Automotive Functional Safety: Scope, Standards, and Perspectives on Practice

Md Rafiul Kabir
University of Florida, USA

Srivalli Boddupalli
Lucid Motors, USA

Atul Prasad Deb Nath
Qualcomm Inc., USA

Sandip Ray
University of Florida, USA

***Abstract*—Modern automobiles include hundreds of Electronic Controller Units (ECUs), a large number of sensors and actuation modules, several in-vehicle networks, and several megabytes of software code. The goal of functional safety is to assess the potential risk of hazardous conditions resulting from malfunctioning in these components. Achieving functional safety for modern automotive systems entails a variety of complex steps including interpretation of safety standards, developing safety solutions, and making a safety case, all of which are getting constantly refined and updated as architectures, system designs, and electronic/software features are added. In this paper, we provide a comprehensive overview of automotive safety approaches, standards, and approaches involved in safety solutions for automotive systems. We include perspectives, constraints, and requirements from the different players in the automotive supply chain and the conflicts and trade-offs among stakeholder interests involved in safety design. Emerging trends in automotive systems and their impacts on functional safety are discussed.**

INTRODUCTION

The goal of functional safety is to comprehend and mitigate the risks associated with errors and malfunctions in electronic and software components, ensuring these faults do not compromise the safety of the system or its operating environment. We consider functional safety of *automotive systems*, where "compromising safety" unacceptable risk of physical harm or health damage to people or property through an accident, either directly or indirectly. Functional safety has become paramount in automotive systems over the last two decades, as automobiles have transitioned from primarily mechanical and electro-mechanical entities to sophisticated consumer electronics items. Vehicles now extensively use advanced electronic and software technologies, such as infotainment systems, autonomous driving features, and connectivity with the Internet of Things (IoT) [1]. This evolution reflects the integration of sophisticated sensors, artificial intelligence, and electronic components that are characteristic of traditional consumer electronic devices. The push towards electric vehicles (EVs) and consumer demand for technology-rich vehicles further aligns the automotive industry with the consumer electronics sector, emphasizing software and electronics as key components in modern vehicles' functionality and

Digital Object Identifier 10.1109/MCE.2023.Doi Number

Date of publication 00 xxxx 0000; date of current version 00 xxxx 0000

This article has been accepted for publication in IEEE Consumer Electronics Magazine. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MCE.2024.3394165

appeal. Such electronics-driven autonomous features that hold the promise of dramatically increasing safety by reducing and eventually eliminating human errors while improving the efficient utilization of the transportation infrastructure, comfort in travel, and reducing environmental impacts. However, autonomy also increases the susceptibility of these systems to errors and malfunctions in electronic and software components. Recent research [2], [3] has shown that it is possible — even relatively straightforward — for errors and malfunctions to undermine the functionality of vehicular systems, cause catastrophic accidents, and bring down the transportation infrastructure.

Given the sophistication and complexities of the electronics deployed in automotive systems, functional safety is a challenging enterprise. Strategies for functional safety typically involve detecting a failure or malfunction in an electronic component before it can lead to hazardous outcomes and implementing suitable mitigatory actions. These actions vary based on the nature of the failures and may range from initiating emergency protocols, alerting the driver to the malfunction, to transitioning the vehicle to a secure state. Thus, as vehicles increasingly resemble consumer electronics in their complexity and functionality, addressing functional safety issues becomes critical. This ensures that the intricate electronics and software that enhance vehicle capabilities do not, through design or implementation flaws, lead to unsafe conditions. Fig. 1 depicts an overview of automotive safety systems.

Obviously, as electronic and programmable components increase in sophistication, it gets increasingly complex to achieve or even precisely characterize functional safety goals. Furthermore, automotive systems are developed through a complex, globally dispersed supply chain which includes OEMs, Tier 1 and Tier 2 suppliers, service providers, software vendors, and many others. Safety implications are different for the different players, *e.g.*, a Tier 1 supplier has to comprehend safety at the subsystem level, while an OEM has to comprehend the implications of integrating subsystems into a vehicle. To address these concerns, various safety standards have been designed to enable a common framework for designing, testing, and certifying automotive systems. Unfortunately, with the increase in design complexity, the standards are also becoming complex, hard to comprehend, and even controversial. It is non-trivial to sift through this plethora of documents, comprehend their implications on various automotive features, and design safety

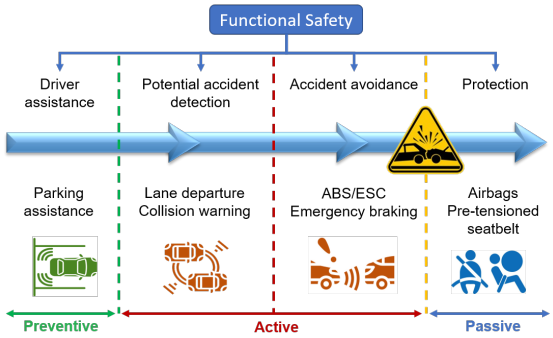

Figure 1. An overview of safety in automotive systems

specifications, implementations, and verification flows.

In this paper, our goal is to improve the understanding of automotive functional safety by beginning researchers and practitioners, especially considering the integral role of consumer electronics in modern vehicles. We explain the scope and limits of various standards, examine them from the perspective of various automotive supply chain players, and illustrate how they can be used to drive design and implementation. Additionally, we discuss the impact of emerging autonomous features on safety standards and their implementation in the context of the evolving landscape of automotive consumer electronics.

1. Trends in Automotive Electronics and the Role of Safety

The evolution of the automotive industry over the past decades has brought about a transformative shift in vehicle safety. A modern automobile is typically equipped with Electronic Control Units (ECUs), ranging from a few dozen in standard models to over a hundred in more sophisticated, high-end vehicles. Each ECU is connected to a different set of sensors and actuators, as well as several in-vehicle networks, interfaces, and wireless protocols for communicating with various external entities [4]. With the integration of intricate electrical and electronic (E/E) architecture and sophisticated domain-specific software systems, the automotive sector has witnessed a remarkable advancement in safety-related technologies. These technologies encompass a wide range of applications, spanning from entertainment-rich touchscreen-based infotainment systems and high-speed cloud connectivity to critical safety functionalities like airbag deployment and automated emergency braking. A variety of

This article has been accepted for publication in IEEE Consumer Electronics Magazine. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MCE.2024.3394165

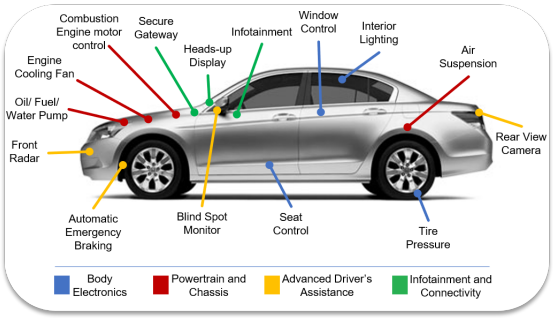

Figure 2. An illustrative example of electronic systems prevalent in modern-day vehicles.

in-car user interface systems have been adopted, including Windows Embedded Automotive, Carrio, and smartphone-based applications (like Apple CarPlay and Android Auto) [5]. The illustration of modern automotive electronic systems in high-end vehicles, as depicted in Figure 2, underscores the complexity and significance of these safety-driven innovations.

The electronics in automotive systems can be classified into five broad categories, defining specific functional domains [6].

- **Powertrain**: In automotive electronics, the powertrain domain includes crucial systems responsible for the vehicle's propulsion and transmission. It consists of Engine Control, which maintains the performance and efficiency of the engine, and Transmission Gear Control, which ensures smooth gear transitions and appropriate power distribution. These systems operate together to provide power and control to the wheels to eventually drive the vehicle.
- **Chassis:** The chassis domain is primarily concerned with the stability and safety of the vehicle when in motion. It includes important features such as the Antilock Braking System (ABS), the Electronic Stability Program (ESP), Automatic Stability Control, and Adaptive Cruise Control. These solutions help to make driving safer and more regulated.
- **Body:** A vast range of functions are managed within the body of automotive electronics. This includes Air Conditioning and Climate Control for interior comfort, Dashboard Functions that provide essential driver information, and control over doors, seats, windows, mirrors, wipers, and lights, ensuring convenience and safety. Features like Cruise Control and Park Distance Control further enhance the driver's experience and make vehicle operation more efficient.
- **Telematics:** The in-car communication and entertainment systems are part of telematics. Because of its multimedia functions, users can enjoy movies, music, and more. Infotainment Features offer connectivity and information services, while Rear Seat Entertainment keeps passengers entertained. Additionally, GPS and Navigation Systems provide location and routing information, making journeys more efficient and enjoyable.
- **Passive safety**: This domain focuses on systems that respond to and mitigate the impact of accidents. It includes rollover sensors, airbags, belt pretensioners, etc. that aim to minimize injuries and improve passenger safety in the event of an emergency.

Because every automotive electronic domain has different features and requirements, switching between them presents different safety challenges. Hard real-time constraints and the need for large computational power are common concerns in domains such as chassis and powertrain. However, the Chassis domain exhibits a more widely distributed hardware architecture within the vehicle. This distribution introduces safety challenges related to ensuring the proper coordination and communication between various components to maintain vehicle stability and safety. Notably, despite their lack of flexibility, time-triggered software technologies bring well-suited solutions for this domain [7]. On the other hand, telematics has to address the requirements for high data throughput [6]. This requirement leads to distinct technological solutions, such as communication networks with high bandwidth and low latency. Furthermore, the design techniques and verification of embedded software in telematics must address specific safety concerns related to data integrity, cybersecurity, and preventing distractions for the driver. In the body domain, it is critical to protect against electrical system failures that could affect basic operations such as lighting and air conditioning. Additionally, cybersecurity measures must be in place to safeguard against potential hacking and data breaches. The timely and reliable deployment of airbags, as well as the accuracy of safety sensors, are critical in the passive safety domain for minimizing injuries and improving passenger safety in emergency situations.

How big a problem is functional safety in automobiles? It is hard to directly measure the impact of electronic failures since most accidents (or lack

This article has been accepted for publication in IEEE Consumer Electronics Magazine. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MCE.2024.3394165

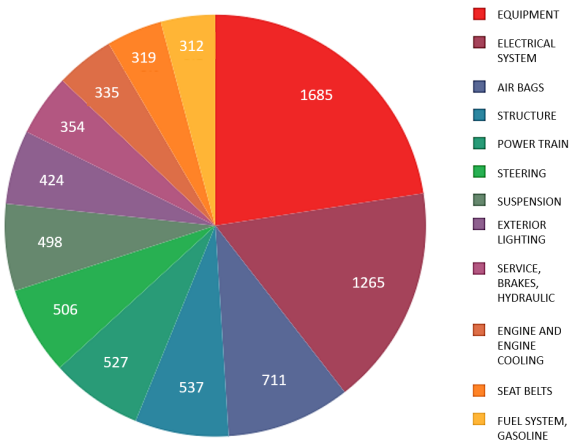

Figure 3. NHTSA Recalls by top 12 manufacturers in the last 10 years

thereof) in today's vehicles can additionally include a human error component: on the one hand, human errors are responsible for most of the accidents on the road, even if the error is induced or enhanced by electronic malfunction; on the other hand, humans alacrity may reduce or minimize the effect of an electronic system malfunction resulting in a safe maneuver when the result could have been fatal without the human intervention. Nevertheless, we can have an *indirect* understanding of the scope and complexity of the challenges induced by electronic system failures from the data on component recalls. Fig. 3 displays data from the National Highway Traffic Safety Administration (NHTSA) on recalls by the top 12 automotive manufacturers for the years 2014-2023 [8].[1] Observe that virtually every electronic component is included, and the numbers are significant. According to data from the first quarter of 2023, automotive recalls increased, with electrical systems being the leading cause [9]. An inescapable conclusion from this data is that failures at this rate would result in unacceptable risks of safety hazards, particularly as we move into the era of autonomous vehicles.

Note that the design complexities discussed above contribute to challenges in other aspects of automotive robustness in addition to functional safety. In particular, they increase the vulnerability of the systems to security and component reliability, and can even increase human errors. In this paper we do not discuss these interplays, focusing instead only on functional safety. However, security in particular is emerging as critical even to the implementation of safety requirements in emergent systems and we will briefly consider its role in safety standards in Section 6.

[1]Manufacturers must notify the NHTSA within 5 business days if they find any safety defects or non-compliance with federal safety standards in their products or equipment. They are also required to submit initial defect and noncompliance reports, along with quarterly updates, as per Federal Regulation 49 Part 573 under the National Traffic and Motor Safety Act. This regulation outlines the procedures for conducting safety recalls.

2. Functional Safety Standards

Functional safety is an integral aspect of safety-related equipment systems, dependent on automated protection for accurate response to inputs. It ensures consistent, actionable reactions to potential issues such as human errors, hardware malfunctions, and operational disruptions. Key safety standards, *e.g.*, the IEC 61508 standard, followed by the automotive-centric ISO 26262 standard, have emerged to methodically ensure functional safety. These standards recognize the intricacies of modern automotive technology and align safety practices with these advancements, thus fostering the development of vehicles that are not only innovative but also inherently safe. Obviously, the standards themselves are voluminous documents covering a variety of aspects of safety design and validation. Here we recount some specific aspects to provide a flavor and role of standards and their limitations and to provide the context for how to guide automotive safety design practices by various stakeholders.

2.1. IEC 61508 Standard

IEC 61508 serves as the foundational cornerstone for all subsequent standards. It adopts a risk-based approach by emphasizing the assessment and management of risks associated with safety-related systems. The standard mandates a systematic evaluation of potential hazards and risks related to safety functions within a system. This involves identifying potential failure modes, their likelihood, and the severity of their consequences. IEC 61508 generally covers all safety-related systems related to mechanical/electrical/electronic/programmable electronic devices that may include electromechanically operated devices through to sophisticated Programmable Logic Controllers [10]. It has achieved significant success from the beginning as a standalone standard focusing on the implementation of E/E/PE safety systems where no other application-specific standard was present. Users can define requirements in terms of the safety functions to be implemented together with the

performance requirements of those safety functions [11]. However, there are a few technical problems with IEC 61508 that were not sufficiently addressed. Compliance with IEC 61508 signifies adherence to a risk-based methodology that comprehensively covers a range of safety-related aspects in various technologies. These are:

- As the standard claims to solve safety-critical issues for E/E/PE technology, the safety and *derivative* measures are not based on engineering science.
- It is misleading to denote all dangerous behaviors as potential *failures*. For example, an aircraft pitching down while in close proximity to the ground may seem dangerous, but, historically [12], [13], it is acceptable for a pilot to pitch down like this when it is necessary.
- There is no mandatory traceability of SW safety requirements from the system to the component level.
- The methods depicted to produce a quality software development process that includes going through a chain of Safety Integrity Levels (SILs) are inappropriate. The standard constitutes a table showing an abstract structure of SIL 1...SIL 4, where no reasonable distinction between these levels is present.

2.2. ISO 26262 Standard

In order to develop a functional safety standard specifically for the automotive industry, a new standard ISO 26262 for automotive electrical/electronic (E/E) systems was introduced in November 2011 [14]. The standard is an adaptation of IEC 61508 for the automotive industry, which describes functional safety for automotive equipment used over the entire lifecycle of all automotive electrical and electronic safety-related systems. ISO 26262 creates a platform that provides high confidence to customers to get automobiles where the prevention of accidents and risks would be acceptable [15]. Given this insight, the following components of this standard are discussed in light of state-of-the-art practices, providing a follow-up perspective on it.

2.2.1. Automotive V-model: An automotive safety life-cycle is documented in the ISO 26262 standard along with instructions to carry out the necessary activities during these life-cycle phases [16]. The concept phase of the safety life-cycle is owned by automobile manufacturers, and it outlines the safety system to implement a function at the vehicle level. The Automotive V-model is a graphical representation (shown in Fig. 4) of the system development life-cycle originating from software development. From a safety-critical perspective, the V-model stands as a feasible depiction of the safety life-cycle processes that help to achieve the safety goals in every phase individually. However, a limitation of this model is that it suggests that the SW and HW requirements are absolute at a preliminary phase. For product development, this is definitely not true because the design and validation often iterate several times before finally finishing the process. This leads to a risk-driven development process, which the standard should address as a concrete discipline.

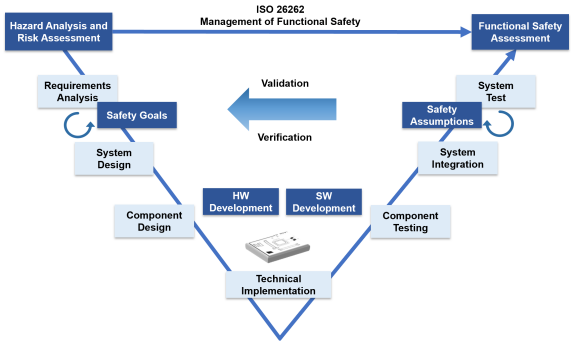

Figure 4. Automotive safety V-model

2.2.2. Automotive Safety Integrity Level (ASIL): ASIL stands as a critical component of the ISO 26262 standard that is determined at the initial phase of the development process by HARA based on a combination of the probability of Exposure (E), the Controllability (C) by a driver, and the Severity (S) of injuries [17]. The key difference between ISO 26262 and IEC 61508 is that ISO 26262 considers controllability for ASIL determination, while IEC 61508 does not. Nevertheless, as we mentioned before about the unsuitability of SIL for IEC 61508, a similar statement can be made for the ASIL of ISO 26262. As there are four different ASILs (ASIL A, B, C, and D), the differences among them are based on the abstract forms of assumptions *i.e.*, opinions based on guesses, human feelings, and cognitive interpretations. As a result, a product can fall under ASIL B and the same product can again fall under ASIL C with different sets of safety concerns.

2.2.3. Qualification of Hardware Components: The hardware qualification has two main objectives:

This article has been accepted for publication in IEEE Consumer Electronics Magazine. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MCE.2024.3394165

Table 1. Perspective on HW and SW qualification methods

Method	Strengths	Limitations
FMEA	A highly effective way to evaluate processes, services, or products that provide valuable information for future design.	Some issues beyond the engineering team's knowledge aren't likely to be detected accounting for unknowns.
	It can identify areas of concern in a logical, structured manner while minimizing development costs.	the technique is time-consuming and sometimes too tedious to find failures via charts
	Identifies critical areas where performance might be diminishing	Still very much unknown and unmanageable in most of the Automotive companies
Fault Tree Analysis	Visually depicts the analysis that helps the engineering team to work on the cause of failures	It examines only one top event ignoring the bottom-down details
	Unlike other methods, human errors are also included in this analysis	Not enough experienced individuals in the industry to understand their many logical gates.
Hardware Metric Fault Calculation	Presents a calculated estimate of the rate of failure that helps alleviate them	The numerical values cannot always represent the actual rate as it is based on assumptions
Tool Confidence Level (TCL)	Provides detailed guidelines on assessing software qualification quite efficiently	ISO 26262 does not mention anything about how to deal with the same arguments for several tools

(1) to show how the components fit into the overall system and (2) to determine failure modes. ISO 26262 standard usually focuses on techniques like Failure modes effects and diagnostic analysis (FMEDA), Fault Tree Analysis (FTA), and Hardware Metric fault calculation to qualify hardware components by testing in various environmental and operational conditions [18]. As we dive deep into the assessment of these methods, there are some pros and cons to consider *i.e.*, summarized in Table 1. Upgrades to the existing methods can contribute to a more advanced version of the standards *i.e.*, improving the assessments of failures.

2.2.4. Qualification of Software Components: Qualifying software components involves activities like defining functional requirements, using proper resources, and predicting software behavior in failure and overload situations. This process is greatly simplified by using qualified software through the determination of Tool Confidence Level (TCL) by using the Tool Impact (TI) and Tool Error Detection (TD) [16]. For example, Simulink is a test automation multi-domain tool used to validate the functionality of a controller, *e.g.*, induced torque-slip characteristics. Being an important task by impacting the final software, it might be denoted as a high confidence level (*i.e.*, TCL 2 or 3). Nevertheless, TCL has its strengths and limitations for software components *i.e.*, mentioned in Table 1.

2.3. Benefits of Adopting Functional Safety Standards

The functional safety standards provide a guideline on safety practices to be employed by the automotive industry. Adopting functional safety standards offers numerous benefits to carmakers, ensuring that the vehicles they produce meet high safety and reliability criteria. Here are some key advantages.

- Safety and Reliability: It enhances vehicle safety by identifying and mitigating risks, *e.g.*, unintended acceleration or brake failure, leading to increased component reliability and fewer malfunctions. By following ISO 26262, automotive manufacturers can ensure that their suppliers meet safety standards, avoiding costly issues during the manufacturing process [19].
- Market Advantage: Achieving safety certifications can distinguish a brand in the competitive market. For instance, a high rating in the European New Car Assessment Programme (Euro NCAP) [20] safety tests often translates into higher consumer trust and potentially increased sales.
- Innovation and Technology Development: The process of adhering to functional safety standards often drives innovation, as carmakers seek to develop new technologies and solutions that comply with these guidelines. For example, the development of advanced driver-assistance systems (ADAS) that use sensors and software to improve safety and driver comfort is a direct result of striving to meet these safety standards [21].
- Traceability and Documentation: ISO 26262 enhances vehicle safety by ensuring systematic traceability and documentation. It mandates structured process models, linked documents, and evidence preservation, facilitating the tracking of development activities. This standard also requires that all actions are planned, executed, documented, and archived (often up to 15 years), improving safety management and compliance throughout a vehicle's

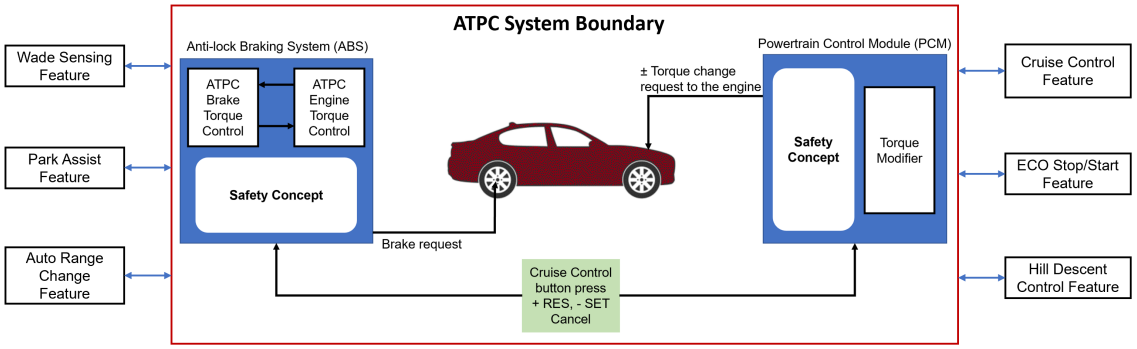

Figure 5. High-Level system architecture for All Terrain Progress Control (ATPC) with sample feature interaction

lifecycle.

On the other hand, standards alone are *not* sufficient to ensure the safety of vehicular functionality. In particular, ISO26262 does not define the safety implementation or even the technical specification of safety requirements for specific automotive products: it only provides an overall skeletal infrastructure that defines what the stakeholders need to do at different stages (*e.g.*, define safety concepts, perform ASIL analysis, etc.). Actually designing safety specifications, architecting safety solutions, and making a safety case must be done by the different constituent organizations, and the quality of functional safety in the deployed product depends on how well these have been performed. We turn to that question in the next section.

3. Functional Safety in Practice

How do various players in the automotive supply chain define functional safety specification (and implementation)? Note that safety specification in practice requires significant collaboration among the variety of players involved, including Original Equipment Manufacturers (OEMs), the spectrum of suppliers across various tiers, software and service providers, and others. Some aspects of the verification and validation can only be validated by the OEM responsible for the system on the vehicle level, and some can be validated by the supplier on the component level [22]. Additionally, some organizations provide ISO 26262 consultation, certification, and training for well-structured implementation of this standard. Furthermore, the goals and challenges can be different for individual players and may even be at odds. Here we provide a brief sketch of the different perspectives of the different players, to comprehend the cooperation, conflicts, and trade-offs involved.

3.1. OEM perspective

One of the main requirements for any OEM to be ISO 26262 compliant is to ensure that their supply chain is also compliant. They usually deal with tier 1 suppliers only and do not get involved with the tier 2, 3, or 4 layers. In the V-model, the OEM is responsible for system-level implementation. For instance, Jaguar Land Rover's Research and Technology department has over a hundred features in development aligned with the ISO 26262 standard at a system level. Some of these features interact with each other and this is where the safety-critical scenarios arise.

We now take a closer look at Jaguar's All Terrain Progress Control (ATPC) as an illustrative feature for functional safety. Woodley, J [23] discussed the ATPC system in a workshop to describe the challenges of implementing a complex distributed architecture in terms of functional safety. ATPC is a low-speed cruise control system that has a distributed architecture by design and has many interactions with other features where interactions are desirable, and designs are undesirable. It controls the vehicle speed by automatically modulating the engine and braking torque under the existing cruise control system.

The requirements for ASIL decomposition are an essential part of the beginning steps. It is essential to understand the failure mechanisms and consequences of the vehicular network communication (*e.g.*, CAN, LIN, FlexRay) between the ECU architectural elements. With the development of a safety plan, item definition, and implementation of HARA, the OEM derives potential hazards for the ATPC system. Here, the two potential hazards are unintended vehicle acceleration and deceleration. In general, the ATPC functionality is performed by the Powertrain Control Module (PCM) and the Anti-lock Braking System

Table 2. HARA analysis of MCU system

Failure	Operation	E	Reason	S	Reason	C	Reason	ASIL
Torque control	Vehicle moves forward	4	Pedestrians in front	2	>10% probability of AIS 3-6	3	>90 % of all traffic participants are able/ barely able to avoid harm	C
	Vehicle moves forward	4	City road	2	>10% probability of AIS 3-6	2	90 % or more of all traffic participants are able to avoid harm	B
	Turning; stopping	4	Stopping at light	2	>10% probability of AIS 3-6	2	90 % or more of all traffic participants are able to avoid harm	B
	Driving in reverse	2	Driving in reverse	1	>10% probability of AIS 1-6	1	90 % or more of all traffic participants are able to avoid harm	QM
	Evasive maneuver	2	Evasive maneuver	3	>10% probability of AIS 5-6	2	90 % or more of all traffic participants are able to avoid harm	A

(ABS) ECU. A high-level system architecture diagram for ATPC is shown in Figure 5.

- **ABS ECU requirements:** The vehicle acceleration induced by ATPC, is limited to a fully developed mean acceleration of 2.5 m/s^2, based on a four-wheel speed sensor [23]. The vehicle's active safety features, including ABS, Dynamic Stability Control (DSC), Roll Stability Control (RSC), Cornering Brake Control (CBC), and Electronic Traction Control (ETC), shall override the ATPC and generate positive or negative torque requests as required.
- **PCM ECU requirements:** The vehicle acceleration induced by ATPC, is limited to a fully developed mean acceleration of 2.5 m/s^2, based on gearbox output shaft [23]. If this acceleration level is breached, the PCM will fail to distribute torque requests and activate the DC fault mode.

The whole process follows a sequence of actions that involve (1) assessing the functional behavior of the interacting features, (2) determining compatibility with the system under development, (3) defining the design intent after evaluating which actuators are affected, (4) using the HARA method to determine the potential failure consequences related to ABS and PCM requirement compromises, and (5) deriving the requirements to reduce the identified hazards. Note that the technical safety requirements are obtained and implemented by the supplier regardless of whether the OEM finishes the above-mentioned actions or not. The big question here is whether the OEM is confident enough to find and reduce the corresponding hazards. The ISO standard provides such a safety concept, which is likely to change for different scenarios. The unintended attribute of both ABS and PCM can have a lower or higher threshold, resulting in an uncertain safety concept. These issues need to be addressed in the standard by including more case-specific information.

While reviewing electric vehicle powertrain technologies, Karamuk, M [24] summarized the OEM perspective on system-level problems related to functional safety. HARA analysis is one of the key responsibilities from the OEM end to establish safety goals for critical components like vehicle control unit (VCU), anti-lock braking, traction inverter, charging unit, electric power steering, high voltage (HV) battery, and CAN network. Following from that perspective, Li *et al* [25]. discussed the analysis and evaluation of the safety goals, and functional safety requirements of the motor control unit (MCU) system via HARA analysis performed by OEM. The goal of their safety design is to lower the risks of the relevant components by simulating various driving scenarios. The safety level can be determined by analyzing the MCU system in various scenarios using the three metrics *i.e.*, S, E, and C. The scene library is based on a specific evaluation of local special traffic conditions as described by ISO 26262 Hazard Analysis and Risk Assessment. Their functional safety HARA analysis of the MCU system is shown in Table 2. From this table, it can be derived that the highest level of safety is ASIL C. Therefore, the OEM combines the necessary safety goals based on ASIL C and passes on the next steps to the supplier. Note that this ASIL level is not definite enough and based on situational assumptions that might be susceptible to changes in the real-life scenario.

3.2. Supplier perspective

After the OEM goes through the complete functional safety system-level requirements, the supplier becomes responsible for technical safety requirements at the component level. By developing the E/E system at this level, a supplier will usually own a significant portion of the faults that can result in potential hazards. ISO 26262 work products and requirements result in System Safety Statements of Work (SOW) which include joint reviews of deliverables for both OEM and supplier for development monitoring. The

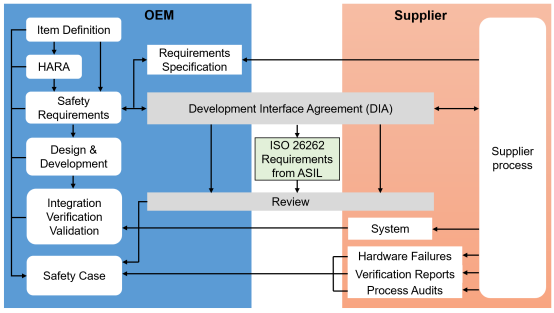

Figure 6. OEM supplier relation for functional safety.

content of SOW may consist of a safety plan, HARA, functional safety requirements, technical safety requirements, safety analysis (*e.g.*, component FMEA, FTA), proof of qualification of software tools, etc. The supplier needs to provide results of safety analysis, verification, and process audit reports as the OEM needs to determine if the design has introduced new failure modes. Agreements to give these are usually formalized in the Development Interface Agreement (DIA), which is stated as a part of the System Safety SOW. Fig. 6 depicts a simplified OEM-supplier relationship.

For the ATPC system discussed above, the supplier will be responsible for the technical safety requirements and implementation of software and hardware at the component level. They may work on the interactions of different features and the software components of both ABS and PCM to make sure that the safety goals are met. In most cases, the supplier traditionally develops the E/E system before OEM engagement [26] *e.g.*, developing the ABS functionality for any upcoming vehicle model by identifying the requirements years before the involvement of the OEM. Similarly, for the MCU system discussed earlier, the supplier would take responsibility for the technical safety requirements of software and hardware components in the MCU. A major challenge that the suppliers face is the lack of properly experienced functional safety personnel to help implement such a safety-critical system. The standard provides the structure of the safety plan but does not base it on practical engineering models. The supplier can enhance product reliability if the SOW and the component-level safety requirements are more integrated with a concrete engineering plan.

3.3. Certification provider perspective

Before the standardization of ISO 26262, project assessments used to depend solely on processes and work products. This resulted in undocumented processes without any proper structure and lengthy evaluations. Therefore, the need for early safety assessments emerged to establish a safety case with a defined structure and purpose. An initial functional safety assessment can identify weaknesses early on in the project life cycle, minimize cost and effort, and ensure a documented safety structure. Several well-reputed organizations provide an ISO 26262 assessment service where functional safety experts work closely with the OEM or supplier to meet safety requirements according to the standard by all means. Part of their assessment services includes GAP analysis, HARA, system safety assessment based on FMEA and FTA, assessment of both hardware and software development processes and analysis, elaboration of project documentation, interface management between OEMs and suppliers, etc.

A comprehensive range of certification and training for both IEC 61508 and ISO 26262 standards is available to be obtained through rigorous training, which provides a consistent framework for securing the functional safety of the vehicles in scope. Customized in-house training is also arranged to meet specific company requirements. The optional certification exam allows the engineers to obtain a Functional Safety Certified Automotive Engineer (FSCAE) designation. Overall, the organizations working on it are establishing the ISO standard's guidelines in the industry to some extent. However, there are differences in training structures from one organization to another that sometimes create confusion and disparity during implementation.

4. Emerging Challenges

Modern automotive systems will be equipped with autonomous driving features that not only *assist* humans in different aspects of driving but can even *obviate* the need for human involvement in navigating the vehicle through different driving environments. Along with various interfaces that provide connectivity to the internet, emerging automotive systems will be equipped with vehicular communication (V2X) capabilities. V2X forms a critical component in realizing advanced autonomous driving applications, by enabling dynamic information transfer among vehicular ad-hoc networks (VANETs). With the proliferation of connected autonomous vehicles (CAVs), functional safety has become increasingly challenging to achieve.

The safety requirements of CAVs differ from traditional automotive systems in various respects. Conventional risk assessment practices require significant updates to account for the evolving hazard spectrum resulting from increasing autonomy and connectivity.

4.1. Challenges due to Increasing Autonomy

CAVs rely heavily on accurate situational awareness through advanced sensor systems including lidars, cameras, radars, etc. Complex artificial intelligence (AI) algorithms are continuously fed high volumes of sensory data for making critical driving decisions. Safety considerations for modern autonomous vehicles expand beyond E/E system malfunctions. Unanticipated changes in weather conditions, unintended usage of the system function by the driver, and limitations in sensor performance may also lead to hazardous situations compromising the safety of the vehicle. For instance, an autonomous vehicle can face a hazardous situation when the onboard sensors fail to detect an icy road due to poor performance. If the vehicle continues driving at higher speeds on such a road, it could skid and lose control. Moreover, validating the complex deep learning and statistical signal processing software is challenging due to the non-deterministic behavior involved. Traditional functional safety does not explicitly account for such scenarios as it only recognizes unreasonable risk due to hazards caused by the E/E system malfunction. However, there are various independent safety assessment tests (*e.g.*, Euro NCAP), that complement these standards by providing a broader, consumer-focused assessment of vehicle safety that includes the performance of components like sensors in real-world scenarios. Euro NCAP's safety assessment tests serve as a reliable indicator for vehicle crash safety, focusing on severe or fatal injuries in car-to-car collisions. Studies show cars with higher Euro NCAP ratings (three or four stars) are about 30% safer than those with lower ratings or no rating, highlighting the correlation between Euro NCAP scores and reduced injury risk [27].

4.2. Challenges due to Connectivity

Automotive systems are typically equipped with a head unit that enables connectivity to the internet (*i.e.*, WiFi and/or mobile broadband) and a radio transceiver. Additionally, modern CAVs will be equipped with specialized transceivers supporting vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in VANETs [28]. Several emerging autonomous driving applications, such as platooning, cooperative collision detection, dynamic route management, smart intersection management, etc., rely on V2X communication to make real-time driving decisions. The safety of the underlying vehicle engaging in such autonomous driving applications can be compromised if V2X communication is unreliable, intermittent, or corrupted. Furthermore, V2X communication, along with the conventional interfaces can be subjected to security attacks that can directly cause a safety threat to the vehicle. The vehicle can be misled into making unsafe driving decisions through malicious V2X messages or can be hacked by an adversary, forcing it to cede control of the vehicle. Hazard analysis can become increasingly challenging under such considerations. It is critical to have holistic safety engineering and validation approaches that account for the reliability and security aspects of the communication channels simultaneously.

5. Limitations in Current Practice

5.1. Caveats in Safety Standards

5.1.1. Inadequate Guidelines for CAV Safety: Traditional functional safety standards (*i.e.*, IEC 61508 or ISO 26262 standards) recognize functional safety in the context of unreasonable risk due to hazards caused by E/E system malfunction. However, it becomes insufficient in the context of modern CAVs. Hazardous situations in CAVs can stem from a combination of several factors extending beyond E/E system malfunctions. These factors include loss in connectivity or corrupted communication, sensor system performance limitations, unintended use by the driver, etc. Conventional safety standards do not provide sufficient guidance for safety engineering practices and validation approaches that address the broader functional safety paradigm of modern CAVs.

5.1.2. Open-ended Safety Definition and Process Guidelines: Safety standards define automotive functional safety as the absence of unreasonable risk due to hazards caused by the malfunctioning behavior of E/E systems. However, this definition includes terms such as 'unreasonable risk' that are subjective and contextual. The standards do not provide a formal and scientific interpretation of functional safety that can be adopted unambiguously by automotive design and safety engineers. The HARA methodology, which is fundamental to the functional safety concept, is often

ambiguous and open to interpretation. However, there is no formal procedure spelled out in the standards that ensures the comprehensiveness and accuracy of hazard analysis in practice. Due to these inherent caveats, mere compliance with safety standards may not always guarantee the functional safety of the vehicles.

5.2. Limitations in Industry Practices

5.2.1. Ad-hoc Automotive System Validation: In the current industry, state-of-the-art validation procedures are not fully systematic. It is done very late in the product development life cycle, not considering all the standardized hardware and software safety requirements. Moreover, time-to-market and cost constraints affect the validation process, leading to complex problems and safety-critical scenarios. It is carried out just before the functional safety evaluation, at the end of the development process. Typical validation activities like validation testing, safety FMEA, FTA, etc. are either not done in a standardized manner or performed with missing processes in between.

5.2.2. Unformed Safety Engineering Practices: Functional safety is treated more like a clerical or legal issue than an engineering problem. Safety engineering is often an afterthought, whereas there is a greater likelihood of detecting hotspots and achieving the ASIL goals if functional safety analysis is performed early in the design cycle. A greater emphasis on safety standards is required to establish them throughout the significant automotive industries, starting from tier-3 suppliers to OEMs.

5.2.3. Security Vulnerabilities Compromising Safety: There has been in a way limited focus on designing secure systems by following the safety standards in the industry, thus conventional security practices are reactive. Security and safety policies are often developed in silos not accounting for co-analysis methods. In order to ensure that both safety and cybersecurity concerns are taken into account, co-analysis at the concept phase must ensure that interactions between various concerns are taken into account. Because previously unidentified attacks may have the potential to jeopardize functional safety, highly connected vehicles require a way to monitor the security status throughout the course of their existence [29].

6. Impact of Limitations and Emergent Standards

Addressing the limitations in current safety practices is obviously an active — and vast — area of research. A thorough exploration of the entire spectrum of safety research will take us far afield. However, it is worth exploring the impact of safety and its interplay with autonomy on security on the different safety standards. Here we briefly touch upon that specific topic.

6.1. Impact of Autonomous Vehicles

ISO/PAS 21448:2019 is developed in conjunction with ISO 26262, addressing the safety requirements of modern autonomous vehicles. This standard focuses primarily on guaranteeing the Safety of Intended Functionality (SOTIF) in the absence of system failure [30]. ISO 21448 proposes the design, verification, and validation practices that autonomous vehicle developers can adopt to guarantee SOTIF in their systems. While ISO 26262 continues to apply to well-studied E/E systems such as airbags or electronic stability control (ESC), the SOTIF standard comes into play for ADAS and emerging autonomous applications that rely on advanced sensors and complex AI for situational awareness and decision-making. The standard utilizes the same vocabulary and methods defined in ISO 26262 but focuses on intended functionality. Therefore, the SOTIF standard, in combination with ISO 26262, allows the developers of autonomous driving to adopt more comprehensive hazard analysis and threat modeling techniques. System verification will be extended to include fine-grained virtual simulations of the driving environments and road conditions. This allows for a systematic account of hazardous events that stem from performance limitations of sensors or systems, and unanticipated changes in weather conditions.

ANSI/UL 4600 Standard was developed to address the safety requirements of fully autonomous mobility systems such as self-driving cars [31]. The primary focus of the standard is to guide the designers to make a concrete goal-based safety case for their autonomous systems. The standard offers principles and methods for evaluating safety-critical autonomous systems, on their ability to perform safely as intended without human intervention. It sheds light on the reliability aspects of the software and hardware systems necessary for AI algorithms and sensors. The standard recommends design practices and evaluation methods that remain agnostic to the underlying technology

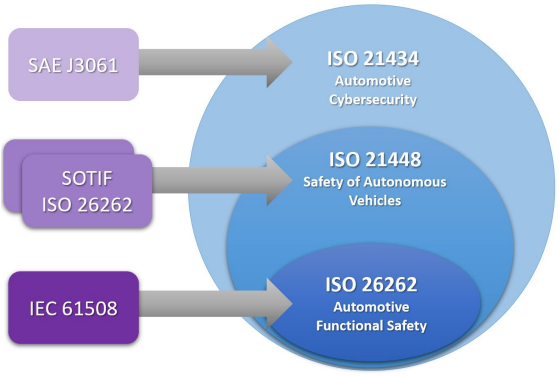

Figure 7. Relationship of road vehicle standards.

and tools used by autonomous vehicle developers. It presents itself as an agile alternative to the existing incarnations of inflexible safety regulations.

The combined safety standard, *i.e.*, ISO 26262 + ISO 21448 + UL 4600, is a promising step toward improving the functional safety of autonomous vehicles. However, like most other existing standards, this enhanced standard can only provide high-level guidelines for the development and testing of autonomous vehicles. The onus remains on the developer community to interpret the standard and derive best practices and design methodologies that effectively obey the proposed safety guidelines.

6.2. Safety with Cyber Security

Automotive companies and policymakers use functional safety to ensure safe driving conditions. However, with the increased development of cyber-physical systems, wireless interfaces, and embedded systems, it has become essential to address the cybersecurity of automobiles associated with safety. Today's autonomous vehicles have numerous communication interfaces, which are preferred targets for attackers. They employ a range of attack methods, such as mobile apps, Bluetooth, WiFi, telematics, and keyless entry systems [32]. In order to address this problem, the Society of Automotive Engineers (SAE) released the cybersecurity guidebook for electronic vehicle systems (SAE J3061) [33]. The 2018 edition of ISO 26262 acknowledges cybersecurity as an essential part of functional safety, thereby pointing out the necessity for establishing a correlation between functional safety and cybersecurity [3]. Additionally, security standards like ISO/WD 4398 for guided transportation service planning and ISO 14815:2005 for automatic vehicle identification can lead to products that inherently conform to best practices [34].

However, an integrated cyber-security standard must be considered to counter such attacks on communication interfaces and that is why the automotive cybersecurity standard ISO/SAE 21434 was released in 2021. Note that the document describes the requirements for cybersecurity risk management, not any specific technology or solutions related to cybersecurity [35]. Fig. 7 depicts the relationship of three corresponding standards for road vehicles and their sources of derivation. The ISO 21448 standard will be outside the scope of ISO 26262 and the ISO/SAE 21434 standard for cybersecurity will be outside the scope of ISO 21448 *i.e.*, SOTIF.

7. Conclusion

As electronics and software continue to proliferate in vehicular systems, functional safety is becoming a topic of paramount concern. On the other hand, safety implications and the interplay of safety with technology are becoming increasingly obscured with a plethora of standards, design guidelines, certification needs, etc. In this paper, we have provided an overview of the trends in functional safety for current and emergent automotive systems, roles of standards, and methodologies and approaches to implement safety features from the perspective of various players in the complex supply chain involved in the development of vehicular systems. We believe that this treatment will help disentangle the challenges and complexity involved in functional safety, resulting in a demystification of the need, facilitating understanding of the state of the practice, and paving the way for future research.

REFERENCES

1. D. Kenjić and M. Antić, "Connectivity challenges in automotive solutions," *IEEE Consumer Electronics Magazine*, vol. 12, no. 5, pp. 53–59, 2023.
2. C. Miller, "Lessons learned from hacking a car," *IEEE Design & Test*, vol. 36, no. 6, pp. 7–9, 2019.
3. G. Xie, Y. Li, Y. Han, Y. Xie, G. Zeng, and R. Li, "Recent advances and future trends for automotive functional safety design methodologies," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 5629–5642, 2020.
4. B. B. Y. Ravi, M. R. Kabir, N. Mishra, S. Boddupalli, and S. Ray, "Autohal: An exploration platform for

ranging sensor attacks on automotive systems," in *2022 IEEE International Conference on Consumer Electronics (ICCE)*, 2022, pp. 1–2.

5. S. Chung, "Interface-driven customer experience: Redefining user interface (ui) design for automotive infotainment system," *IEEE Consumer Electronics Magazine*, vol. 12, no. 1, pp. 12–20, 2022.
6. F. Simonot-Lion and Y. Trinquet, "Vehicle functional domains and requirements." CRC Press, 2023, ch. 1, pp. 1–30.
7. H. Koptez, "Real-time systems: design principles for distributed embedded applications," *Kluwer Academic Publisher*, 1997.
8. U.S. Department of Transportation, "NHTSA Recalls by Manufacturer," https://datahub.transportation.gov/Automobiles/NHTSA-Recalls-by-Manufacturer/mu99-t4jn, Accessed: 2024-03-21.
9. J. Brill, "U.s. product recalls hit four-year high in first quarter of 2023," *Quality Assurance & Food Safety*, May 2023. [Online]. Available: https://www.qualityassurancemag.com/news/us-product-recalls-hit-four-year-high-in-first-quarter-of-2023/
10. S. Brown, "Overview of iec 61508. design of electrical/electronic/programmable electronic safety-related systems," *Computing Control Engineering Journal*, vol. 11, no. 1, pp. 6–12, 2000.
11. R. Bell, "Introduction to iec 61508," in *ACM International Conference Proceeding Series*, vol. 162, 2006, pp. 3–12.
12. G. Xu, G. Liu, X. Jiang, and W. Qian, "Effect of pitch down motion on the vortex reformation over fighter aircraft," *Aerospace Science and Technology*, vol. 73, pp. 278–288, 2018.
13. Flaps 2 Approach, "Ground Effect - Historical Perspective & Technical Explanation," October 2012, [Online; accessed 23-04-2024]. [Online]. Available: https://www.flaps2approach.com/journal/2012/10/8/ground-effect-historical-perspective-technical-explanation.html
14. A. Ismail and W. Jung, "Research trends in automotive functional safety," in *2013 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (QR2MSE)*. IEEE, 2013, pp. 1–4.
15. P. Kafka, "The automotive standard iso 26262, the innovative driver for enhanced safety assessment & technology for motor cars," *Procedia Engineering*, vol. 45, pp. 2–10, 2012.
16. *ISO 26262 "Road Vehicles – Functional Safety"*. International Organization for Standardization, 2011.
17. S.-H. Jeon, J.-H. Cho, Y. Jung, S. Park, and T.-M. Han, "Automotive hardware development according to iso 26262," in *13th International Conference on Advanced Communication Technology (ICACT2011)*. IEEE, 2011, pp. 588–592.
18. S. Burton, J. Likkei, P. Vembar, and M. Wolf, "Automotive functional safety= safety+ security," in *Proceedings of the First International Conference on Security of Internet of Things*, 2012, pp. 150–159.
19. Synopsys, "What is iso 26262 functional safety standard?" https://www.synopsys.com/automotive/what-is-iso-26262.html, 2024, accessed: 2024-03-22.
20. C. A. Hobbs and P. J. McDonough, "Development of the european new car assessment programme (euro ncap)," *Regulation*, vol. 44, no. 3, pp. 2439–2453, 1998.
21. U. Z. A. Hamid, F. R. A. Zakuan, K. A. Zulkepli, M. Z. Azmi, H. Zamzuri, M. A. A. Rahman, and M. A. Zakaria, "Autonomous emergency braking system with potential field risk assessment for frontal collision mitigation," in *2017 ieee conference on systems, process and control (icspc)*. IEEE, 2017, pp. 71–76.
22. K. Beckers, I. Côté, T. Frese, D. Hatebur, and M. Heisel, "A structured and systematic model-based development method for automotive systems, considering the oem/supplier interface," *Reliability Engineering and System Safety*, vol. 158, p. 172–184, 2017.
23. "An OEM's Perspective on ISO 26262," 2015. [Online]. Available: http://www.iqpc.com/media/1001640/44136.pdf
24. M. Karamuk, "Review of electric vehicle powertrain technologies with oem perspective," in *2019 International Aegean Conference on Electrical Machines and Power Electronics (ACEMP) 2019 International Conference on Optimization of Electrical and Electronic Equipment (OPTIM)*, 2019, pp. 18–28.
25. H.-P. Li and Y.-w. Li, "The research of electric vehicle's mcu system based on iso26262," in *2017 2nd Asia-Pacific Conference on Intelligent Robot Systems (ACIRS)*. IEEE, 2017, pp. 336–340.
26. J. Birch, R. Rivett, I. Habli, B. Bradshaw, J. Botham, D. Higham, P. Jesty, H. Monkhouse, and R. Palin, "Safety cases and their role in iso 26262 functional safety assessment," in *International Conference on Computer Safety, Reliability, and Security*. Springer, 2013, pp. 154–165.
27. A. Lie and C. Tingvall, "How do euro ncap results correlate with real-life injury risks? a paired

comparison study of car-to-car crashes," *Traffic injury prevention*, vol. 3, no. 4, pp. 288–293, 2002.

28. A. Lautenbach, *On Cyber-Security for In-Vehicle Software*. Chalmers Tekniska Hogskola (Sweden), 2017.
29. R. Bramberger, H. Martin, B. Gallina, and C. Schmittner, "Co-engineering of safety and security life cycles for engineering of automotive systems," *ACM SIGAda Ada Letters*, vol. 39, no. 2, pp. 41–48, 2020.
30. A. Schnellbach and G. Griessnig, "Development of the iso 21448," in *European Conference on Software Process Improvement*. Springer, 2019, pp. 585–593.
31. P. Koopman, U. Ferrell, F. Fratrik, and M. Wagner, "A safety standard approach for fully autonomous vehicles," in *International Conference on Computer Safety, Reliability, and Security*. Springer, 2019, pp. 326–332.
32. V. K. Kukkala, S. V. Thiruloga, and S. Pasricha, "Roadmap for cybersecurity in autonomous vehicles," *IEEE Consumer Electronics Magazine*, vol. 11, no. 6, pp. 13–23, 2022.
33. SAE International, "Cybersecurity guidebook for cyber-physical vehicle systems," SAE Standard J3061, January 2016. [Online]. Available: https://www.sae.org/standards/content/j3061_201601/
34. M. K. Khan and A. Quadri, "Augmenting cybersecurity in autonomous vehicles: Innovative recommendations for aspiring entrepreneurs," *IEEE Consumer Electronics Magazine*, vol. 10, no. 3, pp. 111–116, 2020.
35. "Road vehicles - cybersecurity engineering iso/sae dis 21434," 2020. [Online]. Available: https://www.sae.org/standards/content/iso/sae21434.d1/

Md Rafiul Kabir is a Ph.D. student at the Department of Electrical and Computer Engineering, University of Florida. Before that, he was an Electrical Engineer at Horizon Global Americas in Michigan, where he worked in the design and development of OEM Trailer Brake Controllers used in automobiles. Prior to that, he got his MSc degree in Electrical Engineering from the University of Toledo. He received his B.Sc. degree in Electrical and Electronic Engineering from Ahsanullah University of Science and Technology, Dhaka, Bangladesh. Rafiul's current research interests are digital twins, automotive security, and IoT applications.

Srivalli Boddupalli received the B.Tech. degree from the Chaitanya Bharathi Institute of Technology, Hyderabad, India, in 2016, and both M.S. and Ph.D. degrees from the University of Florida, Gainesville, FL, USA, in 2022, with a focus on developing security architectures using machine learning techniques for connected vehicle applications. Her research interests include automotive security and intelligent transportation systems.

Atul Prasad Deb Nath received a B.Sc. degree from the Khulna University of Engineering and Technology (KUET), Khulna, Bangladesh, in 2011, the M.Sc. degree from the University of Toledo, Toledo, OH, USA, in 2016, and the Ph.D. degree from the University of Florida, Gainesville, FL, USA, in 2021, with a focus on investigating major aspects of SoC security and developing novel architectural features against various adversarial models. His research interest includes system-on-chip (SoC) platform security and CAD for security and trust.

Sandip Ray is a Professor at the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL, where he holds an Endowed IoT Term Professorship. Before that, he was a Senior Principal Engineer at NXP Semiconductors, and prior to that, Research Scientist with the Intel Strategic CAD Laboratories. Dr. Ray's current research targets correct, dependable, secure, and trustworthy computing through the cooperation of specification, synthesis, architecture, and validation technologies. He is the author of 3 books and over 100 publications in international journals and conferences. He has also served as a Technical Program Committee Member of over 50 international conferences, as Program Chair of ACL2 2009, FMCAD 2013, and IFIP IoT 2019, as Guest Editor for IEEE Design and Test, IEEE TMSCS, and ACM TODAES, and as Associate Editor of Springer HaSS and IEEE TMSCS. Dr. Ray has a Ph.D. from the University of Texas at Austin and is a Senior Member of IEEE.