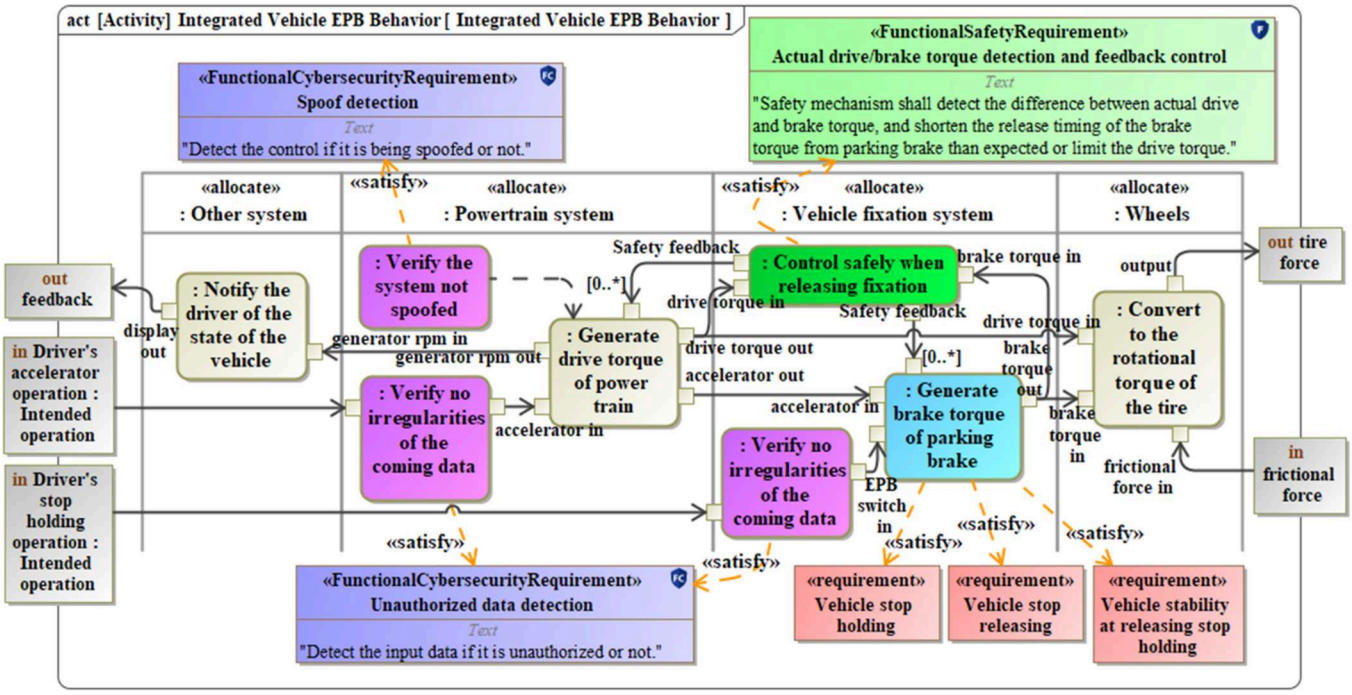

Figure 6. Integrated Functional Architecture of the EPB System

Conclusion

The proposed integrated approach enables consistent consideration of the system by overlaying functional safety and cybersecurity onto the basic architecture. It provides an effective method for designing systems that operate safely and securely and offers a process for achieving high reliability and safety in increasingly complex vehicle systems.

However, the current study primarily focuses on static architecture structure diagrams and does not fully address functional extraction based on use cases or dynamic state transitions of the system as described in ISO/IEC/IEEE15288. Future work should integrate these perspectives into functional safety and cybersecurity studies. To avoid redundant efforts, further advancement of integration approaches is necessary.

Furthermore, we are considering integrating the fourth standard, ISO 21448: Safety of The Intended Functionality (SOTIF), into this approach, using Advanced Driver Assistance Systems (ADAS) as a case study.

References

ISO. (2023). ISO/IEC/IEEE 15288:2023, Systems and software engineering — System life cycle processes. International Organization for Standardization.

ISO. (2018). ISO 26262:2018, Road vehicles — Functional safety. International Organization for Standardization.

ISO. (2021). ISO/SAE 21434:2021, Road vehicles — Cybersecurity engineering. International Organization for Standardization.

ISO. (2022). ISO 21448:2022, Road vehicles — Safety of the intended functionality. International Organization for Standardization.

Macher, G., Messnarz, R., Armengaud, E., & others. (2017). Integrated Safety and Security Development in the Automotive Domain. SAE Technical Paper 2017-01-1661. SAE International.

Nolte, M., & Maurer, M. (2025). Towards Closing the Gap between Model-Based Systems Engineering and Automated Vehicle Assurance: Tailoring Generic Methods by Integrating Domain Knowledge. arXiv preprint arXiv:2502.06627

Nolte, B., Stein, A., & Vietor, T. (2025). Designing a Method for Identifying Functional Safety and Cybersecurity Requirements

Utilizing Model-Based Systems Engineering. Applied Systems Innovation, 8(2), 45
VDA/QMC. (2023). Automotive SPICE® process assessment model
Macher, G., Schmittner, C., Dobaj, J., Armengaud, E., & Messnarz, R. (2020). An Integrated View on Automotive SPICE, Functional Safety and Cyber-Security. SAE Technical Paper 2020-01-0145. SAE International
INCOSE. (2023). Systems Engineering Handbook: A Guide for System Life Cycle Process and Activities. Fifth Edition.
Kono, F., & Nishimura, H. (2021). Proposal of a Safety Analysis Approach Based on Interaction of Behavior Models for Automobile Onboard Products — A Case Study of Safety Analysis of Electric Parking Brake Systems. Proceedings of the Society of Automotive Engineers, 52(2), March.

Biography

Takatsugu Adachi

JCOSE Automotive Working Group, SubWG-3 Leader

After 20 years in aircraft development at a Japanese heavy industry manufacturer, he joined Fujitsu Limited in 2024 to drive MBSE, DX and AI

Seiji Honda

Co-chair of JCOSE Automotive working group from 2024 to present, and MBSE Deployment Group Manager in Toyota Motor Corp. in Japan. Certified: INCOSE CSEP

Midori Daida

Software engineer at Change Vision, Inc. in Japan, engaged in improving the quality of requirements for automotive embedded systems.

Takeshi Ejima

Leader in the promotion and implementation of the MBSE approach at Yamaha Motor Co., Ltd. since 2019.

Akiyuki Takoshima

Automotive SPICE competent assessor at Business Cube & Partners, Inc.

Akinori Kamiya

Country Portfolio Development Executive at Siemens K.K.

Ken Kawamura

CATIA Cyber Systems Industry Process Expert Specialist under Global/Asia team in Dassault Systèmes. Certified: INCOSE ASEP, OMG SysML (OCSMP-MBF), UAF (UAF-MU), and Ph.D.

Kao Ito

Kao Ito is a leader in Systems Engineering in Nissan ADAS development group since 2022.

Takahiro Osada

Since 2022, Engaged in the deployment of software security diagnostic services at Fujitsu Limited. Currently, he develops AI applications for MBSE.

Shota Matsumoto

Member promoting systems engineering in the automotive domain at DENTSU SOKEN INC. in Japan.

Seiichi Takahashi

Automotive Electronics Control System Development, Technical Consultant, ST Research.