

RESEARCH ARTICLE

Framework for Development of Trustworthy Cyber-Physical Vehicle Systems

Prathik Menta Praveen Kumar^{1,a}, Ion Barosan^{2,*}, Avinash Varadarajan^{1,b}¹*BRACE Automotive B.V., Eindhoven, The Netherlands*²*Eindhoven University of Technology, Eindhoven, The Netherlands*^a*Email: prathik.menta.praveen.kumar@brace-automotive.com*^b*Email: avinash.varadarajan@brace-automotive.com***ABSTRACT**

Modern automotive system design requires a revised development technique, motivated by substantial progress in vehicle capabilities. This article examines critical system-level factors relevant to cyber-physical vehicle systems, emphasizing the concept of trustworthiness. Establishing a reliable relationship between users and automobiles is increasingly essential, particularly in the area of autonomous driving systems, where trust drives the implementation of secure systems. The research suggests improvements to the current development framework by presenting approaches for identifying, integrating, evaluating and documenting essential trustworthiness elements throughout the development lifecycle. The data collected through this approach aids in system certification efforts, according to both existing and forthcoming regulatory standards. Research indicates that the suggested modifications to traditional development methodologies may significantly enhance user trust and acceptance of automated vehicle technology.

ARTICLE DATA**Article History**

Received 2 October 2024

Revised 2 June 2025

Accepted 5 September 2025

Keywords

Development

Trust

Trustworthiness

Safety

Security

Privacy

Cyber-physical systems

ADAS

ADS

V-cycle

1. INTRODUCTION

The importance of automotive electronics has increased significantly in recent years, driven by the need for safer and more efficient automobiles. In the 1980s, Electronics/Electrical (E/E) components represented only 10% of a vehicle's production expenses. By 2010, this percentage had risen to roughly 35% [1]. Original Equipment Manufacturers (OEMs) anticipate that by 2030, these costs will constitute up to 50% of the total manufacturing expenditures. This escalation is driven mainly by OEM commitment to investing in new technologies, motivated by four critical trends in the automotive sector: electrification, connected vehicles, autonomous driving and active safety [2]. These changes are expected to significantly increase the need for vehicle electronics and software in the next decade. Over the past fifty years, OEMs have progressively

incorporated cyber-physical systems into automobiles to meet these advancing technological demands.

Automated driving represents a transformative technology that profoundly impacts the development of future mobility. Advanced Driver Assistance Systems (ADAS), which are fundamentally dependent on cyber-physical systems, enable the performance of automated driving functions and activities. Historically, vehicle operations were limited to producing reliable responses to user inputs specified. In conventional manual driving, the driver is responsible for perception, decision-making and planning, while the car performs actuation based on these inputs. However, the emergence of machine learning models has enabled increasingly advanced autonomous driving systems (ADSs) to autonomously perform cognitive, decision-making and planning tasks related to driving. The

*Corresponding author. Email: i.barosan@tue.nl

transition of primary driving responsibilities from the driver to the vehicle system requires the development of trust between these parties, essential for user acceptance.

The trust connection between the driver and the system is profoundly affected by their respective trustworthiness characteristics or attributes [3,4]. Trust is fundamentally subjective and resists quantification or standardization. Trust levels can be deduced from behavioral consequences, as direct measurement of trust is impractical. Moreover, trust is characterized as bidimensional, asymmetric, context-dependent and dynamic [5]. User trust materializes when the user endorses the system's decisions and its role within the driving environment. Conversely, the ADS is considered to trust the user when the user behaves ethically and complies with the system's guidelines, thus avoiding misuse or manipulation. Trust can be conceptualized on two primary dimensions: competence and integrity [6]. A trust relationship involves two parties, as illustrated in Fig. 1, where the trustor (the trusting party) places trust in the trustee (the trusted party). Due to its universal applicability, trust extends to human-machine interactions. Trust assumes critical importance in scenarios characterized by uncertainty or risk, particularly when the outcomes are of significant value to the trustor. In autonomous driving, a dynamic trust relationship evolves between the user and the system.

The dynamic of evolving dependency between the driver and the vehicle is captured in the Fig. 2. Historically, OEMs and standardization organizations have focused on creating reliable automotive systems that continuously exhibit high performance. However, with the emergence of advanced degrees of ADS, vehicles face significant technical obstacles, particularly in navigating complex interactions with non-autonomous vehicles, vulnerable road users and passengers. These issues are compounded by the need for exact localization and scene comprehension, updated infrastructure, and the development of strong control and path planning algorithms suitable for highly changeable situations [7]. In addition to technical challenges, autonomous vehicles encounter considerable social obstacles such as protecting fundamental rights, addressing data privacy concerns and ensuring consumer acceptability. These complex issues highlight the intrinsic bidirectional dependency between the user and the vehicle. Therefore, OEMs carry the substantial obligation to secure the confidence of users, regulatory authorities and other stakeholders in the advancement of future Automated Driving Systems (ADS). As a result, conceptualising the trustworthiness of cyber-physical systems, such as ADS, is essential for understanding their role in establishing trust with users.

The development framework and methodology for generating a new product must incorporate the expanded

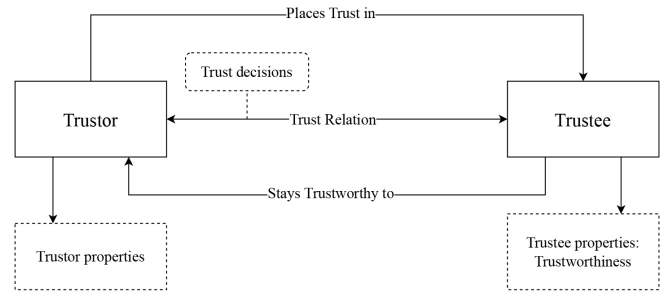


Figure 1. Relationship between a trustor and a trustee.

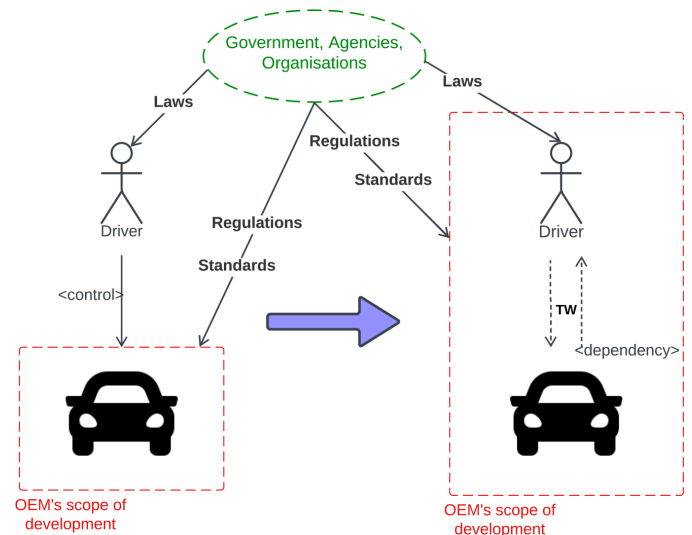


Figure 2. Underlying problem in trust relationship.

scope to establish trustworthy systems and ensure reliable users. The present study aims to explore a framework for the development of reliable cyber-physical vehicle systems. The modified approach aims to assist system developers in recognizing, integrating and assessing the relevant trustworthiness attributes of cyber-physical vehicle systems. A comprehensive framework can facilitate compliance with the requisite norms and standards of the systems. Adherence to standards, regulations and laws will predominantly influence the trust relationship, as these compliance requirements dictate the behavior of both the vehicle and the user on roads. Compliance serves as an effective mechanism for establishing trust and confidence among stakeholders. Compliance and certification enhance an organization's dedication to quality and reliability, resulting in sustained success and a distinctive market position.

Compliance regulations and standards directly influence the development of OEMs, Tier 1 suppliers, Tier 2 suppliers and future tiers of the supply chain. Attaining prescribed compliance requires adherence to norms and standards at all levels of the supply chain. The gap analysis underscores existing norms and regulations in the EU region. The European Commission amended the General Safety Regulation on 27 November 2019,

which became effective on 6 July 2022. The modification implemented a variety of mandatory Advanced Driver Assistance Systems (ADAS) features, including speed assistance, reverse detection and driver attention warnings, to improve road safety. The regulation established the legislative foundation for the approval of methods of development and technical standards for autonomous and automated vehicles. These constituted the initial global regulations for fully autonomous vehicles functioning in Level 4 automation, including urban shuttles and robotaxis. The EU regulations established the rules, specifically EU R32022R2236 and EU R32022R1426 [8]. The implementing regulation R32022R1426 includes testing protocols, cybersecurity standards, data recording guidelines, safety performance oversight and incident reporting obligations for OEMs manufacturing highly automated vehicles. The EU Commission collaborates with the Economic Commission of the United Nations for Europe (UNECE) to implement legislation for Level 3 Advanced Driver Assistance Systems (ADAS) used on motorways. The World Forum for Harmonization of Vehicle Regulations (WP.29) established by UNECE has developed a framework encompassing subjects such as Automated Commanded Steering Function (ACSF) and cybersecurity, as well as software upgrades (Over the Air, OTA).

The absence of explicit standards and regulations designed to address the increased capabilities of Autonomous Driving Systems (ADS) presents major obstacles to the development of compliant systems throughout the supply chain. Changing the law to include higher levels of ADS would improve and advance road safety, especially for autonomous vehicles [9]. Although current legislation generally addresses autonomous systems, there is a significant lack of particular legal frameworks for developing functionalities such as Level 3 Traffic Jam Chauffeur, Level 4 Automated Valet Parking and Level 3 Highway Pilot. The European Commission, in conjunction with relevant working groups, is actively reviewing existing laws and developing new ones for highly automated cars. This continuous effort underscores a notable regulatory deficiency between forthcoming ADAS capabilities and current legislation. Therefore, it is essential that the ADS development framework integrates a systematic and organized approach to both development and validation to guarantee the creation of reliable autonomous vehicles.

This article is organized as follows. Section 2 introduces the concepts of trust and trustworthiness in the context of automotive systems, providing a brief overview of the key attributes of trustworthiness pertinent to these systems. Section 3 details the development processes employed within the proposed framework, which extends the traditional V-model development cycle, to improve trustworthiness. The effectiveness

of this framework is demonstrated through an example, discussed in Section 4. The study conclusions and insights derived from the demonstration are presented in Section 5. Recommendations for future research are described in Section 6.

1.1. Research Questions

The research centers on identifying properties that strengthen the trust relationship and enhance trustworthiness in vehicle systems. Upon determining these properties, the challenge extends to developing strategies for their integration into existing or new development processes. Consequently, the following research questions have been formulated to guide the investigation appropriately.

- Question 1 (RQ1): What are the essential characteristics that define trust-worthiness in automotive systems?
- Question 2 (RQ2): What constitutes a comprehensive development framework that can effectively ensure trustworthiness in automotive systems?
- Question 3 (RQ3): What evaluation methods can be established to assess the trustworthiness of automotive systems?

2. TRUST AND TRUSTWORTHINESS

2.1. Overview of Trustworthiness

The bi-directionality of trust fundamentally represents a reciprocal and dynamic relationship between a trustor (user) and a trustee (system), characterized by the trustor's ongoing assessment of the trustee's trustworthiness. To further elucidate this trust dynamic, it is instructive to examine its manifestations from both the system and user perspectives, as well as their mutual dependence and interaction. The following sections detail these aspects, providing insight into the multifaceted nature of trust within automotive systems.

- **System Aspect.** The trustworthiness of the system can be quantified through rigorous testing and validation processes that evaluate the adherence to established safety and performance metrics. Systems must be engineered to handle both anticipated and unforeseen scenarios reliably. The trust placed in the system by the user is predicated on the user's risk assessment and the system's demonstrated reliability in fulfilling its operational commitments.
- **User Aspect.** Trustworthiness from the user's perspective varies significantly, influenced by the subjective nature of human factors such as mood, fatigue and

situational awareness. Key strategies for enhancing user trust include educating users, improving system interfaces and refining the interaction between users and automotive systems to ensure that users can both trust and effectively operate these systems.

- **Mutual Dependence and Interaction.** The decision to trust by the trustor (user) is based on their expectations and the perceived attributes of the trustee (system), which collectively define its trustworthiness. Violations of trust by either party can severely damage the trust relationship. Therefore, enhancing trustworthiness requires a dual focus on both system reliability and user behavior. This balanced approach is essential to ensure that both parties fulfil their mutual expectations, thereby maintaining a strong trust relationship.

The dynamics of trust and trustworthiness detailed in the initial discussion set the stage for a deeper exploration of the relationship between the trustor and trustee within automotive systems. The trustworthiness of the trustee plays a critical role in determining the level of trust that the trustor can gain. Simply put, the greater the trustworthiness of the trustee, the more it merits the trustor's confidence. Fig. 1 presents a model that illustrates how a trust relationship is formed. The trustor's decision to trust is influenced by their expectations and trustee risk assessment, with the trustor's own characteristics also playing a significant role in this decision-making process. Once trust is bestowed on the trustee, it is imperative that the trustee meet the trustor's expectations or fulfill the terms of their agreement. Any breach of this agreement can significantly damage the trust relationship due to unmet expectations and often, once trust is compromised, it is challenging to fully restore it.

This decision-making process is heavily influenced by the attributes of the trustee, which define its trustworthiness. The concept of trustworthiness is aptly summarized in Nazila Gol Mohammadi's book *Trustworthy Cyber-Physical Systems*, where it is defined as *"The quality of a system that provides assurance that the cyber-physical system will perform as expected or meet the required standards."*

However, in the context of cyber-physical vehicle systems, trustworthiness encompasses both the system and the user, each playing an integral role in establishing and maintaining trust. The discussions on trustworthiness, therefore, integrate the system's capabilities and the user's reliability into a unified framework. This approach addresses the dual nature of trust in automotive systems, recognizing the critical contributions of both elements to the overall trust ecosystem.

Furthermore, the exploration of trust in automotive systems will include a detailed examination of the following

definitions and attributes of trustworthiness specific to the automotive context.

- **System Trustworthiness:**

"Trustworthiness of an automotive system refers to the quality of the system to perform its intended functions consistently and correctly, ensuring that overall safety is maintained throughout its operation. The quality of a system ensures that the cyber-physical system will perform as expected or meet the required standards. This involves predictable behavior under similar conditions, adherence to safety and performance standards, and reliability over time."

- **User Trustworthiness:**

"The Trustworthiness of a user in the context of interacting with automotive systems refers to the user's ability to interact consistently with the system safely and predictably. This depends on the user's understanding of the system, adherence to operational guidelines, and avoidance of misuse or manipulation."

In the above definitions, the term "system" may implicitly refer to the entire vehicle or any individual systems within it. Automotive systems encompass both automated driving systems and driver assistance systems. To earn the user's trust, these systems must be developed with a focus on trustworthiness. Trust is subjective, which implies that two users may perceive different levels of trust towards the same system. Dynamic levels of trust depend greatly on age, gender, level of driving experience, history with automated systems, background, or specific conditions at hand [5]. However, the current study limits the scope to system properties and does not highlight user trust properties. Trustworthiness can be further examined to identify some of the key properties highlighted in Nazila Gol Mohammadi's book *Trustworthy Cyber-Physical Systems* [3]:

- **Objective.** When the system is trustworthy, the system produces the same results whenever tested under similar conditions. Moreover, the trustworthiness of a system does not depend on the level of trust of the users. Therefore, trustworthiness attributes are provided to help users make informed decisions about whether they can rely on the system to deliver satisfactory results.
- **Proportional to effort and investment.** More guided efforts and monetary investments lead to better system development to meet user expectations or requirements. For example, standards that can improve trustworthiness may require additional processes to be performed. This addition can imply an extended timeline and expenses to account for the workload.

- *Dynamic.* Trustworthiness is not constant. To maintain trustworthiness, developers/manufacturers need to continuously service and update the system over time to ensure the system works as intended.
- *Trade-off.* The attributes that contribute to trustworthiness are often contradictory. In other words, if one attribute increases, the other may be negatively impacted. Hence, a conscious trade-off has to be considered to keep the system attributes situated for the context.

The determination to rely on systems or users depends on their trustworthiness, influenced by particular qualities. These features serve as indications of the system's or user's characteristics that profoundly influence trust. Each quality trait can be measured using a metric to objectively assess trustworthiness. The trustee's reliability serves as an indicator of the trustor's contentment, assessed by the extent to which the trustee fulfils these quality standards.

2.2. Trustworthiness Attributes of Cyber-Physical Vehicle Systems

In this study, the trustworthiness of the system is a focal point, with a specific emphasis on system development processes. The attributes defining the trustworthiness of a cyber-physical system are shaped by the domain of application, which may include sectors such as medical, automotive, home automation, or aerospace. Therefore, trustworthiness is inherently context-dependent. The Industrial Internet Reference Architecture (IIRA) identifies five principal attributes that contribute to trustworthiness: safety, security, reliability, resilience and privacy [10]. Furthermore, the book *Trustworthy Cyber-Physical Systems* conducted a thorough literature review to investigate trustworthiness attributes [3]. This review encompassed an analysis of a wide range of sources, including research articles, developer reports, scientific

journals and workshop proceedings, with the aim of categorizing characteristics and qualities of cyber-physical systems that impact trustworthiness. From this analysis, thirteen key attributes pertinent to software-centric systems were delineated: safety, security, compatibility, configuration quality, compliance, privacy, cost, data quality, dependability, performance, usability, correctness/accuracy and complexity [3]. Of these, security, dependability, usability and safety emerged as particularly critical for cyber-physical systems.

In 2020, the EU Commission established seven fundamental criteria for evaluating Trustworthy AI, encompassing human agency, technical performance, safety, privacy, data governance (security) and transparency, among others [11]. User acceptability is closely related to usability and safety, which are essential to cultivating trust among users [12]. In addition, numerous traits can be categorized into more detailed subdivisions. Security can be categorized into confidentiality, accountability, integrity and auditability, while dependability includes availability, fault tolerance, robustness, reliability, scalability and maintainability. The specificity of these sub-categories is customized to the distinct attributes of the system being developed.

Considering that ADS is a pivotal cyber-physical system within the automotive sector, its pertinent system qualities were delineated to illustrate dependability. Seven critical system attributes were identified as significantly influencing the dependability of automotive systems. The mutually inclusive set of qualities identified in the numerous study publications mentioned above served as the basis for these seven characteristics. Fig. 3 demonstrates the aggregate contribution of these seven attributes to the overall trustworthiness of cyber-physical vehicle systems. The trustworthiness attributes in automotive systems are as follows:

1. **Safety.** The ability of the system to operate without any unreasonable risk of harming or causing

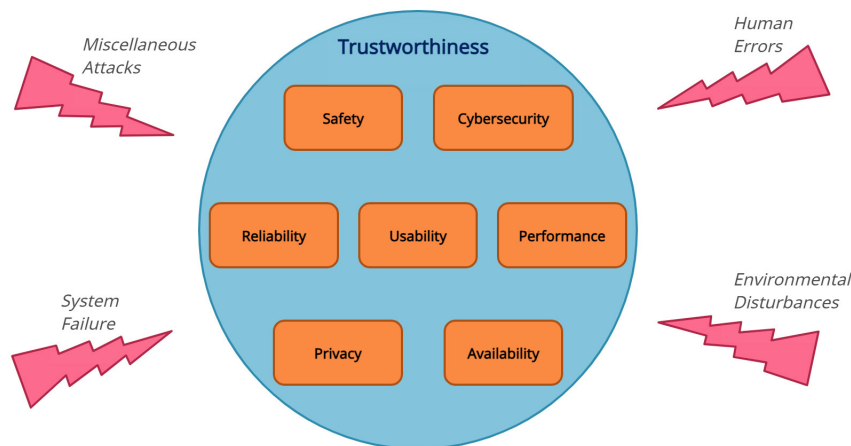


Figure 3. Trustworthiness attributes of cyber-physical vehicle systems.

the system's capacity to operate without causing any unnecessary risk of harm or damage to human users, property, or the environment [10]. The dangers may originate from hazardous events resulting from either system malfunction or environmental influences. The malfunction of system components will result in the system encountering dangerous events that may cause injury. Nevertheless, the system may encounter hazardous situations when the operational environment exceeds its capabilities or when environmental elements interfere with its performance. This attribute is essential when considering elevated levels of automation, as the system assumes vital driving responsibilities and sensing, diminishing the driver's role in monitoring these activities. Standards like Functional Safety (FuSa) and Safety for Intended Function (SOTIF) are employed to prevent the system from encountering hazardous scenarios.

2. **Security.** Security is the capability of the system to protect the software components and data from unintended or unauthorized access, change, or destruction. It guarantees integrity, confidentiality and availability of data. Furthermore, it protects the control systems and applications from inappropriate utilization. Attribute Standards, such as ISO 21434 Cybersecurity, govern the minimum requirements to ensure the security of systems [10]. Security can be further sub-categorized into:

- *Integrity:* The capacity of the system to prevent data corruption is referred to as integrity. Additionally, it includes the prevention of unauthorized system alternations or the removal of vital information from the system.
- *Confidentiality:* The ability of the system to limit access to the resources and critical information for select authorized personalities.

3. **Privacy.** Privacy refers to the system's ability to provide the user the privilege to control or manage the information relating to them. Often, user information is collected or generated by the products owned by the users. Privacy also encompasses determining with whom such information shall be revealed. It is perceived to be a significant contributor to trustworthiness, particularly when the system has access to internet connectivity. The system's trustworthiness is enhanced when the users have extended control over or regulate the visibility of their private information (for example, name, photos and activity) [3]. Most countries have strict legislation governing privacy. Henceforth, the manufacturers must ensure that the development process incorporates measures for handling private information and complies with all the applicable laws.

4. **Performance.** This system characteristic measures how well the system performs its intended function [3]. Performance can be sub-categorized into:

- *Response time:* The time taken to complete a service transaction. Latency can be accounted for in response time. Latency determines the time to execute the service from receiving a request.
- *Throughput:* The system's capacity to handle several event responses during an interval. Throughput can be further distinguished as input, communication and processing throughput.

5. **Reliability.** The system can function without failure under designated conditions for a defined duration. The system consistently executes its designated functions and yields satisfactory outcomes. It is an essential attribute for fostering user trust that, over a designated period, the system will reliably yield consistent and intended outcomes [10].
6. **Availability.** The system's characteristic of being available to users for executing the intended function within a designated time frame [3]. When the system or its components malfunction, the system will be unable to execute the intended operation. Nevertheless, if the system is designed to manage internal faults, it will remain operational. Consequently, user confidence increases as the system demonstrates its ability to manage hazardous events resulting from the unavailability of particular system components.
7. **Usability.** Usability includes all user-related attributes, such as the simplicity of system operation, input modalities and comprehensibility of system output. Usability becomes significant when the system engages in notable interactions with the user. Usability can be analyzed into attributes like learnability, utilization efficiency, comprehensibility, satisfaction and effectiveness [3]. Consequently, when the user can effortlessly and efficiently learn to manage the system to fulfil their needs, it inherently fosters an increase in user trust.

The essential trustworthiness features stated must be seamlessly included in the system to enhance its overall reliability. Integration is a fundamental duty of the development framework which acts as the structural foundation for embedding these qualities. Therefore, it is essential to create a development framework that identifies the relevant trustworthiness features and enables their methodical development and integration into the system.

A framework must be developed to evaluate the pertinence of particular trustworthiness attributes according to the system's intended application and operational

environment. It must also offer strategies for converting these attributes into actual system features that can be evaluated and confirmed. The framework guarantees that the system not only complies with theoretical trustworthiness features but also manifests these characteristics in practical applications, hence enhancing the system's reliability and the trust users invest in it.

3. TRUSTWORTHINESS FRAMEWORK

3.1. Overview of Trustworthiness Framework

Addressing trustworthiness in cyber-physical systems is a complex task that requires a systematic execution of the development and verification process. Consequently, modifications and additions to an existing development process are required. Designing a completely new development process requires expertise and it is difficult to comply with all existing regulations and standards. Therefore, considering the complexity, the study was limited to proposing additions and/or modifications to a well-established and certified development process. The V development cycle of the ASPICE standard, widely used within automotive companies, was considered the foundational skeleton for the modified development process. The hardware and software development and verification process was combined into a single process step for ease of understanding.

The trustworthiness framework intends to have a well-structured method to manage the various processes to make the development process constructive, transparent and completely traceable. The process steps which are drawn parallel to the process from the ASPICE V model enlisted in VDA QMC standard [13] are briefly mentioned in the respective steps below. Therefore, the framework recommends the use of industry-standard methodologies and approaches to build trustworthy cyber-physical systems. The study identified three critical areas where additions were necessary in the standard V-model, as shown in Fig. 4. Every process block in the framework is associated with an identifier, for instance, TWF1, TWF2 and TWF3, where TWF refers to Trustworthiness Framework. The process blocks highlighted in blue represent the additions proposed in the current study, while the green-shaded blocks are reused from the standard V-model. The three areas are briefly discussed below.

1. *TWF1 Assess Trustworthiness Intensity.* It is a crucial process in the development framework, as the trustworthiness parameter is evaluated to determine the degree of applicability of the proposed framework to develop a system based on context and application. A trustworthiness intensity parameter is assigned, which will decide to what extent the proposed framework needs to be adopted. Consequently, OEMs must account for the additional demand of human resources and development costs to design the system. The current study

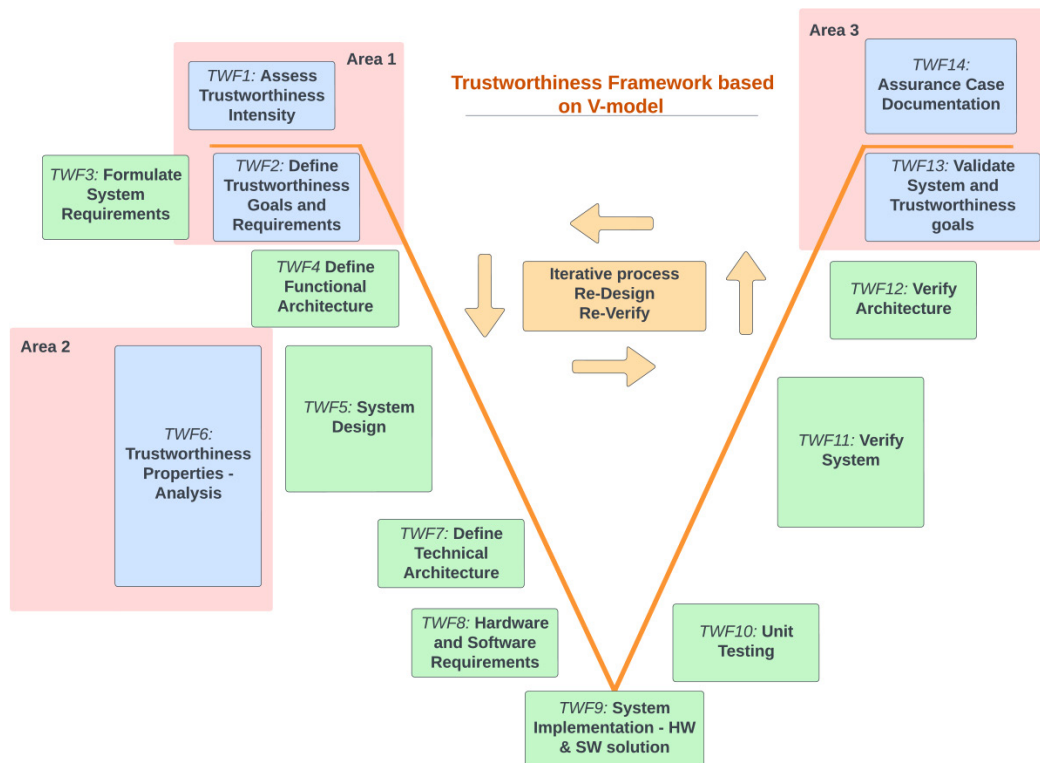


Figure 4. Trustworthiness framework based on a standard V-model.

proposes an assessment table that can guide system developers in assessing the degree of trustworthiness. Assessment involves allocating a rating for a system's safety, security and availability that forms the fundamental concepts of maintaining the trust relationship. These 3 system properties are specifically chosen among the other trustworthiness attributes based on the recommendations of industry experts. However, the study acknowledges that the parameters can change based on the quantitative data analysis of crashes and user interviews. Therefore, the assessment table can be redefined with real-world data and provide a more accurate degree of trustworthiness relevant to the system. The respective properties can be rated based on the following parameters:

- **Safety.** Rated as SF0, SF1, SF2 or SF3 as per:

- (a) *SF0*: No injuries to anyone due to failure or system limitations.
- (b) *SF1*: Light injuries or light environmental damage due to system failure or limitation.
- (c) *SF2*: Moderate injuries to severe injuries or heavy environmental damage due to system failure or limitation.
- (d) *SF3*: Life-threatening injuries and significant damage due to system failure or limitation.

- **Security.** Rated as SC0, SC1, SC2 or SC3 according to:

- (a) *SC0*: No information is required to protect.
- (b) *SC1*: System operation involves basic non-critical information.
- (c) *SC2*: System operation deals with only critical information of vehicle or private information of user.
- (d) *SC3*: System operation deals with critical information of the vehicle and private information of users.

- **Availability.** Rated as AV0, AV1, AV2 or AV3 according to:

- (a) *AV0*: Vehicle basic operation does not depend on the system's availability.
- (b) *AV1*: Vehicle operation depends on the system, but the system's unavailability will not hinder basic vehicle functionality.
- (c) *AV2*: Vehicle operation moderately depends on the system and the system's unavailability will cause the vehicle to operate in degraded functionality.
- (d) *AV3*: Vehicle operation highly depends on the system and the system's unavailability will cause critical failure of vehicle functionality.

Once all three ratings have been assigned to the system, the assessment matrix proposed by the study is used to determine the degree of trustworthiness. The assignment of safety, security and availability is performed on the basis of the developer's experience and any real-world data of crashes. The assigned values are summed together to get the degree of trustworthiness. If the sum of values is less than or equal to 2, TW1 is assigned to the system. If the summation lies between 3 and 5, TW2 is assigned to the system. TW3 is assigned when the summation equals a value greater than 5. The matrix is shown as a table in Fig. 5. By mapping the ratings, the trustworthiness rating is realized as TW1, TW2 or TW3, which are elaborated as follows:

- **TW1:** Basic trustworthiness satisfied by the existing quality process.
- **TW2:** Moderate trustworthiness can be proved by the existing quality process and building a *assurance case*.
- **TW3:** Trustworthiness is highly relevant and requires additional development processes to incorporate or improve the properties of the system.

2. *TWF2 Define Trustworthiness Goals and Requirements.* The trustworthiness requirements can be met using an 8-step approach based on the problem-based requirements engineering method. The method promotes systematic derivation of trustworthiness requirements from user trust concerns, as shown in Fig. 6. This step is performed in parallel to the SYS.1 Requirements Elicitation of ASPICE model. The analysis performed on customer stakeholder requirements is used as input to the first substep. The steps involved in eliciting requirements are as follows.

- (a) *Gather user trust concerns.* Concerns can be obtained by interviews of users, questionnaires for users, literature review and experience of subject experts, depending on the system's application and operational domain.
- (b) *Define trustworthiness vector.* All the trustworthiness attributes that seem to address a particular trust concern are identified and grouped. The group of attributes forms a vector known as the trustworthiness vector. This vector is demonstrated in Section 4. The vector may contain a different set of attributes for every system in the hierarchy of System-of-Systems. Therefore, the trustworthiness vector differs for a super-system using the system under development.
- (c) *Develop a system model.* A six-variable system model encompasses the system or software under consideration, the basic inputs and outputs of the system, the monitored and controlled domain, and the requirement that

Safety	Security	Availability			
		AV0	AV1	AV2	AV3
SF0	SC0	TW1	TW1	TW1	TW2
	SC1	TW1	TW1	TW2	TW2
	SC2	TW1	TW2	TW2	TW2
	SC3	TW2	TW2	TW2	TW3
SF1	SC0	TW1	TW1	TW2	TW2
	SC1	TW1	TW2	TW2	TW2
	SC2	TW2	TW2	TW2	TW3
	SC3	TW2	TW2	TW3	TW3
SF2	SC0	TW1	TW2	TW2	TW2
	SC1	TW2	TW2	TW2	TW3
	SC2	TW2	TW2	TW3	TW3
	SC3	TW2	TW3	TW3	TW3
SF3	SC0	TW2	TW2	TW2	TW3
	SC1	TW2	TW2	TW3	TW3
	SC2	TW2	TW3	TW3	TW3
	SC3	TW3	TW3	TW3	TW3

Summation	SF + SC + AV	1,2	3,4,5	6,7,8,9
Colour Coding:				

Figure 5. Trustworthiness assessment matrix.

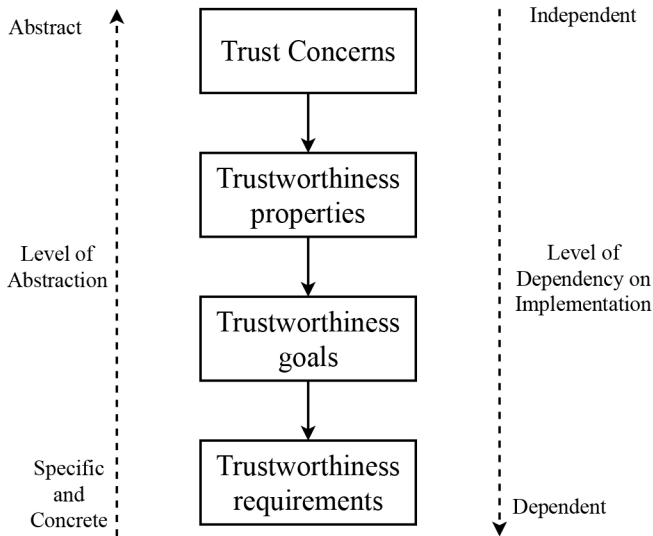


Figure 6. Relationship between trust concerns and trustworthiness requirements.

the system is fulfilling. The four variables from the standard four-variable model are reused and two new variables are added to the model. The variables constitute input (i), output (o), monitored (m), controlled (c), and the new variables, referenced (r) and desired (d) variables [14]. The template of the system model, which demonstrates the system interaction with the real world domain, is shown in Fig. 7.

- (d) *Assign trust concerns to the elements.* The trust concerns of the users obtained from the stakeholder analysis are assigned to the model

elements that are responsible or may influence the concerns. This step can localize the problems and allow the developers to find an appropriate solution.

- (e) *Annotate trustworthiness vectors.* The trustworthiness attributes identified in step two are now associated with every trust concern. The association enables traceability and justifies the selection of certain attributes that are relevant to the system under consideration. At least one attribute should be associated with every trust concern in the system model.
- (f) *Define Trustworthiness Goals.* A Trustworthiness Goal is used to address the trust concerns notified by the end users. These goals specify targets for the system to gain the user's trust. Documenting them in the system model diagram can serve as justification for design decisions taken during the development of the system. Furthermore, the goals are mapped to the relevant elements from the system model.
- (g) *Refine system model.* The system model is refined to decompose the high-level system requirement into sub-requirements so that each sub-requirement is modeled further into a problem diagram. The general requirements are now decomposed into several functional requirements. Trust concerns and goals can also be refined to fit the model, if necessary, and then assigned to particular elements in the problem diagram.

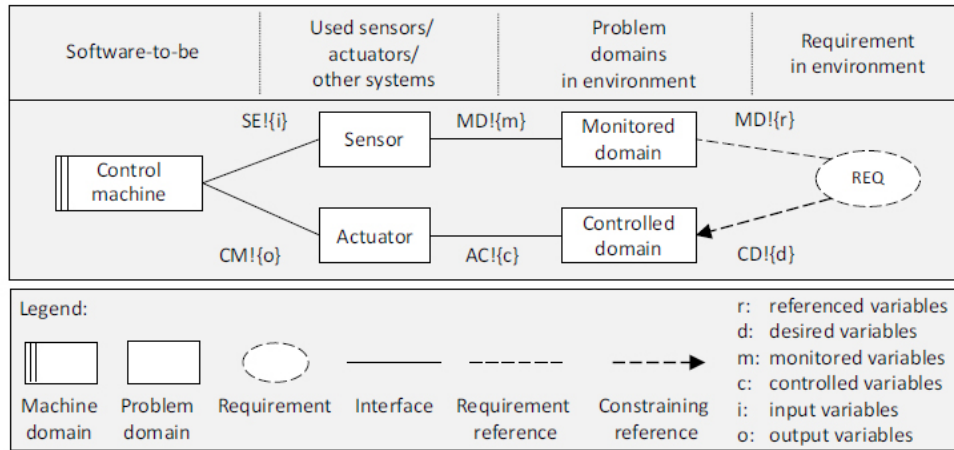


Figure 7. Six variable model template [14].

- (h) *Derive Trustworthiness requirements.* Requirements are derived from the trust goals in the refined system model. It could be noted that requirements might be similar to the trust goals. The requirements may be specific or defined at a system level. Suppose the requirements are defined on a system level. In that case, the satisfaction of the requirement is deferred to the later development phase of the respective subsystem by the concerned team of developers. The requirements are connected with the trustworthiness vector with an included type of association indicating that the properties contain the following requirements.
3. *TWF3 System Requirements.* The functional and non-functional requirements for the system are defined in the current process block. Various requirements, engineering methodologies and tools can be employed to improve traceability. This process corresponds to the ASPICE model step SYS.2 System Requirements Analysis where the system requirements are created, updated and reviewed.
 4. *TWF4 Define Functional Architecture.* Functional architecture contains functional blocks of the system. The interactions between the blocks are defined and the input and output channels of the system are realized. The architecture provides the system's blueprint on an abstract functional level. This process step ASPICE's SYS.3 System Architectural Design where the system architecture with subsystems are designed and documented is spread across the framework's TWF4 to TWF7. The framework's process steps are detailed out to systematically define the architecture of the system as compared to ASPICE's SYS.3 where these steps are compressed to one process step.
 5. *TWF5 System Design.* The system design comprises designing the system at lower levels. Each of the functional blocks from the functional architecture are examined to develop their subsequent sub-components. In other words, the primary function of a block is decomposed into sub-functions, which are allocated to the components of the respective block. This development process leads the functional architecture towards a technical architecture.
 6. *TWF6 Trustworthiness Properties-Analysis.* The trustworthiness properties [15] identified in earlier stages of development would imply the addition of specific analyzes or additional processes to meet the trustworthiness requirements. A common example of such an analysis is functional safety analysis, safety analysis of intended functionality and cyber security analysis, which are executed alongside the System Design. However, these additional analyses are not limited to being conducted alongside the System Design, TWF5. They can be carried out throughout the V-cycle as per needs and demands. However, the research study decided to provide a parallel analysis that could have a high degree of influence on the design of the system. This added process step runs parallel to the ASPICE's SYS.3 process, which has an iterative influence over architecture development. The input of the additional analysis is incorporated into the system design to develop a technical architecture.
 7. *TWF7 Define Technical Architecture.* The technical architecture evolves from the functional architecture, which contains the technical details of the system. The architecture specifies the system components that fulfill the functions defined within the functional blocks. In addition, the architecture demonstrates the interfaces between the system components and the types of exchanges between them to meet the requirements.
 8. *TWF8 Hardware and Software Requirements.* These requirements are intended to define the hardware and software components of the system. The technical architecture provides details on the role of

hardware and software components; however, to develop each of these components individually, specific requirements are required that govern the development of individual system components. Unlike the process steps of ASPICE SWE.1 and SWE.2 to define the Software Requirements and Software Architecture Design, the process steps TWF7 and TWF8 focus on defining requirements and architecture design of both Hardware and Software elements of the system.

9. *TWF9 System Implementation.* The implementation of the system is carried out by the respective development teams within an organization. The developers of the respective components also define the hardware and software requirements according to the technical architecture. The system's individual components are developed and later integrated as per the definition in architecture. This step is identical to the ASPICE SWE.3 Software Detailed design and Unit construction. However, in the process step, both HW and SW units are constructed.
10. *TWF10 Unit Testing.* Before integrating individual hardware and software components to build the system, components are individually tested to verify their respective requirements defined by component developers. The components are integrated only when they meet the requirements. This step is similar to the process step of ASPICE's SWE.4 Unit testing.
11. *TWF11 Verify System.* In this phase of the testing, the system is checked for compatibility and efficiency of the interfaces. Integrating hardware and software components to build the overall system is successful only when the interfaces work appropriately without impacting the working of other components. The ASPICE SWE.5, SWE.6 and SYS.4 processes ensure the verification of the software. In contrast, TWF11 verifies the integration of HW and SW.
12. *TWF12 Verify Architecture.* The functioning of the system is verified with respect to the requirements of the system defined in the early stages of development. The non-functional requirements are verified by checking the performance parameters of the system.
13. *TWF13 Validate System Function and Trustworthiness Goals.* The goals and the functioning of the system are validated by the user to determine whether the right system was developed. After testing a system prototype, users provide feedback about the system to the developers. The system developers complete the development process when all the goals are achieved. However, often, the user validation feedback is decomposed to iterate the development cycle to re-design the changes

proposed in the feedback. The iteration process is repeated until the relevant stakeholders of the system are sufficiently satisfied. Validating the trustworthiness goals is crucial to ensure that the system is acceptably trustworthy. The system validation in the ASPICE model is performed by the process SYS.5 System Qualification Test. The TWF13 illustrates a similar process to validate the system.

14. *TWF14 Assurance Case Documentation.* Documentation of the goals developed within a system is a crucial element to improve the traceability of the development process. The assurance case serves as an audit of the trustworthiness properties developed of the system that could be presented to the stakeholders. These cases communicate a clear and comprehensible argument that the system reasonably possesses the properties claimed in a particular context. The documentation also justifies that the developed system complies with all the relevant regulations and standards, which could result in the system's certification. Assurance cases are represented in textual or graphical methods. Graphite methods include the usage of structured notations such as Claims-Argument-Evidence (CAE) or Goal-Structuring-Notation (GSN) [16]. These methods are widely used because of their ability to document clear and well-structured argumentation. In contrast, the structured assurance case metamodel (SACM), a model-based documentation, can be utilized to develop cases. SACM facilitates features such as controlled vocabulary, modularity and traceability of evidence from argument compared to existing approaches [17]. However, Object Management Group (OMG) does not specify a detailed usage of SACM and its relationship to existing approaches is not sufficiently addressed. These reasons introduce challenges for the usage of SACM, primarily due to the complex nature of SACM and its usage.

The development process can be performed using various software and system development methodologies. The system developers can adopt any existing methodologies and approaches based on the context of the system under development and organizational practices.

4. DEVELOPMENT OF AN EXAMPLE

The proposed framework estimates a boost in user trust by improving the trustworthiness of the system. To realize the working efficiency of the framework, the study considered an application example, a Driver Monitoring System (DMS), to develop using the framework. The new process steps proposed in the study are briefly highlighted in the current section to limit the scope of the article. TWF1: The trustworthiness assessment step involved the DMS evaluation that resulted in trustworthiness level TW3. The three properties for

the intensity assessment were rated as SF2 for Safety, SC2 for Security and AV2 for Availability. The respective rationales for the ratings are tabulated in Table 1. Referencing the Trustworthiness Matrix shown in 5, the summation of ratings results in TW3 (high relevance of trustworthiness). Hence, the proposed framework is relevant to develop the DMS according to the TWF1's definition.

The TWF2 process was followed, where three user trust concerns were derived from a literature study as enlisted below.

- **TC1:** Can the system accurately identify the driver's attention levels under all operating conditions?
- **TC2:** Is the system capable of protecting against miscellaneous attacks by hackers trying to steal driver personal information, video and audio files?
- **TC3:** Whether the vehicle offers the user to decide what information is stored and shared with the company and what prevents the company from using those data for other purposes?

Furthermore, the literature study highlighted the desirable system properties *Performance, Safety, Security and Privacy*, which comprise the trustworthiness vector. These trust concerns along with their relevant system properties from the vector are assigned to the six-variable DMS model as shown in Fig. 8. Potential solutions for trust concerns were utilized to derive trustworthiness goals. Such goals are assigned to the relevant system elements in the six-variable model. Consequently, the model is refined to derive six trustworthiness requirements for DMS. For instance, one of the TW requirement for DMS included “*The system should have a diagnosis manager to monitor for any malfunctions or failures of the components*”. The trustworthiness requirements serve as parent high-level requirements that are used to formulate system requirements as a part of TWF3. The framework defines other system requirements for DMS and the process moves toward developing a functional architecture of the DMS as a part of TWF4 and TWF5. The functional architecture for DMS developed in the study is illustrated in Fig. 9.

System Properties	Assessment	Rationale
Safety	SF2	The system failure may lead to inaccurate estimation of driver's awareness and lead to an accident in high or moderate speed.
Security	SC2	The system deals with the private information of the user that includes video footage of the driver, face bio-metrics, and so on.
Availability	AV2	The unavailability of the DMS can cause the ADS to operate with degraded functionalities.
Trustworthiness	TW3	The proposed development changes are necessary to improve the trust relationship between the system and the user.

Table 1. DMS trustworthiness intensity assessment.

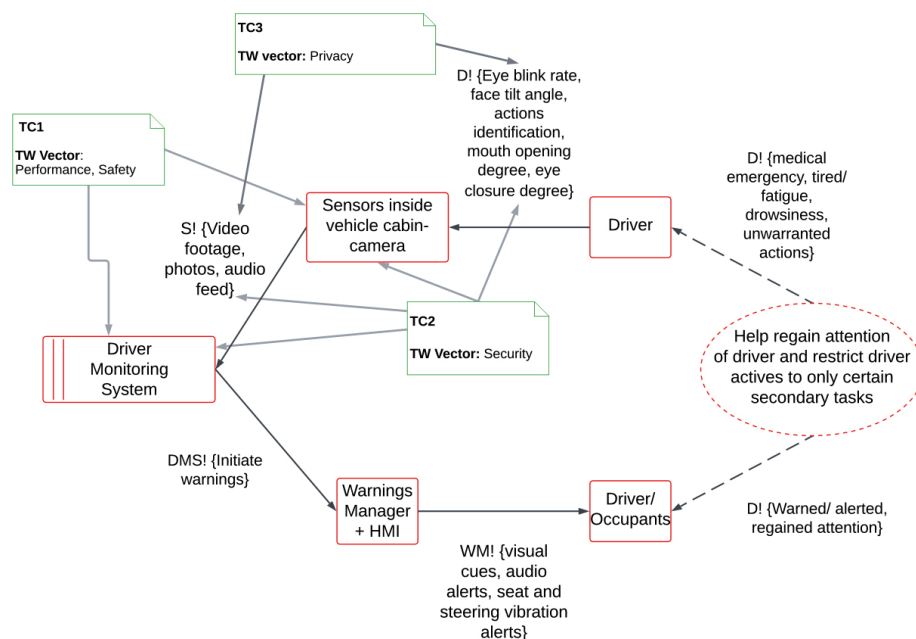


Figure 8. Six variable model for DMS.

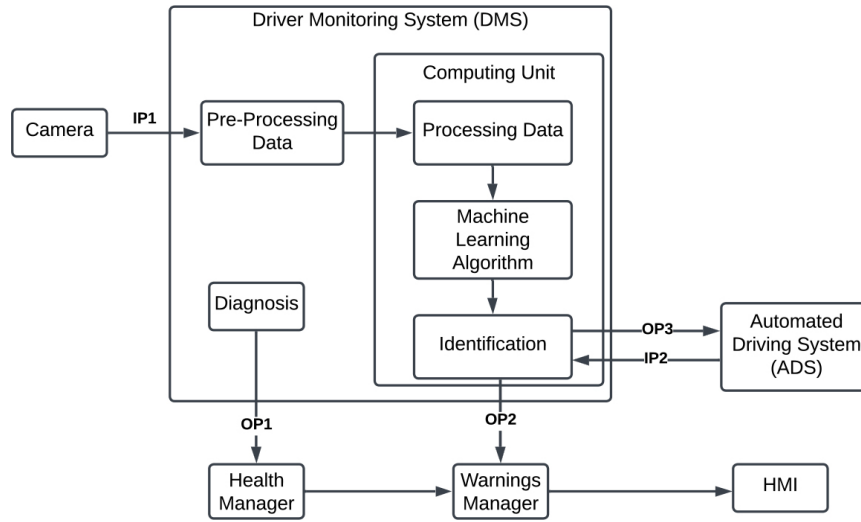


Figure 9. Functional architecture of DMS.

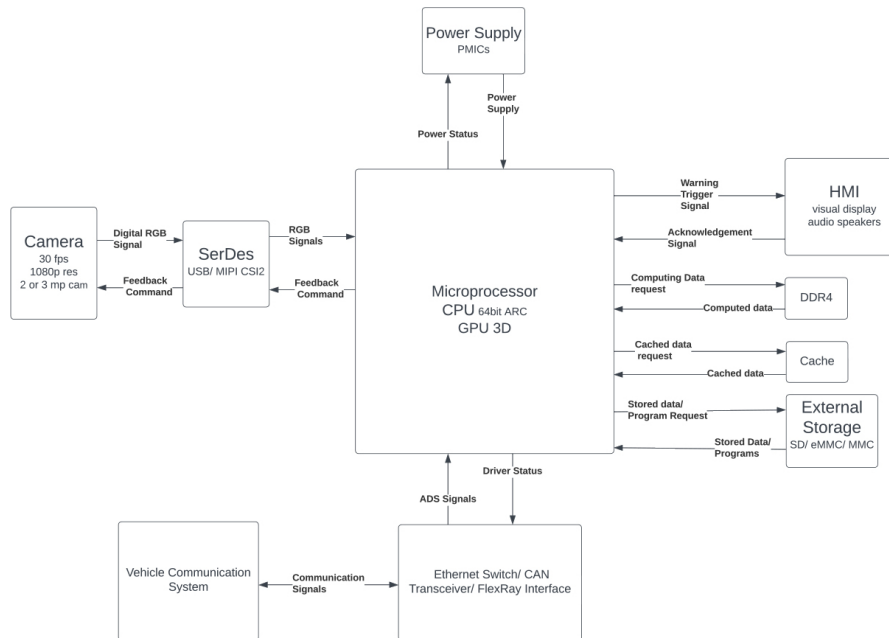


Figure 10. Technical architecture of DMS.

The TWF6 provides the input to iteratively redesign the system architecture through various analysis determined by the trustworthiness vector. For DMS, the trustworthiness vector Safety property was considered and a SOTIF (Safety Of The Intended Functionality) analysis was performed following the ISO 21448 standard. However, the study posits that the demonstration of the SOTIF analysis will effectively guide developers in conducting similar evaluations of trustworthiness properties from TWF2.

The SOTIF analysis produced a series of mitigation strategies, which were subsequently incorporated into the system requirements as safety requirements. An example of such strategies included “Prevent or minimize as far as possible incorrect detection under the

cases of full or partial blockage in field-of-vision of the camera. If the camera’s vision is fully, or partially blocked, whiteout, or blurred image is recorded, alert the control unit”. In the TWF5 phase of system design, the functional architecture assigns specific responsibilities to the system components, leading to the realization of the technical specifications required to fulfill these responsibilities. This process results in the formation of a technical architecture, as depicted in Fig. 10 as part of TWF7. This architecture provides a framework for component developers to establish technical requirements for each hardware and software component within the Driver Monitoring System (DMS). These components are developed as developers implement the requirements to achieve the intended functionalities and are then integrated to assemble the complete DMS.

Only a selective subset of requirements was implemented in the example. The DMS was setup using an NVIDIA Xavier NX board connected to a monitor and a webcam. The software for the DMS utilized an open-source, pre-trained deep-learning Python algorithm designed to detect facial features such as eyes, nose and mouth. This setup demonstrates the practical application of integrating selective trustworthiness requirements into a functioning system.

The Driver Monitoring System (DMS) successfully detected the user’s face and eyes, as illustrated in Fig. 11. The system is configured to issue a warning when the eyes are detected to be partially or fully closed for more than 15 frames in the video feed. The warning is displayed on the monitor for demonstration purposes, as shown in Fig. 12. Furthermore, DMS incorporates one of the SOTIF mitigation strategies designed to prevent or mitigate the risks associated with intentional or unintentional obstruction of the camera by the user.

The system was evaluated through five test cases, defined during the verification stage TWF10 to TWF12. The Driver Monitoring System (DMS) successfully met the criteria for four of these five test cases, which were meticulously documented in the test specifications. These specifications provide crucial artifacts for

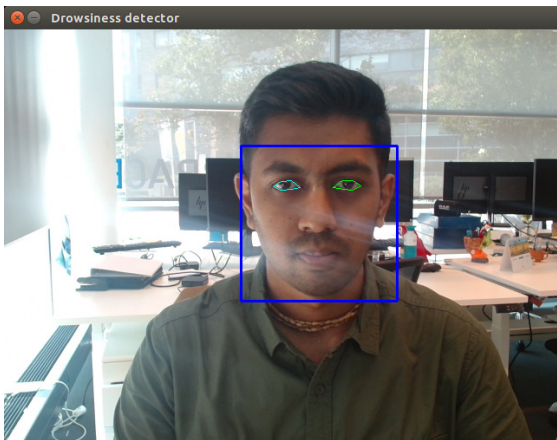


Figure 11. Face detection by DMS.

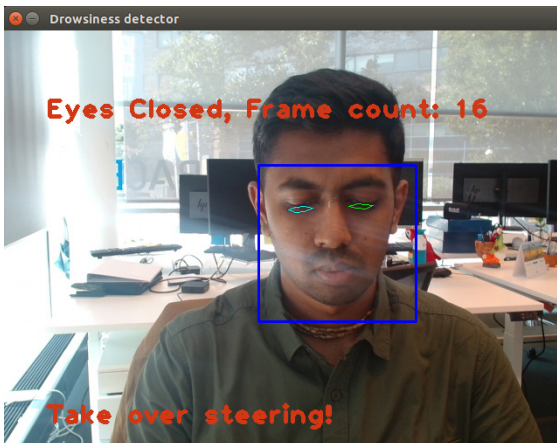


Figure 12. Warning alert displayed by DMS.

evidence-based documentation of the system’s trustworthiness. Furthermore, the DMS was validated by feedback from general users; 20 individuals who interacted with the example demonstration were surveyed to gather user feedback. The general satisfaction of the user is shown in Fig. 13, with most of the respondents expressing high levels of satisfaction and a reasonable proportion maintaining neutral views. However, the feedback was predominantly positive, indicating user comfort with the DMS. The survey also highlighted the attributes that contributed to the perceived trustworthiness of the system, with the results displayed in Fig. 14. Safety was identified as the most valuable property, followed by reliability, cybersecurity, accuracy (performance) and privacy, in descending order of preference. In particular, four out of the five key desirable properties were correctly identified by the proposed trustworthiness framework, indicating the positive potential of the current framework.

This example of the DMS illustrates the practical application of the proposed framework. However, for trustworthiness properties to be comprehensively documented and achieve certification, they must be systematically integrated into all aspects of the development framework. In line with this approach, the study documented a safety case as part of TWF14 for the SOTIF mitigation strategy. This GSN case was translated into a SACM safety case. The transition from GSN to SACM, as shown in Table 2, was carried out using state-of-the-art methods approved by the Assurance Case Working Group [17]. This process exemplifies a holistic development approach, underscoring the framework’s capacity to bolster the trustworthiness of cyber-physical vehicle systems.

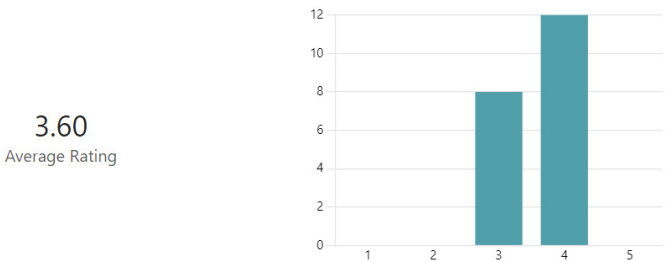


Figure 13. User satisfaction rating.

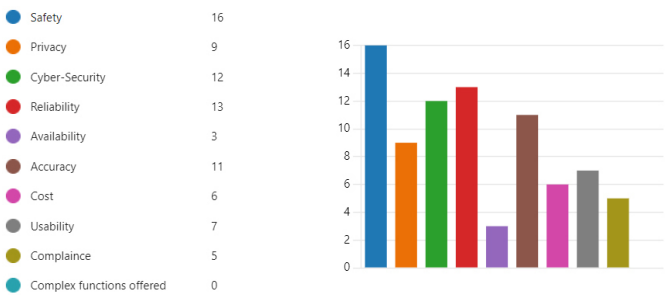


Figure 14. Trustworthiness properties of DMS preferred by users.

S1 No.	GSN Element	SACM Element	Remarks
1	GSN: Goal	SACM: Claim	The goals are represented as Claims. The class Claim has attributes describing the type of Claim. The attributes include: <ul style="list-style-type: none"> <i>assertionDeclaration</i>: String <i>isPublic</i>: boolean <i>undeveloped</i>: boolean For a GSN: Goal, the attribute <i>assertion-Declaration</i> is set to assert. The <i>isPublic</i> is initialized to True if the goal needs to be publicly available to other Assurance packages. The <i>undeveloped</i> attribute notifies if the goal is yet to be fulfilled.
2	GSN: Strategy connecting N sub-goals to M parent goal by the aid of GSN: <i>SupportedBy</i> links	SACM: <i>ArgumentReasoning</i> attached (by means of reasoning) to a SACM: <i>AssertedInference</i> connecting n sources and m targets.	The Argument Reasoning is a node that associates with an <i>AssertedRelationship</i> . They do not connect to directly to a Claim or <i>ArtifactReference</i> .
3	GSN: <i>SupportedBy</i>	SACM: <i>AssertedInference</i>	Sources (GSN: Sub-goals) to M targets (GSN: Goals). Converting GSN to SACM models needs additional attention because the SACM utilizes a reversed approach to connect GSN: parent goals to sub-goals. The semantics of SupportedBy (A is SupportedBy B) and the semantics of AssertedInference (B infers A) need to be noticed.
4	GSN: Solution	SACM: <i>ArtifactReference</i>	The <i>ArtifactReference</i> is a reference to an evidence such as result of test case, and so on. The references reside in the Artifact Package. The solutions are connected to a Claim through <i>AssertedEvidence</i> interface. The semantics of <i>Assertedevidence</i> is similar to that of <i>AssertedInference</i> .
5	GSN: Context	SACM: <i>ArtifactReference</i> attached to a SACM Claim to SACM: <i>ArgumentReasoning</i> through a SACM: <i>AssertedContext</i> .	The GSN: Context could be either explanatory or referential. Explanatory: a description of context to an element; SACM uses an <i>AxiomaticClaim</i> for explanatory type of context. Referential: referring to an artefact for providing contextual information. SACM uses an <i>ArtifactReference</i> for this type of context.
6	GSN: Assumption	SACM: Claim	SACM represents Assumptions as a Claim but with the attributes specifying the <i>assertionDeclaration</i> as 'assumed'.
7	GSN: Justification	AGSACM: ClaimO	SACM represents Justifications as a Claim but with the attributes specifying the <i>assertionDeclaration</i> as 'axiomatic'.
8	GSN: <i>InContextOf</i>	SACM: <i>AssertedContext</i>	The context to a Claim or <i>ArgumentReasoning</i> . is provided through an <i>AssertedContext</i> . The semantics of <i>AssertedContext</i> is similar to that of <i>AssertedInference</i> .

Table 2. Mapping of GSN element to the respective SACM elements.

5. CONCLUSION AND DISCUSSION

The fundamental element in using a system is the trust relationship between the user and the system. The literature review emphasized the significance of cyber-physical systems and their function within the automobile sector for full autonomy (self-driving capability). Consequently, the fundamental necessity of cultivating a robust trust connection becomes very vital. Finally, the literature review emphasized that there are currently limited norms and laws especially designed for emerging autonomous driving systems.

The study defined trustworthiness as the quality of an automotive system or its user to execute intended functions accurately and consistently, thereby ensuring the preservation of overall safety during operation. The trust connection depends on the attributes of

both the users and the system, which are termed as trustworthiness attributes. Therefore, a development framework has to facilitate the development of such attributes within the system.

The study presents a development framework grounded in the ASPICE V-development model, focusing on the identification, evaluation and adoption of the system's trustworthiness attributes or properties. The requirements phase also needed to include the identification of important trustworthiness properties based on user trust concerns. Additional analyses are performed concurrently with the system design to meet trustworthiness requirements. The generation of an Assurance case is a valuable addition to the process, as it documents evidence-based justification for the presence of trustworthiness properties within the system. The Driver Monitoring System example exemplifies the

application of the framework. User surveys revealed a significant increase in satisfaction levels with the demonstration. The framework demonstrates reasonable efficiency in emphasizing the specific properties of the system that contribute to trustworthiness.

The study's essential finding indicated that numerous trustworthiness criteria are already being fulfilled by current processes, such as Functional Safety, SOTIF, Cybersecurity, Privacy and Quality Management. The creation of an entirely new framework may be unnecessary; therefore, the study offered supplementary processes to the existing V-model framework to enhance Trustworthiness. The study also includes a trustworthiness evaluation table that can be refined to ascertain whether the updated framework is essential to achieve the requisite level of trustworthiness for a specific application of the system. The study aims to demonstrate that advanced cyber-physical automotive systems necessitate a modification in the development process and suggests a paradigm that system developers can effectively implement.

6. FUTURE SCOPE

The future scope of this project will explore various techniques to improve the effectiveness of trustworthiness detection and evaluation within the system. This may entail employing computational techniques alongside machine learning algorithms to determine exact degrees of desirable attributes in cyber-physical vehicle systems. The complex nature of the evaluation can influence the acceptance rate among system developers due to deficiencies in prior knowledge of computation and machine learning. The creation of abstract applications can address knowledge gaps and thus improve the adoption rate among system developers in the automotive sector.

The required levels of trustworthiness assurance in systems may remain unattainable due to the diverse interpretations of trustworthiness and the methodologies employed by suppliers and manufacturers throughout the supply chain. More study is required to standardize the process or framework, particularly in establishing uniform metrics for each system property and associated measurement methodologies.

Different approaches, such as the House of Quality matrix from Quality Function Deployment, could be examined to establish a standardized approach for evaluating and determining the necessary trade-offs among system trustworthiness properties. The results of this analysis can improve the efficiency of the overall framework by optimizing the use and development costs of human resources. Furthermore, using model-based engineering can establish a framework for integrating work outputs to create a digital twin, thereby expediting the testing part of the development cycle.

Ultimately, the attributes of user trustworthiness affect the trust relationship. Although this facet of trustworthiness was briefly examined in the present study, a conclusive methodology is necessary to determine the complex user attributes that enhance the trust connection. Subsequent studies may investigate approaches that compensate for user backgrounds and provide valuable insights to the manufacturer for informed decision-making in system development.

Conflict of Interest

The authors declare that they have no conflicts of interest.

Data Availability

The data that support the findings of this study are available from the corresponding author, upon reasonable request.

Funding

The authors declare no funding was used for this study.

Authors' Contribution

P.M.P. Kumar contributed in study conceptualization, system implementation, testing and writing (review & editing) the manuscript. Ion Barosan and Avinash Varadarajan supervised the project, state-of-the-art research and writing (review & editing) of the manuscript.

REFERENCES

- [1] Martin Placek. Automotive Electronics Worldwide - Statistics and Facts — Statista. Statistica, 2023. URL: <https://www.statista.com/topics/7983/automotive-electronics-worldwide/topicHeaderwrapper>
- [2] Harry Fowle. Four Megatrends in the Automotive Industry. Electronic Specifier, 2023. URL: <https://www.electronicspecifier.com/industries/automotive/four-megatrends-in-the-automotive-industry>
- [3] N.G. Mohammadi. Trustworthy Cyber-Physical Systems: A Systematic Framework Towards Design and Evaluation of Trust and Trustworthiness. Wiesbaden: Springer Vieweg, 2019, p. XXIII, 320.
- [4] S. Kate Devitt. Trustworthiness of Autonomous Systems. In: H. Abbass, J. Scholz, D. Reid (Eds.), Foundations of Trusted Autonomy. Studies in Systems, Decision and Control, Vol 117. Cham: Springer, 2018, pp. 161–184.

- [5] F. Walker, Y. Forster, S. Hergeth, J. Kraus, W. Payre, P. Wintersberger, M. Martens. Trust in Automated Vehicles: Constructs, Psychological Processes, and Assessment. *Frontiers in Psychology*, 2023, 14: 1279271.
- [6] H.A. Abbass, J. Scholz, D.J. Reid. Foundations of Trusted Autonomy: An Introduction. In: H.A. Abbass, J. Scholz, D.J. Reid (Eds.), *Foundations of Trusted Autonomy. Studies in Systems, Decision and Control*, Vol. 117. Cham: Springer, 2018, pp. 1–12.
- [7] D. Fernández Llorca, E. Gómez. Trustworthy Autonomous Vehicles: Assessment Criteria for Trustworthy AI in the Autonomous Driving Domain. EUR 30942 EN, Publications Office of the European Union, Luxembourg, 2021.
- [8] Vehicle Safety and Automated/Connected Vehicles. URL: https://single-market-economy.ec.europa.eu/sectors/automotive-industry/vehicle-safety-and-automatedconnected-vehicles_en
- [9] B. Koller, R. Matawa. Automated Driving Requires International Regulations. In: P.E. Pfeffer (Ed.), *11th International Munich Chassis Symposium 2020: Chassis Tech Plus. Proceedings*. Berlin, Heidelberg: Springer Vieweg, 2021, pp. 39–53.
- [10] M. Buchheit. Journal of Innovation July 2022 - Industry IoT Consortium, Industry IoT Consortium Journal, 2022. URL: <https://www.iiconsortium.org/news/journal-of-innovation-july-2022/>
- [11] Assessment List for Trustworthy Artificial Intelligence (ALTAI) for Self-Assessment. URL: <https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment>
- [12] Annie Pauzie, O. Orfila. Methodologies to Assess Usability and Safety of ADAS and Automated Vehicle. *IFAC-PapersOnLine*, 2016, 49(32): 72–77.
- [13] VDA QMC. Quality Management in the Automotive Industry. Automotive SPICE Version 3.1. 2017. URL: https://vda-qmc.de/wp-content/uploads/2023/02/Automotive_SPICE_PAM_31_EN.pdf
- [14] N. Ulfat-Bunyadi, R. Meis, M. Heisel. The Six-Variable Model – Context Modelling Enabling Systematic Reuse of Control Software. In: *International Conference on Software Paradigm Trends*, Vol. 2. Lisbon: SCITEPRESS, 2016, pp. 15–26.
- [15] ISO/IEC TS 5723:2022: Trustworthiness — Vocabulary. ISO Organization Online, 2024. URL: <https://www.iso.org/standard/81608.html/>
- [16] R. Wei, T.P. Kelly, X. Dai, S. Zhao, R. Hawkins. Model Based System Assurance Using the Structured Assurance Case Metamodel. *Journal of Systems and Software*, 2019, 154: 211–233.
- [17] The Assurance Case Working Group (ACWG): Goal Structuring Notation Community Standard Version 3. SCSC-141C, 2021. URL: <https://scsc.uk/scsc-141c?tab=all>