Authors' version (postprint)

Human Interaction Safety Analysis Method For Agreements with Connected Automated Vehicles

Fredrik Warg, Martin Skoglund, Matthew Sassman

Published/presented in:

2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)

DOI: 10.1109/VTC2021-Fall52928.2021.9625202

2021-12-20

Postprint – To appear in *2021 IEEE 94th Vehicular Technology Conference (VTC 2021-Fall)*

Human Interaction Safety Analysis Method for Agreements with Connected Automated Vehicles

Fredrik Warg
RISE Research Institutes of Sweden
Borås, Sweden
fredrik.warg@ri.se

Martin Skoglund
RISE Research Institutes of Sweden
Borås, Sweden
martin.skoglund@ri.se

Matthew Sassman
Semcon Sweden AB
Göteborg, Sweden
matthew.sassman@semcom.com

***Abstract*—Connected and automated vehicles with a large variety in operating modes and operational contexts are now emerging. A vital safety assurance issue, also stressed by recent standards and guidelines, is the safety of human-machine interaction (HMI). This paper proposes, and shows a small example of using, a framework for human interaction safety analysis. It is intended for integration in an iterative development lifecycle and to be used in conjunction with relevant standards. In the framework, an analysis is first conducted to elicit all agreements between humans and the automated function, then an interaction analysis method is used to find potential problems with proposed interfaces affecting each agreement. Risk assessment is conducted to determine if risk reduction is necessary, and verification and validation activities are used to provide support for the analysis results and evidence of HMI safety for an assurance case.**

***Index Terms*—Human-machine interaction, Connected automated vehicles, Safety, Human factors, HMI agreements.**

I. Introduction

The use of connectivity and more advanced automation in vehicles are on the rise. Key expected benefits are improvements in efficiency, accessibility and safety. However, safety assurance is a challenge, and requires convincing evidence before the release of a product showing that all relevant hazards have been identified and addressed such that the residual risk is deemed acceptable. This is typically demonstrated by using a combination of analysis, design, and test methods. E.g., the standard ISO 26262 [1] describes such methods for achieving functional safety of electrical/electronic (E/E) systems in road vehicles. Another vital safety aspect, and the focus of this paper, is how to make sure all types of human machine interaction (HMI) is designed to ensure avoidance of accidents induced by an inadequate HMI. Several recent safety standards and guidelines for automated vehicles also require consideration of HMI safety, including ISO PAS 21448 [2], ISO TS 4804 [3] and UL 4600 [4].

Connected automated vehicles (CAVs) can differ significantly when it comes modes and contexts in which they can operate. For instance remote operation, driver assistance, or unsupervised driving (”self-driving”); it may be road vehicles for passengers or goods, or vehicles used in confined areas; and a vehicle could act independently or be part of a group or fleet of cooperating vehicles. For each type of function, there will typically be a number of stakeholders to consider, such as local or remote drivers, passengers in the automated vehicle, or other protected or unprotected road users. This means a wide variety of potentially safety-relevant interactions, including but not limited to driver interface issues such as control transitions and automation information, communication and behaviour towards other road users, and temporal aspects such as what happens if a function is updated over-the-air and suddenly behaves differently than what the driver has come to expect? We use the term *agreement* to refer to any context where a mutual understanding of what to expect and how each involved party should behave is needed for successful interaction. HMI safety assurance thus includes both showing that all relevant agreements have been identified, and that the interactions required for each agreement are understood, designed, and implemented in the CAV to meet acceptable risk.

In this paper, we contribute by proposing a structured human interaction safety analysis process (henceforth referred to as *HISA*) to help ensure that all agreements are identified and that interactions have an acceptable risk. It provides an entire lifecycle for HMI safety assurance, a method for eliciting and analysing different types of agreements, and consideration of different causes for HMI safety risks – impact of security weaknesses, human error, and E/E failures. To our knowledge, there are no other HMI analysis methods for CAVs covering all these aspects. The process is aimed to be used within the frameworks of current and upcoming CAV safety standards and includes: elicitation of agreements between function and relevant stakeholders, a structured analysis method for finding interaction hazards, risk assessment followed by adjustment of agreements and/or applying appropriate risk reduction measures if the risk is found unacceptable, verification of the implementation, and validation of analysis assumptions. If the function is updated, an impact analysis is conducted to make sure all agreements remain safe. The process builds upon our earlier work on agreements [5] and interaction analysis [6]. The contribution and focus in this paper is the overall process, improved agreement analysis, inclusion of the multi-concern aspect, and integration with standards. A limited traffic jam chauffeur example is used to illustrate the process.

This research has received funding from the Strategic vehicle research and innovation (FFI) programme in Sweden via the project SALIENCE4CAV (2020-02946), and via the HEADSTART project from European Union’s Horizon 2020 research and innovation programme under grant agreement No 824309. Content reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

II. Scope and Related Work

The aim of HISA is to help developers of automated driving systems (ADSs) to provide HMI safety assurance. To do this, it needs to bridge the human factors work with relevant safety standards; thus integration with standards is discussed in Sec. IV. The framework does not pretend to be able to cover how to conduct the human-centered part of the work, i.e. what is good HMI design or how to perform the evaluation, which are large research areas of their own. Neither does it touch upon the subject of what kind of automation is sensible to build in the first place. There are other methods to apply for this purpose, for instance the framework for automation design by Parasuraman et al. [7], where type and level of automation are evaluated and adapted based primarily on the human performance consequences and secondarily on relevant additional criteria such as automation reliability and cost of decision/action outcomes. This kind of evaluation will also take longer-term factors such as complacency and skill degradation into account. HISA, in contrast, is concerned with the task of making sure the implementation is done right once the type of automation and a proposed HMI are already defined. The primary focus is on vehicles with SAE automation levels 3-5 [8], but lower levels of automation would be covered under agreements in certain contexts. As support for frequent updates is often considered necessary for future CAVs, integration in iterative development processes is discussed in Sec. III-G.

Bengler et al. [9] has presented an HMI framework for automated vehicles which consider a number of HMI types: Automation HMI (aHMI) - interfaces with the automated function(s), vehicle HMI (vHMI) - interfaces with other vehicle functions, infotainment HMI (iHMI), external HMI (eHMI) - interfaces for communication with other road users, and dynamic HMI (dHMI) - communication via vehicle dynamics. We propose to use this classification in HISA. While all types may be safety relevant, aHMI, eHMI and dHMI will be of particular interest. There is a large body of work done on eHMI, but so far thorough evaluation of the safety implications is more scarce [10]. The type dHMI has been found to be of vital importance for the interaction with other road users [11].

A method related to HISA but more generic in nature is HFACS [12]; an example of its application to vehicle automation is included in ISO PAS 21448 Safety of the intended functionality (SOTIF) [2], Appendix E, as a candidate to use for HMI analysis. While there are elements in common between this HFACS-based approach and HISA, the latter specifically analyses the lifecycle of the vehicle with the aim of capturing all agreements - even ones that may have been overlooked in initial design - and also introduces some additional tools to aid in the interaction analysis. Another related method that considers both system and human errors is described by Martinie et al. [13]. It could be considered as an alternative/complement to our interaction analysis [6] as well as help in evaluating design alternatives in the HISA process. Evaluating such a combination is left for future work.

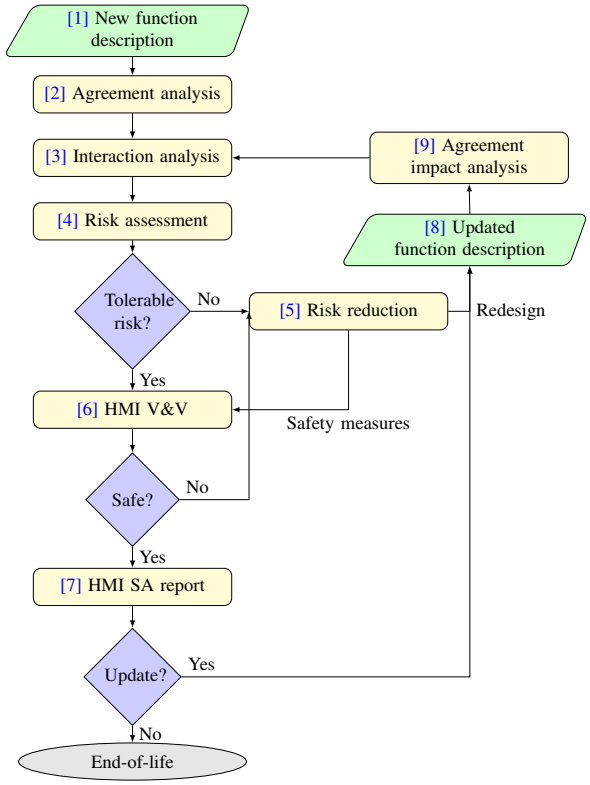


Fig. 1: HISA in an iterative development process.

III. HISA Process

A flowchart of the HISA process is shown in Fig. 1. Design of a new automated function begins with a function description (described in Sec. III-A), which becomes input to the subsequent analysis steps. First, an agreement analysis is conducted to identify relevant agreements (Sec. III-B), followed by interaction analysis to identify hazards in each agreement (Sec. III-C). A risk assessment is conducted (Sec. III-D) to determine if redesign and/or risk reduction measures are necessary (Sec. III-E). These steps are largely manual and rely on combined functional safety and human factors expertise, which we propose would be conducted by an expert team similarly to other safety analysis techniques, e.g. HAZOP [14], but using the systematic methods described below. When the HMI has been implemented, verification and validation (Sec. III-F) is conducted. When planning updates, an agreement impact analysis must be done to determine if there are changes requiring further re-work (Sec. III-G).

A. Function Description

The *function description* (steps [1] and [8] in Fig. 1) of the automated function under analysis (AFUA) shall describe the intended function. In order to enable HISA it must also specifically include information pertinent to the elicitation of agreements and analysis of interactions. This includes:

- the intended nominal behaviour and available fall-back(s) used if the nominal behaviour can not be maintained,
- the planned driving modes and their type of automation,

- the intended operational design domain (ODD) [8],
- the preliminary user interface design of aHMI, eHMI, dHMI, vHMI and iHMI, including expected interaction procedures/protocols, and
- any functionality relevant for lifecycle events such as update policy or user/ownership change procedures.

B. Agreement Analysis

The *agreement analysis* (step [2] in Fig. 1)[1] is a method for eliciting agreements for the AFUA by systematically considering the different aspects of its use, rather than just focusing on a preliminary design. The objective is to increase confidence that all relevant agreements have been considered in the safety analysis. We approach agreement elicitation by considering, in turn, the dimensions illustrated in Fig. 2:

1) Defining Concerns: List the quality attributes considered in the analysis and their respective acceptance criteria. Safety is the main purpose for HISA, but auxiliary attributes related to safety, such as security and legal considerations (e.g. adherence to traffic rules) should be included when applicable.

2) Defining lifecycle phases and events: Specific events or transitions between phases in the lifecycle of a CAV may affect agreements with human stakeholders. This part of agreement analysis aims at listing all such events and phases to make sure they are considered in the safety analysis. Phases are conditions which persist over a period of time. Each phase may contain events which for the purpose of the analysis can be regarded as atomic. Fig. 3 shows an example lifecycle analysis including the phases pre-deployment (could be further subdivided in e.g. design, test, production, sales if relevant), different owners, and decommissioning. For each owner there are sub-phases when the vehicle is operational (with different users) or non-operational. Events are illustrated with different symbols along the timeline and can include e.g. function updates, activation/deactivation of different automated functions, or specific traffic situations. The aim of detailing the vehicle lifecycle is to better be able to capture less obvious agreements that may be safety relevant. Some such examples may be interactions with diverse passengers in a robotaxi; making sure safety-relevant information on updates becomes known to all users of shared use vehicles; choice of route (may be safety-relevant in dangerous areas); interactions at maintenance, transport and decommissioning or when encountering emergency vehicles; interaction with vehicle occupants following ADS failures; or inter-dependencies between several automated functions in the same vehicle (mix-ups - mode confusion among several functions).

3) Defining Stakeholders: Stakeholders that may be part of agreements are listed, we divide stakeholders into three categories each with a different type of relation to the CAV:

- *Users* - human users of an AFUA equipped vehicle. This may be a driver, local or remote operator (i.e. a professional driver), passenger or dispatcher[2].
- *Proximal stakeholders* - persons in the vicinity of the AFUA equipped vehicle, such as users of other (manual or automated) vehicles, or vulnerable road users such as pedestrians and cyclists.
- *Distal stakeholders* - persons or entities with a more indirect relation to the AFUA, such as government agencies, insurance companies or other groups or individuals. More often relevant for agreements in general, i.e. disregarding safety relevance (see [5]), but may sometimes have safety implications. Note that a remote driver should be treated as a user and not a distal stakeholder.

4) Listing Functional Agreements: Given the function description together with selected concerns, lifecycle, and stakeholders, the final step of agreement analysis is to elicit all applicable agreements by considering which combinations of lifecycle/stakeholder that will constitute an agreement for the AFUA. For ISO 26262 users, this can be compared to how hazardous events are derived from relevant combinations of operational situations and hazards. In the agreement analysis, which is part of the concept stage of development, *functional agreements* are listed. These are agreement descriptions on a high abstraction level without any implementation details. To aid the further analysis, we also propose to sort the agreements into three classes:

- *Operational agreements* - situations with one decision point and one action on short time-frame, e.g. a software update of a parameter in the automated function that changes the immediate response behaviour of the automated driving or driver assist system.
- *Tactical agreements* - medium time-frame containing multiple decision points and actions, that could be represented by a decision tree, e.g. a control transition.
- *Strategical agreements* - long time-frame such as a trip or up to the operational lifetime of the vehicle, e.g. liability distribution between manufacturer, owner, and user.

Following system engineering principles [15], a functional agreement will be refined into a *logical agreement* and finally into an exact technical solution. E.g., if the functional agreement is a control transition from human to ADS, the logical agreement would describe how that control transition is performed in the user interface (protocol, buttons, display symbols etc.), and the system design would describe the exact technical implementation. The logical agreement and system design is analysed in the interaction analysis.

C. Interaction Analysis

Interaction analysis (step [3] in Fig. 1) is described in-depth in our previous work [6], which we refer to for more detailed information. In short, potential hazards are listed for each agreement, e.g. mode confusion, unfair transition and stuck-in-transition would be relevant for a control transition agreement [16]. Three tools are then used to find potential weaknesses in the HMI design that may trigger one of these hazards; sequence diagrams, cause-consequence analysis, and fault tree analysis (FTA). Fig. 5 in the example of Sec. V shows results

[1]The agreement analysis is based on our previous work in [5] but updated and expanded in this paper.

[2]Taxonomy of users from [3] and [8].

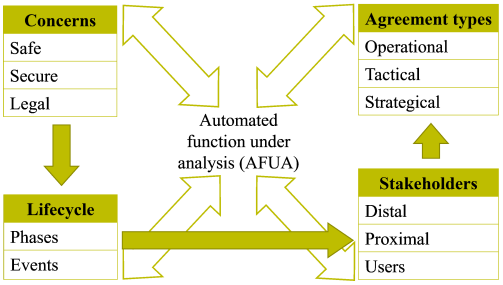


Fig. 2: Agreement analysis dimensions.

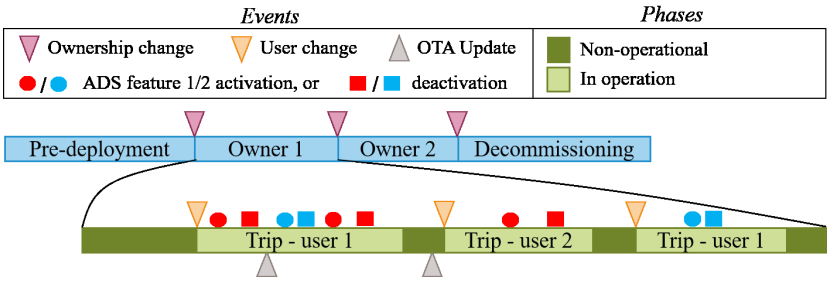


Fig. 3: Lifecycle example for an AFUA.

from each of these tools. Sequence diagrams are made for each agreement showing interactions between the automated function and a stakeholder through the relevant interface. Both the intended interaction and potential erroneous sequences should be illustrated. Based on the sequence diagrams, cause-consequence diagrams (CCDs) can be constructed; the sequence diagrams will be useful for identifying potential initiating events for a CCD, i.e. events that may eventually lead to a hazard given an undesired outcome. A CCD forms a tree showing both desired and undesired outcomes of a series of events. For each undesired outcome, an extended FTA is conducted including both potential faults in the E/E system and human errors that may lead to the same undesired outcome. In this work, we propose that the fault trees can also be supplemented with attacks (similar to attack trees) to be able to find and mitigate malicious activities as a cause of the undesired events. An example of this is shown in Fig. 5d.

It remains future work to expand the interaction analysis to better suit all agreements types, as well as investigate the potential to use simulation- or driving studies to complement the expert-based analysis in early development stages.

D. Risk Assessment

Based on the interaction analysis, a risk assessment (step [4] in Fig. 1) is conducted. Risk assessment can either be quantitative (probabilistic) [17] or qualitative. In [6], we propose to use a qualitative risk assessment similar to criticality ranking in FMECA [18], applied on the fault trees from interaction analysis. All faults that are rated as critical would then be subject for redesign or risk reduction measures. This has the advantage of being possible to apply using expert knowledge complemented with sources such as results from driving studies (on-road, off-road, and virtual simulation to identify potential human errors) and hardware metrics (for E/E components). A fully quantitative assessment requires more statistical data but, if possible to conduct, could be used towards a probabilistic safety case useful with approaches such as establishing a positive risk norm [3] or the QRN approach [19], which states top-level safety requirements in terms of maximum allowed frequencies of accidents resulting in different severity. HISA could be used with any risk assessment method that can provide a useful link between the interaction analysis results and necessary risk reduction measures. Attempting to find a useful method for establishing a quantitative risk contribution is left as future work.

It is important to note that the overall risk of the AFUA can only be determined by a hazard analysis and risk assessment (HARA) considering the function at vehicle level, which is not the purpose of HISA. However, see Sec. IV for a discussion on how HISA can be used embedded in a safety lifecycle with top-level safety requirements from such a HARA.

E. Risk Reduction

If the initial risk (based on the risk assessment) is unacceptable, the risk needs to be reduced (step [5] in Fig. 1). This can be done either by *redesign*, that is altering the specification to obtain a product with lower or no inherent risks, or by applying additional *safety measures* to reduce risks. Altering the function may be necessary if analysis shows that the nominal functionality of the initial design is unsafe or insufficiently specified, e.g. like ISO PAS 21448 [2] treats functional insufficiency by functional modification. It can also be applicable if altering the functionality is a better (e.g. lower risk, lower cost) solution than applying additional safety measures. However, if changing the function does not reduce risks sufficiently, or if modifications would reduce the value proposition of the product, the remaining option is to apply safety measures. Measures can fall into the categories of fault prevention, fault removal, fault tolerance, or fault forecasting [20]. For E/E systems ISO 26262 [1] provides a development lifecycle describing how to apply many such measures.

If a redesign is performed, the function will no longer have the specification assumed in the agreement and interaction analysis steps, hence it is necessary to go back and update these earlier phases, beginning with an agreement impact analysis, see Sec. III-G. When only other safety measures are used, work can continue on detailed design and V&V.

F. HMI Verification & Validation and Safety Report

The safety relevant aspects of the HMI and functional agreements are first defined in the concept phase (cmp. Fig. 4a) and refined in system design. The implementation must be verified to correctly implement these agreements (step [6] in Fig. 1). While V&V methods is not the main topic of this paper, we note that a verification and validation plan for HMI would always include at least a well-informed heuristic evaluation, and preferably clinics with simulated or road testing where

possible. In fact, it would be arguably necessary to include user testing on at least a semi-regular basis in highly iterative design environments.

In the development phases logical agreements can be populated with configurable ranges, and well-known methods such as equivalence- and boundary-value analysis be part of the test strategy. We use the term *concrete agreements* meaning specific instances (specific parameters) of the logical agreements[3]. The main verification effort lies with well constructed concrete agreements, where all relevant parameters in the agreement are defined. ISO 4804 discusses suitable HMI test environments [3] and the HEADSTART project a harmonized test procedure [22] that could be useful for defining test scenarios with concrete agreements. The validation should additionally focus on testing to make sure any assumptions made in the previously discussed analysis steps are true.

The collective results from all previous steps are denoted HMI safety analysis (SA) report (step [7] in Fig. 1). We suggest it can be used as evidence of a safe HMI in a safety case for the AFUA.

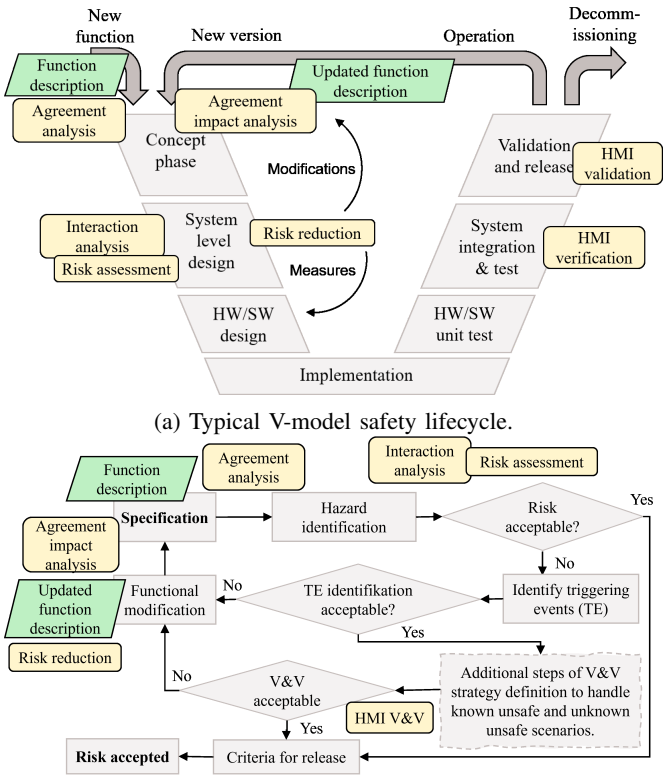
G. Updates and Agreement Impact Analysis

It is becoming increasingly important to be able to update vehicle functions frequently. Some reasons are that connectivity has added remote attack vectors which means it is necessary to be able to deploy updates quickly to fix security and safety weaknesses, that automated functions may require updates due to external changes in the environment (e.g. changed/expanded ODD), to adapt to policy changes (e.g. new traffic rules or regulations for automated vehicles), or for the business value of being able to provide improvements to the product after initial sale.

Updating safety-related functionality will entail planning the updates to make sure that the appropriate safety activities are performed together with the functional change so that a complete and consistent safety case is in place before every release. Hence, for an update of the AFUA, the function description needs to be updated to reflect planned changes (step [8] in Fig. 1) and an agreement impact analysis needs to be performed (step [9] in Fig. 1). The impact analysis entails revisiting the agreement analysis given the updated function description with the aim to identify if the change will alter or add any agreements. For all new or changed agreements the remaining steps of the process must also be repeated. This work is simplified when HISA is integrated in a development process with solid traceability, as discussed in Sec. IV.

IV. HISA in a Safety Lifecycle

As HISA only provides safety analysis for the HMI aspect of an automated function, it is intended to be integrated in a full development process. A V-model is often used to illustrate a development lifecycle for safety-critical products, e.g. in ISO 26262 [1]. In a V-model, the left side shows design phases, where successive refinement and analysis of the design is conducted, ending with implementation. The right side shows different verification phases, and at the top final validation. Fig. 4a shows a generic V-model, and how HISA steps would correspond to its phases. The agreement analysis can be seen as part of the concept phase, where input is a function description of the planned product (*item definition* in ISO 26262). In a safety lifecycle, the concept phase would also contain a hazard analysis on vehicle level, resulting in top-level safety requirements (*safety goals* in ISO 26262). Some of these safety requirements would be assigned to HMI-related components in system-level design phases (corresponding to functional and technical safety concepts in ISO 26262). As interaction analysis is performed given a proposed HMI implementation, it would be part of the system design safety analysis. It should also be verified that all identified agreements actually have a corresponding HMI in the system design! Risk reduction by functional modification would lead to some iteration in the early development phases, while the HMI V&V phases can be performed in conjunction with the corresponding V-model V&V phases. In this figure, a loop-back corresponding to starting development of a new version of a function has been added to show where agreement impact analysis at function updates fit in.



(a) Typical V-model safety lifecycle.

(b) SOTIF workflow (simplified).

Fig. 4: HISA in a development lifecycle.

While HMI analysis is not in scope of ISO 26262, ISO PAS 21448 [2] (SOTIF) explicitly includes HMI safety, and for automated vehicles these two standards are often proposed

[3]This agreement terminology is analogous to how scenarios are defined as functional, logical, or concrete in the Pegasus method [21].

to be used in conjunction. The E/E part of the HMI would then be developed according to ISO 26262, while the influence of human error is treated with ISO PAS 21448. The lifecycle described in ISO PAS 21448 is not based on the V-model, and focus for risk reduction is functional modification. Fig. 4b illustrates how the HISA steps corresponds to a (simplified version of) the SOTIF workflow. While there is another example HMI analysis method in ISO PAS 21448, we believe HISA can be an alternative, for reasons discussed in Sec. II.

Both safety and cybersecurity for an ADS (SAE level 3+) are also the topic of ISO TR 4804. This report refers to ISO 26262, ISO PAS 21448, and ISO SAE 21434 Automotive cybersecurity [23][4] but focuses on application towards an ADS. It specifically mentions the HMI issues of control transition, operating mode and responsibility awareness, potential lingering effects of automated mode, behaviour in traffic while in automation mode (dHMI) and communication with other road users when necessary (eHMI), as well as potential technologies and test procedures to use. UL 4600 - Standard for Safety for the Evaluation of Autonomous Products - takes another route of listing which kinds of hazards must be considered in a safety case and lists many more topics for human interaction than mentioned in this paper. As the standard is goal-oriented and lists what the safety case argument must consider, rather that which methods must be used, we believe HISA can be one appropriate analysis tool towards fulfilling its requirements regarding hazards and risks involving human interaction.

V. Example Use-Case

Our example AFUA is a traffic jam chauffeur (TJC), a function that can temporarily take over the driving task from a human driver in congested traffic[5]. The function description is presented in Table I. An agreement analysis is carried out according to Sec. III-B and documented in Table II. The description as well as analysis is partial and only meant to illustrate the method. Additional details for both function behaviour and HMI implementation would be needed for a full analysis. As an L4 function, the ADS always has a fallback not requiring intervention, however control transitions may be susceptible to transition hazards. Interaction analysis has been carried out for one of the functional agreements, a mode change scenario where control transition from human to ADS is performed. Fig. 5a shows a sequence diagram with human user (HU) and ADS (our TJC function) communicating via the HMI, and illustrates an incorrect TJC available signal that did not actually originate from the ADS itself at point (1), but at (2) the human driver nevertheless attempts activation. Fig. 5b shows initiating events from this sequence, and Fig. 5c a corresponding CCD for initiating event 1. Finally, Fig. 5d shows the two fault trees from the CCD, including both E/E errors, human errors, and attacks that could cause the faulty behaviour. Our example does not include the risk analysis, risk reduction or V&V steps of the process as these are not the focus of the paper.

[4]Standard expected to be released in 2021.

[5]Cmp. [3], Annex A, however we use a SAE L4 TJC instead of L3.

TABLE I: TJC example – Function description.

Intended Behaviour	
Nominal function	Can be enabled and take over driving task from manual driver in congested traffic within ODD (see below). Function max speed is 60 km/h, following a lead vehicle, and performs no lane changes.
Fall-back	Controlled stop-in-lane when nearing ODD exit or due to ADS failure.
Driving modes	Manual driving mode (MD-M) and automated traffic jam chauffeur mode (TJC-M).
Automation level	Unsupervised automated driving, restricted ODD.
Update policy	Over-the-air updates only when vehicle is non-operational. Driver notified of update including any behaviour changes before first trip after update.
ODD[a]	
Scenery	Motorway, divided with barrier, uniform surface, lanes$\geq$ 2 with markings.
Environmental conditions	No rain or snow, clear or cloudy, daytime or artificial lighting, positioning and V2X connectivity.
Dynamic elements	Dense traffic with low flow rate (congested), very few vulnerable road users or animals.
HMI	
aHMI	Mode and TJC available display symbols. Mode switch (two paddles, hold for 2 s).
eHMI	External light bar & V2V message showing TJC-M. Hazard warning lights active at safe stop.
dHMI	Smooth acceleration/deceleration. Adhering to safe following distance with margin.

[a]The ODD uses a subset of attributes from [24] mostly with qualitative metrics (e.g. low, few) as better precision is not needed for the example.

TABLE II: TJC example – Agreement analysis.

Concerns	Safety, security.
Lifecycle phases & events	
Phases	Owner $\rightarrow$ user1, user2, non-operational.
Events	OTA update, user change, CTJ-M enable/disable.
Stakeholders	
Users	Driver, passenger(s).
Proximal	Drivers of other vehicles.
Distal	None.
Functional Agreements	
Operational	Mode information (driver, drivers of other vehicles) Function parameter update (all users).
Tactical	Mode change (driver).
Strategical	Major function update (all users).

VI. Conclusions and Future Work

As vehicle functions become more complex and provide a higher degree of automation, new types of interactions with humans are also introduced. In order to make sure all interactions are considered and designed so that they are safe, HMI safety analysis methods are needed as part of the safety assurance. In this paper, we propose a framework with some tools for human interaction safety analysis. While the framework as described could be used for manual analysis by functional safety and human factors experts, there are also several areas - some already mentioned in the paper - left for future work, where the framework could be improved and give the users more support. Some examples are formalized agreement notation including handshakes (well-defined points where agreements are entered), improved interaction analysis

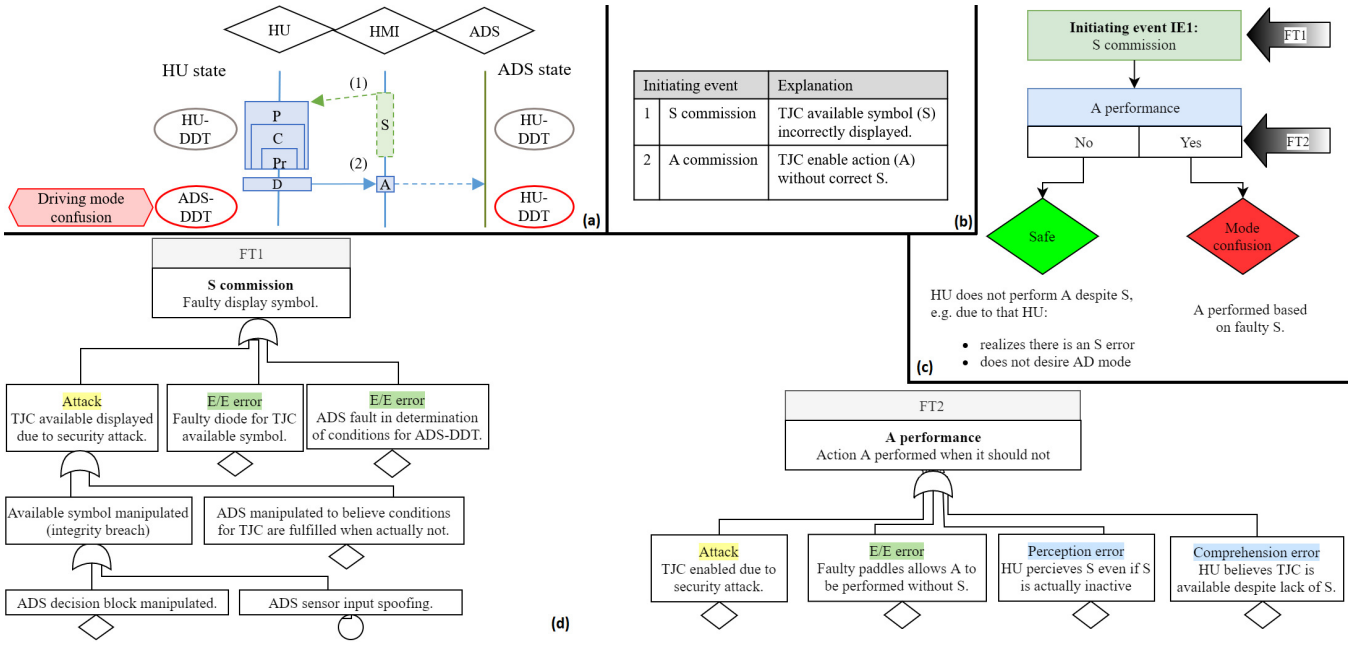


Fig. 5: TJC example – Sequence diagram (a), initiating events (b), cause-consequence diagram (c), and fault trees (d).

with better security integration, methods to establish quantitative contribution to risk, and use of simulation and driving data to strengthen analysis results. Finally, validation of the process on a larger use-case and a more in-depth comparison with other methods is planned for our future work.

References

[1] ISO, "ISO 26262:2018 Road vehicles – Functional safety," 2018.

[2] ISO, "ISO/PAS 21448:2019 Road vehicles – Safety of the intended functionality," 2019.

[3] ——, "ISO/TR 4804:2020 Road vehicles — Safety and cybersecurity for automated driving systems," 2020.

[4] UL, "UL 4600 - Standard for Evaluation of Autonomous Products, Edition 1," 2020.

[5] M. Skoglund, F. Warg, and B. Sangchoolie, "Agreements of an automated driving system," in *37th International Conference on Computer Safety, Reliability, & Security (SAFECOMP 2018) - Fast Abstract*, Vasteras, Sweden, Sep. 2018. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01878603

[6] F. Warg, S. Ursing, M. Kaalhus, and R. Wiik, "Towards safety analysis of interactions between human users and automated driving systems," in *10th European Congress on Embedded Real Time Software and Systems (ERTS 2020)*, Toulouse, France, Jan. 2020. [Online]. Available: https://hal.archives-ouvertes.fr/hal-02441382

[7] R. Parasuraman, T. B. Sheridan, and C. D. Wickens, "A model for types and levels of human interaction with automation," *IEEE Transactions on systems, man, and cybernetics-Part A: Systems and Humans*, vol. 30, no. 3, pp. 286–297, 2000.

[8] SAE, "SAE J3016 - Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles," 2018.

[9] K. Bengler, M. Rettenmaier, N. Fritz, and A. Feierle, "From HMI to HMIs: Towards an HMI framework for automated driving," *Information*, vol. 11, no. 2, p. 61, 2020.

[10] D. Dey, A. Habibovic, A. Löcken, P. Wintersberger, B. Pfleging, A. Riener, M. Martens, and J. Terken, "Taming the eHMI jungle: A classification taxonomy to guide, compare, and assess the design principles of automated vehicles' external human-machine interfaces," *Transportation Research Interdisciplinary Perspectives*, vol. 7, p. 100174, 2020.

[11] M. Risto, C. Emmenegger, E. Vinkhuyzen, M. Cefkin, and J. Hollan, "Human-vehicle interfaces: the power of vehicle movement gestures in human road user coordination," in *2017 Driving Assessment Conference*. University of Iowa, 2017.

[12] S. A. Shappell and D. A. Wiegmann, "The human factors analysis and classification system–HFACS," 2000.

[13] C. Martinie, P. Palanque, R. Fahssi, J.-P. Blanquart, C. Fayollas, and C. Seguin, "Task model-based systematic analysis of both system failures and human errors," *IEEE Transactions on Human-Machine Systems*, vol. 46, no. 2, pp. 243–254, 2015.

[14] IEC, "IEC 61882 hazard and operability studies (HAZOP studies)—application guide," 2016.

[15] C. Haskins, K. Forsberg, M. Krueger, D. Walden, and D. Hamelin, "Systems engineering handbook," in *INCOSE*, vol. 9, 2006, pp. 13–16.

[16] R. Johansson, J. Nilsson, and A. Larsson, "Safe transitions between a driver and an automated driving system," *International Journal on Advances in Systems and Measurements*, vol. 10, no. 3-4, 2017.

[17] S. Kaplan and B. J. Garrick, "On the quantitative definition of risk," *Risk Analysis*, vol. 1, no. 1, pp. 11–27, 1981.

[18] U.S. Department of Defense, "MIL–HDBK–882D: Standard Practice for System Safety," 1998.

[19] F. Warg, M. Skoglund, A. Thorsén, R. Johansson, M. Brännström, M. Gyllenhammar, and M. Sanfridson, "The quantitative risk norm - a proposed tailoring of HARA for ADS," in *50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W) - SSIV Workshop*. IEEE, 2020, pp. 86–93.

[20] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE transactions on dependable and secure computing*, vol. 1, no. 1, pp. 11–33, 2004.

[21] "The pegasus method," 2019, accessed: 2021-04-11. [Online]. Available: https://www.pegasusprojekt.de/en/pegasus-method

[22] HEADSTART partners, "HEADSTART Deliverable D3.1: Guideline of a Comprehensive validation and certification procedure to ensure safe CAD systems," 2020. [Online]. Available: https://www.headstart-project.eu/results-to-date/deliverables/

[23] G. Macher, C. Schmittner, O. Veledar, and E. Brenner, "ISO/SAE DIS 21434 automotive cybersecurity standard-in a nutshell," in *International Conference on Computer Safety, Reliability, and Security (SAFECOMP 2020) Workshops*. Springer, 2020, pp. 123–135.

[24] BSI, "BSI PAS 1883:2020 Operational Design Domain (ODD) taxonomy for an automated driving system (ADS) – Specification," 2020.