

Identification of Interface Related Factors Between Safety Management System and Cybersecurity Management System for Highly Automated Driving Vehicles

Marzana Khatun¹^a, Florence Wagner², Rolf Jung² and Michael Glaß³^b

¹Kempton University of Applied Sciences Kempton, Bavaria, Germany

²IFM- Institute for Advances Driver Assistance Systems and Connected Mobility, Benningen, Bavaria, Germany

³University of Ulm, Ulm, Baden Wurttemberg, Germany

Keywords: SMS, CSMS, HAD FuSa, Cybersecurity.


Abstract: Functional safety and cybersecurity are essential parts of the development of automated vehicles to ensure vehicle safety. Highly automated driving (HAD) vehicles require safe and secure development and communication processes that have to be monitored, maintained and improved through management processes. Hence, interface management systems are required to confirm HAD vehicle safety. The acceptance level of the interface between functional safety and cybersecurity in management systems is crucial for the development of Highly Automated Driving (HAD) vehicles. The Safety Management System (SMS) needs to consider the aspect of cybersecurity to ensure the overall safety of the vehicles or vice-versa. However, the interface methods of SMS and Cybersecurity Management System (CSMS) is challenging given the complexity of the system development and constraints from the company culture. The objective of this study is to present an interface approach in between management systems with a set of interface specifications including communication adaption processes. The main contributions of the paper are, (i) Illustrating the interface areas of the SMS and CSMS by identifying the management factors, (ii) Presenting the degree of influence of the management factors based on the survey results, and (iii) Providing a support to deal with SMS and CSMS interface for HAD vehicle development. A list of interface-related management factors is presented in this paper based on the literature study and findings from other disciplines. Additionally, the degree of influence of the management factors is presented as a result of this research based on the survey results from functional safety and cybersecurity experts.


1 INTRODUCTION

The potential impact of cyberattacks on the functionally safe system needs to be analyzed and considered at the management level. The interface of a Safety Management System (SMS) and Cybersecurity Management System (CSMS) is required to identify critical issues, raise awareness, and pinpoint the importance of both Functional Safety (FuSa) and cybersecurity for Highly Automated Driving (HAD) vehicle development. SAE (Shuttleworth, 2019) and (SAE J3016, 2021) level 3 to higher automation levels is treated as HAD vehicles where the driver is still needed as a fallback strategy but HAD vehicle may be able to drive by

itself for an extended period. HAD vehicles focus on both the functionalities of the systems and the protection of the vehicle components or set of components. Ensuring FuSa (ISO 26262, 2018) and cybersecurity of such vehicles become a necessity because of the involvement of safety-critical systems with cyber-physical systems or vice-versa. The management processes have to be acceptable for FuSa-related activities and cybersecurity-related activities. However, management systems deal with other organizational structures, rules, and methods or encompass other management systems.

While conventional certification process is applicable for safety and cybersecurity are independently applicable for level 2 vehicle, HAD

^a <https://orcid.org/0000-0002-3839-1575>

^b <https://orcid.org/0000-0003-3522-1519>

vehicle certification for on-road driving is still in its infancy. HAD vehicle development activities potentially involve new technologies or approaches for performing dynamic driving tasks and decision-making strategies. Therefore, the introduction of new methods in the management system that support interface aspects is essential and an interesting topic for research. A set of SMS and CSMS interface specification is a prerequisite to deal with the new technology and complex systems applied in HAD vehicles. Therefore, to reduce the complexity of development, a systematic approach of management systems interface is in demand for HAD vehicles development.

Management-related interface analysis is becoming a necessity for HAD vehicles, not only to identify hazard but also to secure the systems. The purpose of SMS and CSMS is to provide policies, procedures, and processes to an organization to meet its respective objectives or project-related goals. FuSa is concerned with preventing accidents by identifying potential hazards, including hazardous events in operational situations, vehicle states (e.g., safe state), and initial conditions. Cybersecurity, on the other hand, is concerned with protecting an asset from potential damage and/or protecting an element or set of components from potential threats and their functions/features. Two important key points for the management systems are first, the identification of acceptable processes and the description of the processes, especially for HAD vehicles where new technologies and innovations are associated with various development activities. Second, understanding the management processes is vital for a safe and secure development with a combination of knowledge and information sharing, lesson learning, and decision-making. The hierarchical dimension of the processes is increasing significantly when interface planning between FuSa and cybersecurity is required. Apart from planning time management and communication management during the development phases, continuous monitoring and improvement of the management systems are essential to achieve not only the organization's goals but also project-dependent goals. Hence the fulfillment of management functions is an essential aspect of the management process including interfaces.

The major challenge for the management systems (SMS and CSMS) interface is to identify the influencing management factors based on the lifecycles and communication aspect. Despite the implementation of management approaches with their interfaces, the enforcement of effective monitoring or control strategies is a prerequisite for

safe and secure HAD vehicle systems development. This paper aims to provide a framework to deal with the interface of SMS and CSMS for HAD vehicles by presenting:

- The interface-related management factors with respect to SMS and CSMS.
- Experts' judgement regarding the interface of the management systems through a series of questionnaires.
- A survey results based on the feedback from the participants by means of the degree of influence of the management factors.

This paper briefly mentions the state-of-the-art based on standards recommended for HAD systems development in chapter 2. Afterward, chapter 3 presents adaptations in the FuSa and cybersecurity processes with respect to risk assessment and communication. Later, chapter 4 describes the survey approach and methods with survey results to build confidence in the proposed interface approaches for SMS and CSMS. Finally, chapter 5 includes the conclude the paper's outcomes and mentions future work.

2 BACKGROUNDS

FuSa focus on the unintended behavior of an Electrical and/or Electronic (E/E) system. The functional insufficiency of the intended functionality of an E/E system is dealt with in the SOTIF aspect. The protection of E/E systems or even components against the threat scenario is covered by cybersecurity. To manage the complexity of risks, an interface between management systems is required, covering areas such as FuSa, cybersecurity and Safety Of Intended Functionality (SOTIF) (ISO 21448, 2022). The section provides a brief overview of management systems related to FuSa and cybersecurity by means of available road vehicle standards and regulations. In this paper, safety covers the area of FuSa and SOTIF, and cybersecurity deals with road vehicle cybersecurity aspects for HAD vehicles.

2.1 Safety and Cybersecurity Management Systems

Both organizational and technical aspects have to be considered and carefully coordinated throughout the product lifecycles. It is therefore important to build a common understanding of safety and cybersecurity among the teams. Safety simply means ensuring the

absence of unreasonable risk, and SMS can be defined as an approach to managing risk and ensuring the effectiveness of the risk controls in a formal or structured manner. SMS includes the safety culture through safety promotion, communication by means of knowledge and information sharing, risk management, and safety assurance processes. SMS is well-established in aviation known as International Civil Aviation Organization (ICAO) and is considered as state-of-the-art for HAD vehicles (ICAO, 2009). According to European Union Aviation Safety (EASA), SMS is defined as “*Safety management benefits the total aviation system by strengthening traditional risk control practices and ensuring safety risks are managed systematically. Safety management allows room for innovation and flexibility: It is less about describing what to ‘do’ and more about how to ‘achieve safety’*” (Ky, 2019).

Cybersecurity is concerned with the protection of an asset that has cybersecurity-related properties such as confidentiality, integrity, and/or availability (ISO/SAE 21434, 2021). CSMS can be expressed as an elevated risk that includes cyber attacks, damage, and/or unauthorized access. However, concerning the harmonization and/or road vehicle type approval UN regulation No. 155 UNECE WP.29 is currently in application. UN regulation No. 155 defines UNECE WP.29 the CSMS by means of “*a systematic risk-based approach defining organizational processes, responsibilities, and governance to treat risk associated with cyber threats to vehicles and protect them from cyber-attacks*” (R155, 2021).

The quality management system is out of the scope of this study because it focuses on the achievement of customer and organizational requirements. However, success in the automotive sector can only be achieved through compliance with the SMS and CSMS. Mastering the interface between SMS and CSMS is one of the main criteria for the entire lifecycle of HAD vehicles, including safety and vehicle type approval.

2.2 Management Systems Interface

The interface between FuSa and cybersecurity is widespread to some degree in various fields such as aviation (Zhang, 2021), robotics and automation (van der Aalst, 2018), and railway (Geyer, 2000). In the aviation sector, the SMS framework consists of components and elements known from the aviation organization (ICAO, 2009) and is considered in this paper for HAD vehicle’s SMS development. ICAO consists not only of the components of the SMS but also of the cultural and reporting systems with the

maintenance of FuSa as a critical aspect of the SMS. Each component, element, and process are explained in terms of functional expectations, and processes for the contribution of management systems that can express a performance evaluation.

Furthermore, management systems interfaces are addressed as a set of components and comply with the standards and regulations including the management frameworks. However, managing cybersecurity is an expensive, time-consuming, and challenging approach. Components for SMS and CSMS consists of operating systems, applications, configuration management, security patches, vulnerability checking, and continuous monitoring of the systems during the product development and post-development phases.

While automotive SMS implements the functional safety activities including the standards and regulations such as FuSa (ISO 26262, 2018), basic FuSa (IEC 61508, 2010), and autonomous evaluation (UL4600, 2020), the CSMS implements the cybersecurity activities including standards like cybersecurity engineering (ISO/SAE 21434, 2021), and/or cybersecurity for operational technology (IEC 62443, 2018). The SMS and CSMS explain policies, procedures, and processes for an organization to meet the objectives because of the intended safety-related functionality of the system at the vehicle level or an asset respectively. The organization culture demonstrates the organizational trust, objectives, and cooperation of people and other areas like organizational capability, safety and security-related development, adaption, and innovation. Functional safety culture and cybersecurity culture are introduced in the standard ISO 26262 and ISO/SAE 21434 accordingly. However, the interface between FuSa and cybersecurity during the concept and product development phases is not explained in detail in these standards. UL4600 is one of the first standards for safety and the evaluation of autonomous vehicles and other products that described the safety principles including the cybersecurity interface. Additionally, the unsafe and unintended behavior of human is one of the aspects that has been considered in the interface of the management systems as the human factor is a prompt problem to be solved. Human factors are considered as one of the influencing management factors as cultural interfaces, communication, and interface analysis.

Two management systems have some overlapping in the area of policy, competence, roles, and responsibilities, change management, and incident response and planning. However, the interfaces between the management systems are not widely

accepted because of the majority of the mature SMS compared to CSMS in the automotive industry. It is important to establish a common understanding between the FuSa team and the cybersecurity team. It should be considered that both FuSa and cybersecurity has different culture and processes. Misunderstanding and clarification need to be dealt with systematically and carefully between both teams to develop safe and secure HAD systems.

3 FUNCTIONAL SAFETY AND CYBERSECURITY INTERFACE PROCESS

For HAD systems of automated vehicles, adaption is in demand and supported by approaches like the model-based approach, and knowledge-based approach. To indicate the interface with respect to system development interface, risk assessment, and communication interface are focused on in this section. The objective of the interface process is to identify the new system areas where management required and to reduce the conflicts between the safety and cybersecurity for a specific system by means of systems integration.

3.1 System Development Interface

Management Processes are known in general for automotive but no specifications for HAD vehicle's SMS and/or CSMS are documented completely. Automated vehicle specifications are packed with necessary goals for safety achievement and their requirements category from mandatory to conformance in UL4600 as goal-based techniques (Tech, 2019). Compliance with UL4600 is still provocative to the industrial application because of its wide range of safety claims. However, UL4600 is the first standard addressing autonomous vehicles and related products like HAD functions applicable to an autonomous vehicle. Additionally, aspect like machine learning and operational design domain with other safety aspects of the autonomous vehicle has been addressed in UL4600. Functional safety, operational safety, autonomy safety, and other safety assurance activities can be used as inputs and demonstrated the contents and relationships of work products as evidence (UL4600, 2020). The idea of adopted management processes is to separate the SMS and CSMS topics to simplify and decrease the management steps to attain the required safety level. This leads to the need for the constant perception of

safety and cybersecurity guidelines (SAE J3061, 2016) and a common understanding of subject divisions.

3.2 Risk Assessment Interface

Regarding the complexity of HAD systems, safety hazards can result in cybersecurity threats. Furthermore, threats can be the reason for new safety hazards (Khatun et al., 2021). Thus, the collected data from scenarios must be handled considering hazards and threats. For the adoption of the risk assessment, it is proposed that the hazard's risks are clustered into sets such as irrelevant to cybersecurity, relevant to a safety hazard, and relevant to a cybersecurity threat. Risks relevant to threats are handed over to the risk assessment and activities are supported by CSMS. An effective risk assessment requires Hazard Analysis and Risk Assessment (HARA) that supports the Threat Analysis and Risk assessment (TARA) for further development of the product including processes. The key elements of safety and cybersecurity are the identification of items and assets, finding the weak points such as hazard and risk together with mitigation approaches.

3.3 Communication Interface

Communication interfaces always exist between two systems of interest that have the intention to exchange information. For that reason, the systems of interest are SMS and CSMS. If these management systems are already in place, they are usually in communication with other interested parties. Known communication channels can be implemented in one or two directions. This means that the ideal case for the SMS and CSMS interface is two-directional communications with information flow from SMS to CSMS as well as information flow from CSMS to SMS. Some structured interfaces are already defined in the regulations and can be adapted. For example, the CSMS to external parties' communication is considered and supported with a proposed guideline in ISO/SAE 21434, Road vehicles — Cybersecurity engineering (ISO/SAE 21434, 2021). Like in this example the communication interface between SMS and CSMS shall be structured and defined. First the basic requirements shall be met from both sides. This includes the proper definition of both systems of interest (SMS and CSMS). Additionally, It is also important for communication to use the same language in a figurative sense. Similar terms and keywords shall be used, a common glossary can be helpful. Accordingly, the data collected and used in

software-based analysis shall be compatible as well. Data and results from threat analysis tools shall be understandable, compatible, and easily implemented in an SMS that apply hazard analysis tool. Same applies the other way around from hazard analysis to threat analysis tools.

For the external communication standards already consider an agreement between the responsible persons. ISO 26262 particularizes the development interface agreement that the responsibilities in between customer and supplier for activities, evidence or work products shall be exchanged and specified by each party (ISO 26262, 2018). This concept can be applied to the SMS and CSMS interface. It is necessary to define roles, responsibilities, and accountabilities. Tasks and person shall be defined and documented. The ICAO Manual gives the idea to introduce a safety service office to coordinate all safety-relevant issues and to pass on the relevant information to the responsible position (ICAO, 2009). For a structured communication interface, it can be helpful to introduce a cybersecurity service office in the CSMS as well. In this case, it is possible to distribute all safety and or cybersecurity-relevant information between the offices and they can coordinate SMS and CSMS internal communication paths. Other standards like the UL4600 also consider the requirements for a comprehensible communication interface. The resolution of potential safety and/or cybersecurity-related issues is done by identifying the processes and activities that support the communication and tracing of issues (Tech, 2019). Consequently, it is natural to specify the SMS and CSMS-related processes and working practices before they are aligned with each other for similar and coordinated issue tracing.

4 SURVEY APPROACH AND CONCEPT

For HAD systems of automated vehicle adaption is in demand and supported by approaches like, model-based approach, knowledge-based approach. To indicate the adaption with respect to management systems, management processes, risk assessment and communication interface are focused in this section. According to our hypothesis, the respondent evaluates the influence factors based on their knowledge and experience.

Several industry partners and research groups have participated to examine the influence factors

related the interface of the SMS and CSMS. In early stages colleagues that are familiar with the topic are asked to examine the survey and to complete the tasks to their best knowledge and experience. After that industry partners related to topics like management systems and FuSa are being introduced to the idea of rating the management factors for their organization. In fact, the option of using the results of their reflection on prior projects is presented as an advantage for future work. Organizations get an overview of which management factors are important for themselves and can easily use them for comparison with the actual state. In total 11 participants from FuSa teams and cybersecurity teams including management leaders have taken part in this survey. The employment status of the interviewee are as follows: 4 of the respondents are FuSa industrial experts and 3 of the respondents are cybersecurity industrial experts, 3 of the respondents are research engineers working in safety and cybersecurity-related projects and 1 of the participants is professor from different faculty of computer science including safety. 36% of the respondent have already worked in products related to FuSa and cybersecurity. The used survey contains the following information:

- SMS and CSMS interface-related questionnaire.
- Identification of management factors.
- Determine the degree of influence of management factors.
- Support to prepare a set of interface related management specification for HAD system.

As a part of the survey preparation, both organization-based management systems and standard-based management systems recommendation related to safety and cybersecurity has been weighed in this section.

4.1 Method and Procedure

In order to represent the interface of the SMS and CSMS, the management related components and elements are considered from a knowledge-based approach, brainstorming method. In addition, to assist the implementation of the survey a range of measurement data are included such as utilization of the existing technologies qualitative and quantitative questionnaires, monitoring employee activities for a specific individuals and company perspectives. Interface between management systems (SMS and CSMS) at functional level consist not only the management of the human factor, processes, and

activities but also the employee awareness and data protection. Good practices targeting different management levels (board level, senior and employee level) within an exemplary organization has been considered. From the viewpoint of safety and cybersecurity management systems interface, the engineering key points and human factor, methods such as brainstorming, scenario-based analysis and STPA are applied. Conventional quantification methods are not efficient due to the communication complexities between FuSa and cybersecurity and human factors. Therefore, the survey supports to evaluate the interface concept by means of decision making, development constraints and identifying the possible actions that needs to be taken when a product consists functional safety and cybersecurity such as high automated driving systems. Although vulnerabilities are often ignored or less prioritized or misunderstood during the processes and considered later in the development, but awareness of cybersecurity is increasing currently with great importance.

The hypothesis of the study is based on knowledge-based approach with respect to safety and cybersecurity interface for HAD vehicles. The survey provides valuable insights in the interface between SMS and CSMS with the opinion from different individuals. Regardless of which methods and process is applied to determine the management factors and degree of influences, the survey will be able to compute the possible safety and cybersecurity countermeasures for assisting the management interface. In general, the simple and common interface factors can be categorized as prediction, decision making and control. The interface factors can be evaluated based on the survey results. In addition, the following survey supports to enhance the risk assessments, impact analysis, and conduct the data collection with interface aspects. Systematic approach for the interface of the management systems is commonly used in conventional organizational stage as a simple manner, usually not a deterministic manner because of the uncertainty of the business.

The defined cases are, (i) chronological representation of the management factors, (ii) indicating the degree of interface between the management factors and (iii) collection of opinion about the possible management systems interface from the interviewee/participants.

4.2 Survey Questionnaires

As survey type the questionnaire is chosen which is usually a paper-and-pencil instrument that the

respondent completes. The respondents are allowed to fill the form at their own convenience. Matrix survey questions are used with a series of rating scale to simplify the questionnaires for the interviewee as listed in Table 1. In an attempt for better understanding the interface between the management systems, the survey is divided into three main cases as defined the in previous section. A brief summarization about why the survey is needed and how it can benefit to overcome the management systems related challenges has been added in the survey. The questionnaires can be used to gather the feedback from different types of respondents and based on their opinion to establish a generic set of management specification for HAD vehicles. The intention of this approach is to make the respondents realize the necessity and further benefit distributed management systems development. The questionnaire is divided into three sections (coding the information, accumulating opinions, and information collection) to compresence the interface aspect.

Survey type research has the potential to enhance the performance of the activities and mature the systems and known as empirical data collection method. Applying survey research provides framework and or requirements for system engineering such as stakeholders requirements analysis, architecture design, project management and risk assessment including information management (Smartt and Ferreira, 2013). A huge number of literatures exists related to survey as questionnaire in different areas as part of data collection, response of the interviewee as human factor, support to provide guidelines of the topic for example influencing factors for interface of management systems. The survey is performed in the context of interface between SMS and CSMS. In addition, the survey can be used in complex systems development processes with a perspective of improvement. The goal of the survey is to collect the interviewee opinion regarding the interface of SMS and CSMS including the management factors with influencing degree identification.

4.3 Management Factors

To identify and analyze the interface of the SMS and CSMS, management factors are investigated and studied in this study with their influences during safe and secure HAD vehicle development. The conceptual outcomes focus on the factors, affecting the interface of management systems (SMS and CSMS). To elect the management factors for HAD

systems, different sectors such as aviation, (ICAO, 2009) (Sawyer, 2021) (Smarrt and Ferreira, 2013) (Li, 2018) robotics, (Kihel and Herbal, 2018) industrial control system (Śliwiński et al., 2018) are inspected. Based on the knowledge and expert judgments, a list of management factors is presented in Table 1 with the concise description of functions related to the defined management factors.

Table 1: Management factors based on the SMS and CSMS interface with function description.

Interface related Management factors (MF)	MF Factors	Function Description
Communication	F1	language barrier, coordination, resource management and maintenance
Documentation	F2	audit report, interface requirements, etc.
Equipment	F3	Tools, traceability, etc.
Incident Investigation	F4	contribution factors, human error, cost, new process, etc.
Interface in Analysis	F5	hazard analysis, threat analysis, scenario-based analysis, mitigation approach, etc.
Policy	F6	organizational structure, roles and responsibilities, plans, commitments, etc.
Rules and Regulations	F7	organizational-based safety and security rules and regulations
Committee	F8	developing strategies for interface, safety plan incl. cybersecurity aspects and vice-versa, correlative actions, allocation of resources, improvement of products.
Conflicts in domains	F9	constraints, limitations
Cultural interface	F10	performance measures responsibilities, organizational values, safety culture and cybersecurity culture etc.
Risk Management	F11	hazard identification, threat identification, analysis/assessment, impact, Goals and requirements, etc.
Training and Competency	F12	team and/or Individual training, competency requirements, etc.
Work Practice	F13	operational, maintenance, service, compliance, standards, activities and etc.

Thereby, the first contribution of this paper has been achieved. The significance of these management factors as listed in Table 1 is evaluated with influencing rate as no influence (No), Low influences (L), Medium influence (M), High influence (H) and very high influences (VH). Based on the evaluators results the most important factors of management systems can be identified. The risk assessment methods can be applied to decrease the hazard related communication hazards.

4.4 Results

It is widely accepted that HAD vehicles focus on the safe and secure driving for the user/driver. The complex system development including interface SMS and CSMS is one of the areas where experts from different domains are having different opinions, judgments, and impressions. Therefore, a survey has been performed to have a view of the interface between SMS and CSMS. Moreover, surveys are one of the valuable research techniques that convey valuable information, outcomes, opinions in a cost-effective manner.

The outcomes of this survey not only support to evaluate the organizational aspects of the SMS and CSMS interface approach but also aid the researchers for further development. The survey results can be used as empirical evidence to optimize the management factors in organizational level and part of impact analysis. Higher management commitments with organization cultures, finance and resources can be fulfilled for safe and secure product development (e.g., HAD vehicle systems) only if interface management factors are identified, prioritized, and monitored.

The answers are categorized as fully, partially, or not to restrict the considered domain. A glimpse of the participant's answers is represented in Figure 1 with three different colors where, blue, orange, and gray colors indicate fully, partially, or not agreed respectively. All participants are requested to answer all questions by selecting the given answer categories and 10 participants answered. Based on the survey results, the following questions will be considered for the development of the interface management specification.

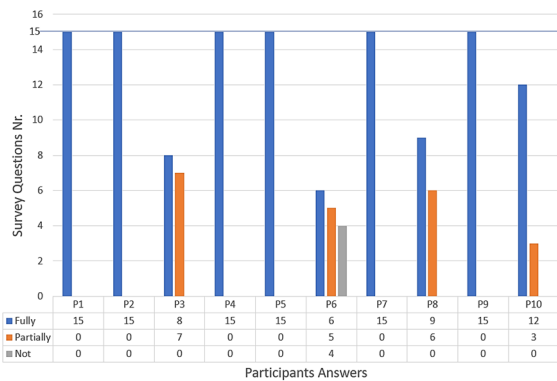


Figure 1: Overall Survey Results from Participants.

The goal of QA session is to allow the user or participants to ask questions, using the standard terminology and obtain a concise answer. Additionally, the aim for accumulating the degree of influence between the management factors is to realize which of the following factors has certain influence that can be acknowledged in the management interface requirement or specifications.

To receive the opinion based on the degree of influence among the management factors linguistic terminology has been requested to use to the participants. For this reason, participants are asked to complete an influence rate chart based on the interface between management factors.

A sample chart from one participant is illustrated in Figure 2. The influence rate chart has been considered to identify the influencing degree of the management factors that can be used to any automated management framework such as fuzzy techniques. The survey provides an ample of information that can be used to determine how management factors interact and influence each other.

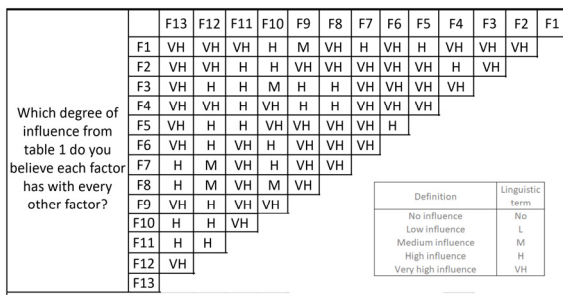


Figure 2: Degree of influences defined by a participant.

The management factors are not only recorded, but the degree of their influence is also determined. As consequence the second contribution has been accomplished as represented in Figure. 2.

The factors that influence the management processes by means of interface to a certain extent are examined as a result of the survey as presented in Figure 3.

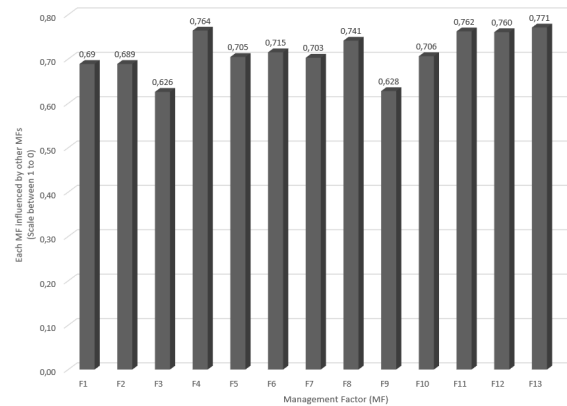


Figure 3: Each of the MF influenced by other management factors.

The degree of influence is scaled between 1 and 0, where 1 means that a factor is very much influenced by other factors and 0 means that the factor is not influenced by other management factors. For example, F13 (work practice) has the most influence among the other management factors and F3 (equipment) has the least influence as displayed in Figure.3 based on the survey results. To be precise, the interface between F12-F13 has the highest degree of influence, while F4-F12, F5-F11 have the second highest degree of influence and F4-F13, F4-11, F6-F7 have the third highest degree of influence. In contrast, F3-F9 have the first lowest degree of influence, F1-F5, F2-F9, F3-F6 have the second lowest degree of influence, and F3-F1, F3-F7, F3-F10, F4-F9 have the third lowest degree of influence. Thus, the third contribution is fulfilled by identifying the interface related management factors that shall be considered during HAD system development.

5 CONCLUSIONS

Safety requires the cybersecurity and can no longer be overlooked. Cybersecurity is tightly integrated with the FuSa processes and communication because of their dependencies between the vulnerabilities and overall safety. Highly automated driving vehicles are challenging the current technologies and engineering methods and approaches in terms of their wide functionalities and setting new expectation for user as driver or passengers. The HAD vehicles offer a vast range of communication and infotainment and

accessibility such as app-based, internet access and remote access. Unfortunately, such vehicle functionalities or features are putting significant stress to safe and secure product development that required mature and continuously improvable SMS and CSMS.

For HAD vehicle system development, an assessment of SMS and CSMS, including their interfaces, needs to be performed (depending on the organization and/or project) to determine if the safety policies and procedures are acceptable. The management systems shall be adjusted and/or modified based on the activities to develop HAD vehicle systems. For this reason, the identification of the management factors is vital at the beginning of the development phase. The management factors not only support the safety culture and cybersecurity culture but also their interaction while developing complex functions for HAD vehicles. Moreover, several design patterns can be applied to support management systems in terms of description and identification in contexts and schemes for recruiting processes. This pattern helps not only in information systems as data management but also support to simplify the development phases, maintenance and services of such complex systems.

The focus area of this paper is to propose the interface of the SMS and CSMS at different level such as at concept phase, development phase and post development phase. Additionally, proposed adaption processes such as risk assessment and communication domains and gives insight to prepare the survey. Moreover, this paper exhibits the interface between the management factors and their degree of influence. A survey has been performed to build confidence and provide argument for the importance of the interface between SMS and CSMS in HAD vehicles that will not only support both vehicle manufacturers and suppliers.

Furthermore, based on the survey results the management factors are evaluated, and the questionnaires support to get a perspective of the management systems interface from different aspects. The adaption of the management process, risk assessment and communication interface are evaluated by the survey results as well. Examining the survey results, the perspective and purpose of the decision making throughout the safety and cybersecurity lifecycles can be realized and possible to provide a set of clarified or specific management interface requirements. Since this paper represents the beginning of the interface between management systems this should be the impetus to organizations to define and evaluate their own management factors

and to take part in a survey so that for further work the relations between SMS and CSMS are more significant.

In the future, the number of survey participants will be increased by including (Original Equipment Manufacturers (OEMs) as well as Tire 1 and Tire 2 suppliers for E/E systems and/or components of HAD vehicles and research institutions. Additionally, the technique of decision making can be applied to improve both the organization and project-related processes. There is a possibility that existing risks and weaknesses will be revealed through the application of such techniques in management systems. Therefore, to understand the management relevant cause and effect relations among the FuSa and cybersecurity decision making trial and evaluation laboratory (DEMATEL) can be considered due to its structured approach and extended use in decision making. The classical DEMATEL and/or Fuzzy DEMATEL methods can be applied on the early stage of research development and this paper will be considered as basis for future research work.

ACKNOWLEDGEMENTS

Founded by Federal Ministry of Education and Research - Project New Multi-Layer Platforms for Security- and Safety-Relevant Automated Driving Function (MLPaSSAD).

REFERENCES

- Shuttleworth, J. (2019). SAE standards news: J3016 automated-driving graphic update. <https://www.sae.org/news/2019/01/sae-updates-j3016-automated-driving-graphic>
- SAE J3016. (2021). Standard, Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles.
- ISO 26262 (2018). Standard, Road Vehicle — Functional Safety, Part 1 to part 13.
- ISO 21448. (2022). Standard, Road Vehicles — Safety of the intended functionality.
- International Civil Aviation Organization (ICAO). (2009). Safety Management Manual (SMM) – Second Edition, approved by the secretary general and published under his authority, ICAO Doc 9859 AN/474, ISBN 978-92-9231-295-4.
- Ky, P. (2019). EASA Executive Director, European Union Aviation Safety (EASA), Safety Management System, <https://www.easa.europa.eu/domains/safetymanagement/safety-management-system-sms>
- ISO/SAE 21434. (2021) ISO/SAE 21434. (2021). Road vehicles — Cybersecurity engineering.

- Sawyer, K. (2021). Senior Manager- Aviation Security Development, Advisory Services, UK Civil Aviation Authority, "Security Management Systems-Technical Assistance by the UK CAA.
- R155. (2021). UN Regulation No. 155 UNECE WP.29, Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system.
- IEC 61508 (2010). Functional safety of electrical/electronic / programmable electronic safety-related systems, Part 1 to part 7.
- UL4600 (2020). Standard for Evaluation of Autonomous Products.
- DIN EN IEC 62443 (2018). Standard, Industrial communication networks- Network and system security, Part 3 and Part 4.
- Khilhel, F. and Herbal, A. (2021). Impact of firms psychological behavior in process performance: the optimal employee's experience, *International Journal of Financial Accountability, Management and Auditing*, ISSN (2788-7189), Volume 3.
- ISO/ TR 4804. (2020). Road Vehicles — Safety and cybersecurity for automated driving systems — Design, verification, and validation.
- Koopman, P. (2019). In Article, An Overview of Draft UL4699: Standard for Safety for the Evaluation of Autonomous Products, Edge Case Research.
- Tech Industry, (2019). Standard For Safety For The Evaluation Of Autonomous Products. Standard for safety analysis and evaluation of autonomous vehicles. Semiconductor Engineering: Deep Inshight For The Tech Industry.
- SAE J3061. (2016). Cybersecurity Guidebook for Cyber-Physical Vehicle Systems.
- Khatun, M. and Wagner, F. and Jung, R. and Glaß, M. (2021). Safety Management System and Cybersecurity Management System Interfaces for Highly Autoamted Driving Vehicle, *FAST-Zero'21 Program & Proceedings*, .doi: 10.13140/RG.2.2.20663.85925.
- Smarrt, C. and Ferreira, S. (2013). Applying Systems Engineering to Survey Research, *Conferece of systems engineering research (CSER)*, Published by Elester B.V., Procedia Computer Science 16, Page 1102-1111, USA.
- M. Śliwiński, M. and Piesik, E. and Piesik, J. (2018). Integrated functional safety and cyber security analysis, *International Federal of Automatic Control (IFAC)*, Published by Elester Ltd.
- Dwivedi, S. K. and Singh, V. (2013). Research and reviews in question answering system, *International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA)*, Procedia Technology 10, page 417-424, Published by Elester Ltd., ScienceDirect.
- Bouziane, A. and Bouchiha, D. and Doumi, N. and Malki, M. (2015). Question Answering Systems: Survey and Trends, *The International Conference on Advances wireless, information, and Communication Technologies (AWICT)*, Procedia Computer Science 73, page 366-375, Published by Elester Ltd., ScienceDirect.
- van der Aalst, W.M.P., Bichler, M. and Heinzl, (2018). In article, A. Robotic Process Automation., *Business & Information Systems Engineering*, **60**, page 269–272 <https://doi.org/10.1007/s12599-018-0542-4>
- Geyer, A., Davies,A. (2002). In Article, Managing project–system interfaces: case studies of railway projects in restructured UK and German markets, *Research Policy*, 29 (7-8), Pages 991-1013, ISSN 0048-7333, ScienceDirect. [https://doi.org/10.1016/S0048-7333\(00\)00116-5](https://doi.org/10.1016/S0048-7333(00)00116-5),
- Guo, D., Zhang, X., Zhang, J., Li, H. (2021). In: Jing, Z., Zhan, X. (eds), An Interface Management Approach for Civil Aircraft DesignLecture Notes in Electrical Engineering, vol 680. *Proceedings of the International Conference on Aerospace System Science and Engineering (ICASSE)*, Springer, Singapore. https://doi.org/10.1007/978-981-33-6060-0_30