Development of Harmony-SE Internalization Methodology for Automobile Functional Safety and Cyber Security Process

ISO 26262, ISO/SAE 21434, and Harmony-SE Integration Process Model

Xuezhu Yang[1, a], Muxi Li[1, b], Yi Liu[1, c*], Chengrui Sun[1, d], Miao Wu[1, e], Shiying Zhou[2, f]

[1]E&E Research Department of Intelligent Connected Vehicle Development Institute, FAW, China
[2]General Research and Development Institute, FAW, China

[a]yangxuezhu@faw.com.cn
[b]limuxi@faw.com.cn
[c]liuyi7@faw.com.cn
[d]sunchengrui@faw.com.cn
[e]wumiao@faw.com.cn
[f]zhoushiying@faw.com.cn

Abstract. ISO 26262, a standard for automobile safety, is a safety standard established by ISO to prevent accidents caused by errors in the E/E (Electric and Electronic) system mounted on vehicles. Recently, as the internet connectivity of automobiles increases, the standard methodology for securing security of the development stage is being presented as the cases of automobile hacking increase. Automobile cyber security has established and introduced ISO/SAE 21434 standard to eliminate threats caused by artificial penetration of hackers existing outside. The basic functional safety and cyber security standards should be reflected to improve the reliability of the E/E system of automobiles which is being developed as autonomous vehicles. In particular, systems engineering standards should be applied in consideration of requirements and constraints such as goals and system operation concepts of stakeholders, problem identification and definition, and solutions from the beginning of development to manage the development life cycle. In this paper, we propose a process integration development methodology based on the correlation analysis of the Harmony-SE model for the Harmonization Internationalization of automobile function safety, cyber security, and systems engineering.

Keywords: Automotive Functional Safety, Cyber Security, Systems Engineering, Harmonization International Method, Integration Development Process, Harmony-SE

H. Wu et al. (Eds.): CSIEDE 2022, ACSR 103, pp. 48–57, 2022.
https://doi.org/10.2991/978-94-6463-108-1_7

1 Introduction

Today, the digital new deal technology, which is converging in the automobile industry, is inducing the conversion of autonomous driving and connected cars that are fused with various technologies such as engines and mission technologies. To achieve this, it is necessary to develop a Harmonization Internationalization Methodology of Functional Safety, Cyber Security, and Systems Engineering, which are divided into development paradigms to secure the safety of E/E systems installed in vehicles [1]. Therefore, in this paper, we develop a design methodology to secure the reliability of the system level and safety of semiconductors, SWs, AIs, and multi-sensors such as radar, lidar, and camera mounted on autonomous vehicles. In addition, we propose a process development methodology that combines ISO 26262, ISO/SAE 21434, Systems Engineering standards, and an integrated model that connects to Harmony-SE.

2 ISO 26262, ISO/SAE 21434 and Systems engineering concept, harmonization and interrelationship

For the safety development of vehicles, the accuracy of determining whether the products operate exactly as designed and the safety of the functions that determine whether the errors generated inside the products can be exposed to the outside and harm the users should be considered [2]. In order to prevent the security threat threatened by the development of vehicle communication from expanding into the system, it is necessary to implement the security internalization technology that implements the product considering the elements such as accuracy, safety, and security of the product from the beginning of development [3]. All processes require the actions required in the conceptual design, development, production, operation, support, and disposal stages from a life cycle perspective and systems engineering techniques in which the output is defined [4].

2.1 ISO 26262, Functional Safety

ISO 26262 was applied as a necessary standard related to the development of automobile safety to minimize accidents and deaths caused by functional malfunctions of the ECU (Electronic Control Unit) [5]. ISO 26262 is standardized to tailor each step requirement through the configuration of a system engineering-based safety life cycle in which a series of activities of the development, management, production, operation, service, and disposal stages of the vehicle are defined [6]. This standard is designed to specify development requirements related to the determination of the level of safety integrity required at the system level, sub-hardware, and software level in the development process stage. It also works with the system engineering process to verify the feasibility of the safety level of the target being achieved and to provide solutions accordingly.

2.2 ISO/SAE 21434, Cyber Security

ISO/SAE 21434 recommends that processes that define the concept design, development, production, operation, and disposal stages, which are the life cycles of automobiles, be integrated with existing functional safety processes and system engineering processes. It included activities related to distributed development such as manufacturers and suppliers by classifying them into continuous cyber security activities including analysis and management of vulnerabilities such as cyber security monitoring and event reporting that were dealt with in production and operation after development [7]. Since safety goal and ASIL in ISO 26262 are applied to the activities to establish security goal of ISO/SAE 2143, risk analysis and risk assessment techniques, HARA (Hazard Analysis and Risk Assessment), threat analysis and risk assessment techniques, TARA (Threat Analysis and Risk Assessment) that the action must be carried out [8].

2.3 Systems Engineering

Systems engineering activities are defined as the process of sharing requirements, recommendations, and pharmaceutical terms and reaching agreements for complex systems to provide goals and system operation concepts of stakeholders, identification and definition of problems, and solutions throughout the life cycle of the initial target system [9]. Figure 1 shows the Vee-model and overall life cycle presented by systems engineering. In the system development stage, the activity to include the system, product, subsystem, assembly, and part level for SE design for attributes or shape items is defined. Systems engineering-based life cycles, which are also applied to functional safety and cyber security standards, start with basic conceptual design based on standards. In order to identify stakeholders' requirements and to propose viable solutions, such as exploring concepts, we define the concept of integrated operations, scenarios, architectures, and basic test cases, and link the process of specifying the necessary output [10]. In addition, requirements and system architecture development are performed for system modeling, which is determined by risk management and reliability-based engineering activities.

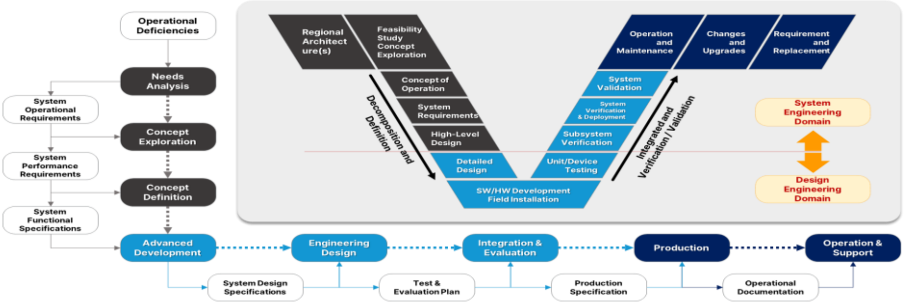
Operational Deficiencies
Needs Analysis
System Operational Requirements
Concept Exploration
System Performance Requirements
Concept Definition
System Functional Specifications
Regional Architect ure(s)
Feasibility Study Concept Exploration
Concept of Operation
System Requirements
High-Level Design
Detailed Design
SW/HW Development Field Installation
Decomposition and Definition
Unit/Device Testing
Subsystem Verification
System Verification & Deployment
System Validation
Integrated and Verification / Validation
Operation and Maintenance
Changes and Upgrades
Requirement and Replacement
System Engineering Domain
Design Engineering Domain
Advanced Development
Engineering Design
Integration & Evaluation
Production
Operation & Support
System Design Specifications
Test & Evaluation Plan
Production Specification
Operational Documentation

Fig. 1. Systems Engineering Lifecycle Process

3 Harmonization Internalization Methodology for Automobile Functional Safety and Cyber Security Process

The integrated methodology for the safety development of vehicles should be considered from the beginning of development such as accuracy, safety, and security of products. Based on this, the combination element of the functional safety element that is linked to the security internalization technology implementing the product and the safety analysis activity of each step of the systems engineering process is constituted. Previous studies suggest an integrated approach to ISO 26262 and SOTIF requirements based on the ISO 26262 life cycle [11]. As the era of self-driving cars arrived, the need to apply cybersecurity along with functional safety emerged as the increase in automobile connectivity. This is applied to the process integration, which is the main methodology of the harmonic internalization of the vehicle and to apply the safety analysis technique for analyzing the cause of the risk events that can occur in the internal and external systems.

3.1 Development of Process Integration

For process integration, systems engineering activities and core activities of ISO 26262, ISO/SAE 21434, as shown in Figure 2, are linked to development stages. In the product concept stage, the conceptual design activities required by each standard are defined and the overall development range is identified. In the risk assessment stage, the initial safety design elements are identified by linking HARA and TARA activities, and safety and security requirements are derived and allocated. Each standard integrated life cycle model systematizes step-by-step activities for IBM harmony-SE Vee-model based modeling. Step-by-step procedures and activities were specified in Table 1.

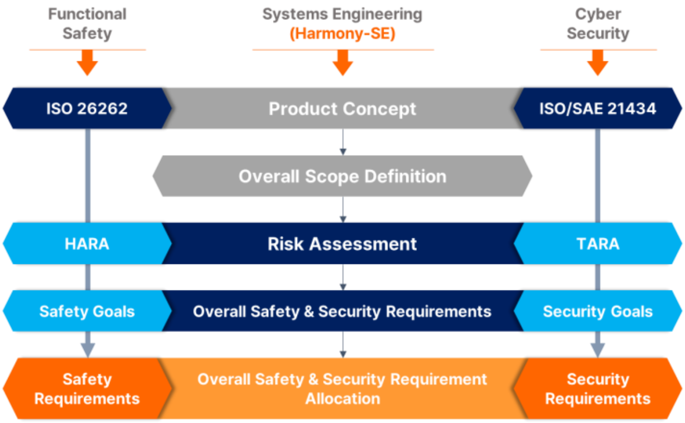

Fig. 2. Implementing the Safety and Security Process

Table 1. Harmony-SE based Procedure and activities

Step	**Description**	
	Procedure Activities	***Expected Output***
Product Concept	The Operation Concept is Drawn based on the Stakeholder Needs related to the Development Object System	Concept Proposal Needs Analytics Operational Concept Report
Overall Scope Definition	The Operating Function and the Expected Specification Definition are Proceed.	Operational Scenario and Specification
Risk Assessment	The Process of the ASIL Crystallization for the Safety and Security Goal Derivation is Proceed	Hazard and Threat Analytics HARA Report TARA Report
Overall Safety & Security Requirements	Function and the Non-functional Requirement Coincided with for Safety and Security Goal are Distinguished	Safety Req. Security Req.
Overall Safety & Security Requirement Allocation	Safety and Security Requirements are Assigned to Harmony-SE Process Step-by-Step Activities The Safety Integrity Requirement about Each Safety Function Allocated to the Safety Related System is stated as the Safety Integrity Level	Safety Integrity Level

3.2 Analysis of Standard's Correlation

To evaluate the risk of the integrated vehicle development process, the cause of the risk events that may occur in internal systems and external factors is derived and the analysis results are analyzed on the areas covered by the standard. The analysis and correlation of the causes of the risk events by standard are followed by Table 2. Since there is a difference in the range of interpretation between standards for core risk events, for the clear analysis of the case, items related to the analysis and evaluation of the risk source of each standard must be followed. Risk events that occur in vehicle development should be applied to the risk analysis and evaluation process presented in ISO 26262 and systems engineering standards due to the failure of the vehicle ECU, misperception of performance and function, problems of use, and system failure. Other risk incidents caused by external factors should be carried out in safety activities required by ISO 26262 and ISO/SAE 21434 due to security vulnerabilities, communication interference, and environmental impacts.

Table 2. Overview of safety relevant root cause

Source	**Hazard Event**	
	Risk Root Cause	***Standards Mapping***
Inner System	Failure of Electrical/Electronic Systems	ISO 26262
	Limits in Performance Misidentified Situational Awareness Misuse are not Predicted	Systems Engineering
	Inaccurate HMI(Human Machine Interface) Incorrect Use	ISO 26262
	The Cause of Failure by System Technology	Systems Engineering
External Factor	Vehicle Vulnerability Attack	ISO/SAE 21434
	The Effect of Internal/External Communication	ISO 26262
	The Effect of Vehicle/ Environmental Environment	ISO 26262

3.3 Integration of Risk Analysis and Assessment Activities

For the safety design of vehicles, it is necessary to meet the ASIL given to safety goals other than the development process required by the international safety standards. In the process of meeting ASIL, risk assessment for the development of risk prevention measures is carried out, and safety-related requirements are identification and allocation activities are included. To apply safety-related requirements, we use the analysis techniques performed in ISO 26262 and ISO/SAE 21434, which are linked to risk assessment activities in the systems engineering process stage. In order to secure functional safety, HARA technique is applied to ISO 26262 where analysis and evaluation are performed based on risk sources. In ISO/SAE 2143, security enhancement method is secured through TARA technique in which analysis and evaluation are performed based on threat factors.

The differences between techniques are as follows.

1. HARA (Hazard Analysis and Risk Assessment)

   a) It is an analysis evaluation method for the safety goal derivation.

b) Safety goal is established to prevent the risk of a vehicle level, and hazard is defined as "Potential source harm caused by malfunctioning behavior of the item" which is ISO 26262 Part 1.57.

c) In order to identify hazard, HARA is performed according to Part 3.7 in ISO 26262, and finally ASIL is determined through the Severity, exposure and controlability of each malfunctioning behavior and hazard.

2. TARA (Threat Analysis and Risk Assessment)

a) It is an analysis evaluation method for the security goal derivation.

b) Intended failure through cyber attack must be identified through TARA, as the intended attack by an attacker causes malfunctions of the intended function that the vehicle must perform.

c) Attack tree analysis (ATA), which defines the goal that an attacker intends to achieve as attack goal, is performed to determine the risk by applying criteria such as attack method and asset attacks.

d) When attack tree (AT) is completed, attack path (Attack Path) is identified, such as cut-set analysis of FTA, and the risk level of all attack paths is evaluated based on the identified attack path.

e) All attack paths must be designed to be mapped with the risks identified in the HARA.

According to the results of the risk assessment process of the vehicle, when establishing the cyber security requirement specified in ISO 26262 Part 4, it is necessary to derive software defense measures in the form of requirement to cope with malicious attacks. Therefore, validated security coding standards such as CERT C and MISRA C Secure are applied and verified.

3.4 System Development Lifecycle's Harmony-SE Model

To implement the integrated methodology for the safety development of vehicles, a standard life cycle model combining security internalization technology, systems engineering, and functional safety activities should be presented. The basic life cycle model can be designed as a harmony-SE vee-model with requirements and architecture design and integrated verification and confirmation process based on three-step modeling of concept, development and production. The entire process is based on systems engineering activities and can be standardized as a model in which core activities of each standard are mapped for security internalization. The integrated development model mapped based on ISO/SAE 21434 is a harmony-SE vee-model and can be designed as shown in Figure 3.

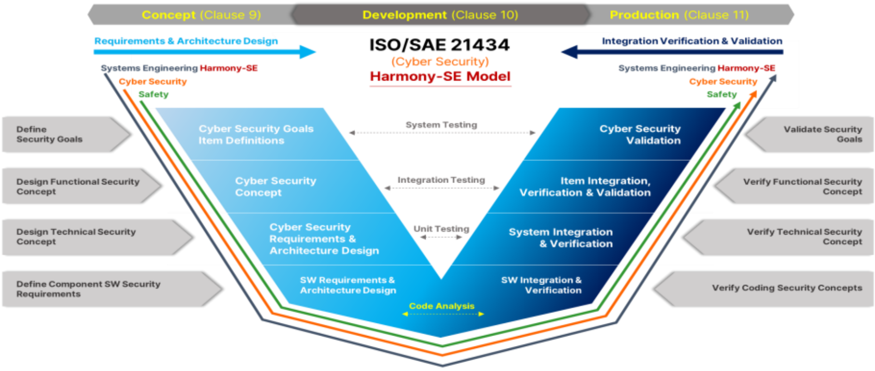
Concept (Clause 9)
Development (Clause 10)
Production (Clause 11)
Requirements & Architecture Design
ISO/SAE 21434
(Cyber Security)
Harmony-SE Model
Integration Verification & Validation
Systems Engineering Harmony-SE
Cyber Security
Safety
Systems Engineering Harmony-SE
Cyber Security
Safety
Define Security Goals
Design Functional Security Concept
Design Technical Security Concept
Define Component SW Security Requirements
Cyber Security Goals Item Definitions
Cyber Security Concept
Cyber Security Requirements & Architecture Design
SW Requirements & Architecture Design
System Testing
Integration Testing
Unit Testing
Code Analysis
Cyber Security Validation
Item Integration, Verification & Validation
System Integration & Verification
SW Integration & Verification
Validate Security Goals
Verify Functional Security Concept
Verify Technical Security Concept
Verify Coding Security Concepts

Fig. 3. Harmony-SE Lifecycle Model

The proposed integrated development methodology can be verified during the development process through checklist verification. Table 3 shows an example of a checklist that needs to be verified in the performance of integrated development.

Table 3. Check-list for harmonization model

Requirements	Evaluation target	Checklist	Results
Establish a plan for functional safety activities	Functional Safety	1) Ensure all functional safety activities are planned 2) Confirmation of detailed information on each functional safety activity	OK
HW/SW development process is defined	Safety Plan	1) Check the hardware development process 2) Check the software development process	OK
SW modification and change using Debug Tool	Cyber Security	1) Check to use a licensed debug tool 2) Confirm that MAC address is applied	NG
Reprogramming requested from outside	Cyber Security	Confirm use of public key provided by OEM	OK

4 Conclusion

The automobile industry is advancing driving technology developed with technologies such as environmental recognition, location recognition, mapping, judgment, and control for autonomous driving and conversion to connected cars. In addition, autonomous vehicles are equipped with technology and passengers, and V2X (Vehicle to Everything) communication technology for acquiring and exchanging surrounding information related to driving. The next generation vehicles with various application technologies are required to advance the development system considering the compliance with basic design principles, functional safety and security. To this end, the systems engineering standard and the function safety standard should be reflected to improve the reliability of the E/E system of the vehicle developed as an autonomous vehicle.

In order to comply with design and safety standards, from the beginning of development, requirements and constraints such as goals and system operation concepts of stakeholders, problem identification and definition, and solutions should be considered for safety life cycle management. The designed harmony-SE vee-model and integrated development methodology can be applied as basic resources for risk analysis and evaluation that can occur in various device interfaces mounted on the vehicle and can be mapped with activities to prepare safety measures. Based on the results presented in this paper, it is expected to help improve the reliability and safety system of vehicle manufacturers and suppliers.

References

1. Young, William, and Nancy G. Leveson. “An integrated approach to safety and security based on systems theory,” Communications of the ACM, Vol.57, No.2, pp.31-35, 2014.
2. Mathias Dehm, Markus Tschersich, “Road Vehicles' Life-Cycle: Mapping of relevant standards and regulations for automotive cybersecurity,” in ESCAR Europe, 2019.
3. H. Khattri, N. K. V. Mangipudi, and S. Mandujano, “Hsdl: A security development lifecycle for hardware technologies,” 2012 IEEE International Symposium on Hardware-Oriented Security and Trust, pp.116-121, 2012.
4. S. Khou, L. O. Mailloux, J. M. Pecarina, and M. Mcevilley, “A customizable framework for prioritizing systems security engineering processes, activities, and tasks,” IEEE Access, Vol.5, pp.12878-12894, 2017.
5. R. Debouk, “Overview of the 2nd Edition of ISO 26262: Functional safety–road vehicles,” General Motors Company, Warren, MI, USA, 2018.
6. Mathias Dehm, Markus Tschersich, “Road Vehicles' Life-Cycle: Mapping of relevant standards and regulations for automotive cybersecurity,” in ESCAR Europe, 2019.
7. S. Khou, L. O. Mailloux, J. M. Pecarina, and M. Mcevilley, “A customizable framework for prioritizing systems security engineering processes, activities, and tasks,” IEEE Access, Vol.5, pp.12878-12894, 2017.
8. N. M. Mohammed, M. Niazi, M. Alshayeb, and S. Mahmood, “Exploring software security approaches in software development lifecycle: A systematic mapping study,” Computer Standards & Interfaces, Vol.50, pp.107-115, 2017.
9. James A. Crowder, Curtis W. Hoff, James A. Crowder, Curtis W. Hoff, Model-Based Systems Engineering, Requirements Engineering: Laying a Firm Foundation, 10.1007/978-3-030-91077-8, pp.197-216, 2022.
10. V. Casola, A. De Benedictis, M. Rak, and U. Villano, “A novel Security-by-Design methodology: Modeling and assessing security by SLAs with a quantitative approach,” Jounal of Systems and Software, Vol.163, 110537, 2020.
11. Kirovskii, O. M., & Gorelov, V. A. “Driver assistance systems: analysis, tests and the safety case.” ISO 26262 and ISO PAS 21448. In IOP Conference Series: Materials Science and Engineering, Vol. 534, No. 1, pp. 012019, 2019.