Author accepted manuscript version of the publication in
2023 Annual Reliability and Maintainability Symposium (RAMS)
Published version: https://doi.org/10.1109/RAMS51473.2023.10088202

Autonomous Vehicles - Trust, Safety and Security Cases: The Complete Picture

Thor Myklebust, SINTEF Digital
Tor Stålhane NTNU
Gunnar D. Jenssen, SINTEF Community

Key Words: Safety case, cybersecurity case, trust case, safety, autonomous, public

SUMMARY & CONCLUSIONS

Safety cases are required by several functional safety standards, specifications, and guidelines. Cybersecurity cases have recently been required by ISO/SAE 21424:2021 for automotive and EN TS 50701:2021 for the railway domain. In this paper we discuss cybersecurity cases and suggest using the topics and structure for a cybersecurity case as described in Annex G of EN TS 50701. BSI PAS 1881:2022 requires: "*Trialing organizations shall develop and publish a publicly available and accessible version of the safety case*". We have already developed a "safety case for the public" [1] to ensure that (1) the public is aware that safety evidence exists, (2) they are aware of relevant safety aspects when they are passengers, and (3) the vehicle's limitations are described transparently.

Trust is a dynamic process that involves initiating and building trust, responding to violations of trust (failures), and trying to rebuild (repair) trust. The building blocks of trust are not limited to the vehicle itself but also include the embedded AI (Artificial Intelligence) and its overt function. Trust is a holistic perception of the complete service, technology, and organizations responsible for developing, implementing, and certifying an autonomous vehicle.

An autonomous vehicle will need acceptance from the certification bodies and the authorities, but we also need to gain the public's trust. Our research found that several aspects are missing in the safety and cybersecurity cases to ensure public trust.

To make self-driving buses a success, they need to be considered trustworthy. Thus, we need a "Trust case" that includes evidence related to distinct trust aspects. Our literature studies, focus groups [4], and surveys found that trust and safety are not correlated. We have developed a "Trust case" to cover the factors not included in the safety and cybersecurity cases. The resulting "Trust case" approach is currently in the form of specific information topics presented in a layman form and a safety case for the public [6], and specific trust topics in [7]. Further research is necessary, related to topics such as deep learning, security, and incorrect reporting to the driver due to e.g., false positive results.

1 INTRODUCTION

Safety cases are required by several functional safety standards, specifications, and guidelines. Cybersecurity cases have recently been required by ISO/SAE 21424:2021 for the automotive domain and EN TS 50701:2021 for the railway domain. We suggest using the topics and structure for a cybersecurity case as described in EN TS 50701. BSI PAS 1881:2022 requires trialing organizations to develop and publish a publicly available and accessible version of the safety case. Trust is a dynamic process involving initiating and building trust, responding to violations of trust, and trying to rebuild trust.

An autonomous vehicle will need both safety & security acceptance from the certification bodies and the safety authorities, and they need to gain the public's trust. Our research found that several aspects are missing in the safety and cybersecurity cases to ensure public trust. Most literature in the area addresses cognitive trust, i.e., the rational, statistical, and engineering aspects of trust. Emotional trust has received little attention.

Self-driving buses need to be considered trustworthy. Thus, we need a "Trust case". To ensure that we have the complete picture, we need a safety case, a cybersecurity case, and a trust case.

2 BACKGROUND

2.1 The TrustMe project

The TrustMe project started on August 1, 2020 and will last until June 2024. The project's main goal is to develop a safety case for autonomous buses and a safety case for the public. Safety cases are important when establishing sufficient confidence in the technology. The long-term goal is a regular operation with passengers without an operator on board the bus. Trials have started in Norway in 2022, where the operator of the self-driving bus is moved to a remote-control room for surveillance and possible control handover if incidents cannot be handled safely or correctly by the self-driving bus. The safety & trust cases shall justify the trust of several user groups, such as passengers and fellow road users, the government, and the insurance industry, by bringing together a large amount of

information that documents the safety level.

2.2 Relevant safety, security, and AI standards, technical reports and specifications

A publicly available specification (PAS) aims to speed up standardization in areas of rapidly evolving technology and generally respond to an urgent market need. A Technical Report (TR) is informational.

Safety standards, technical reports, and specifications are important because they say what should be done by e.g., manufacturers to claim that we have achieved a certain goal – in our case, a certain level of safety, security, and trust. For the automotive domain, the ISO 26262:2018 [8], ISO/PAS 21448:2019 [10] SOTIF (Safety Of The Intended Functionality), UL4600:2022 [16] for autonomous products, and BSI PAS 1881:2022 [12] are relevant safety standards. ISO 26262, UL4600, and BSI PAS 1881 require a safety case to be developed by the manufacturer. The important part for the passengers and the public are the safety requirements based on accident severity, exposure, and controllability that is strongly related to the autonomy level [17]. The challenge comes from the fact that all these factors are decided based on qualitative descriptions, and controlled experiments have shown that qualitative assessments vary widely both for experts and laypersons [19]. However, the ISO 26262 safety standard is a good starting point for discussing automotive safety with laypersons. All this opens up for interesting and important discussions. For self-driving cars, the two first factors – severity and exposure – are related to the traffic. The third factor – controllability – will create requirements for the self-driving car's control system.

The ISO/SAE 21434:2021 security standard [9] is developed to help the automotive industry define a structured process to ensure that the manufacturers incorporate cybersecurity into the design of road vehicles and busses, including their systems, components, software, and connections to any external device or network. The standard specifies the cybersecurity risk management requirements for the design, development, production, operation, maintenance, and decommissioning of road vehicle electrical and electronic systems. The standard includes requirements for "distributed cybersecurity activities" and discusses the cybersecurity relationships between OEMs (Original Equipment Manufacturer) and Tier 1 and 2 suppliers. Tier 1 is a partner with which the OEM conducts business, while Tier 2 suppliers are where Tier 1 suppliers get their materials.

AI standard, technical report, and a specification:

IEEE P7001:2022 [13] "*Standard for Transparency of Autonomous Systems*" includes measurable, testable levels of transparency for autonomous systems. Autonomous systems, and the processes by which they are designed, validated, and operated, will only be transparent if this is designed into them.

This standard provides a framework that helps developers of autonomous systems review and includes design features into those systems to make them transparent. The framework sets out requirements for those features, the transparency they bring to a system, and how they would be demonstrated in order to determine conformance with this standard.

ISO/IEC TR 24027:2021 [14] "*Bias in AI systems and AI aided decision making*" specifies three types of bias: (1) Human cognitive bias, which is important since it influences both the selection of data used as training sets for ML (Machine Learning) and the engineering decisions made throughout the ML development process. Human cognitive bias will come into play when we process or interpret information. (2) Data bias, which will influence the ML system since the data used to train and test the ML – in addition to the system model – will define the ML system's behavior. This bias may stem from design decisions and constraints imposed by developers or management in addition to existing human cognitive bias. How we define the data and how we collect themes may also introduce bias. (3) Bias introduced by engineering decisions is caused by decisions related to requirement, design, choice of parameters, etc.

ISO/IEC TR 24028:2020 [3] "*Artificial intelligence - Overview of trustworthiness in artificial intelligence*". This document surveys topics related to trustworthiness in AI systems, including approaches to establish trust in Al systems through transparency, explainability, controllability, etc.

ISO/IEC TR 5469 draft 2022 [15] "*Functional safety and AI systems*" states that: *there is limited guidance on specification, design, and verification of trustworthy AI systems or on how to apply AI technology for functions which have safety-related effects*. For functions released with AI technology, such as ML, it can be difficult to explain why they behave in a particular manner. In case of continuous improvement of the model using AI technology, the verification and validation activities undertaken during the development of the function could be undermined as the function behavior progressively moves away from the rigorously tested, ideally deterministic and repeatable behavior.

2.3 Safety case and cybersecurity case

Manufacturers and operators want to convince their customers that the vehicle is safe. At the top level, a safety case goal is simple to imagine. The statement "The system is safe because…" says it all. Whatever follows "because" is a safety case [5]. The purpose of a safety case is to inform the reader – e.g., a safety assessor – about the following:

- What you have done to make the system safe.
- How it contributes to safety and compile evidence that you have developed.
- What you claim to have done, including proof that the persons who did the job had the right competencies.

The ISO/SAE 21434 cybersecurity standard includes requirements for a cybersecurity case to be developed by the manufacturer. The cybersecurity case shall provide a high-level argument for the achieved degree of cybersecurity. Patching is weakly described in the ISO/SAE 21434. If patching is necessary, one should perform an impact analysis to evaluate whether safety is impacted. When safety is impacted, the safety case has to be updated. If not, a security patch can be performed by the manufacturer. Security patching is described in IEC TR 62443-2-3 [18] "*Part 2-3: Patch management in the IACS*

environment". It is important to have an agile process for software development to be able to update the software quickly

2.4 Trust case

Trust differs from safety and reliability [2, 7] and is used in several ways, depending on the application area. Trust and risk should be considered in different ways to manage uncertainty [20]. According to Perrow, trust may be used in two ways [21]:

- Reliability trust: the degree of uncertainty that is associated with a specific transaction partner, e.g., the subjective probability that a transaction with this partner – e.g., a trip with a bus – will be successful.
- Decision trust: the extent to which an entity is willing to enter into a transaction (interaction) with another.

Trust is about both technology and psychology. We have seen that the terms used by the public are mostly related to psychology while the terms used by engineers are mostly related to technology. In some fora, trust is used in a rather informal way so that trust, reliability and reliance are all used to identify the same thing. Trust can also be seen as a person-to-person relationship. In this case, trust is a relationship between social actors such as designers, creators, or technology operators.

We need to understand what influences the customers' behavior. To achieve this, we have looked at two types of models:

- Psychology: Ajzen and Fishbein's model for planned behavior.
- Technology: The technology acceptance models (TAM). Even though the TAMs are technical, most of the components are still psychological.

We have run one survey with 54 participants and four focus groups with five to ten participants. When analyzing all the collected information, the findings indicate two types of trust: what it is **now** – situational trust – and how it might develop over time – learned trust. The problem with the trust models we have looked at up until now – e.g., TAM and model for planned behavior- is that they are static. To include a dynamic copoint, we have adapted the tri-part trust model of Hoff and Bashir [22], as shown in the figure below.

The top-level trust arguments – situational trust, system performance, and design features are taken from [7], while the evidence is taken from our survey and focus group inputs.

The use of machine learning, such as deep learning, often result in systems that are complex and difficult to interpret. This is the case when developing autonomous vehicles. Explainability is a means to enhance assessor and user trust in the models. We have started to study this topic, and the results will be published in a later paper.

Current ADAS (Advanced Driver Assistance System) is developed so that there are too many false positives (incorrectly indicating the presence of a condition) to be on the safe side. This may lead to less trust in modern vehicles and should be studied further. Recent research has also shown that "Partially automated driving has higher workload than manual driving:" [31].

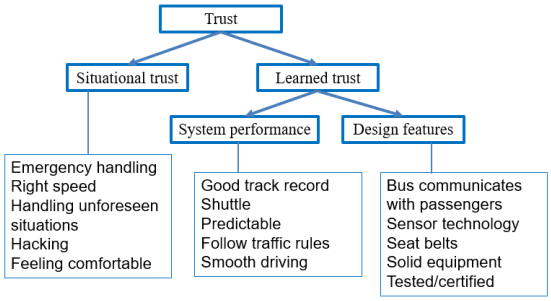

Figure 1: The trust case

2.5 Cognitive and emotional trust

In a review of human trust, Glikson and Wooley [27] argue that trust could be both cognitive (rational thinking) and emotional (affect). These types of trust might differ in their antecedent. The review shows that emotional trust is not commonly addressed in human relations with technology. However, emotions are known to significantly affect human trusting behaviors. Making a robot or a car look or act like a human or a living thing (anthropomorphism) affects users (passengers) emotional reactions toward the technology. To understand passengers' cognitive trust, there is a growing need to understand what and how such features of the technology affect human emotions and emotional trust in autonomous vehicles.

The car industry has for a long time been aware of the role of emotions and affective computing as avenues for increasing a passenger's sense of comfort, safety, and trust. A review by Eyben et al. [29] concludes that "socially competent" interfaces need to be developed. A socially competent interface can influence users' emotional states in several ways, e.g., through engagement, feedback, assistance by a digital assistant, and personalization through personal settings, personalized conversation, greetings, etc., preferably by natural speech. In a review of in-car interface design with partial and increasing automation, Petterson and Ju [28] argue that automotive design is changing from a study of separate HMI (Human Machine Interface) solutions to interaction design considering cultural aspects. Interaction design is important when developing different cognitive and emotional AI solutions, considering how people from different regions and cultures will interact with automation.

The relationship between user and vehicle is transformed with full automation: the human is no longer always in control. Driving becomes a partnership with shared control where most driving tasks except ordering the automated vehicle, entering the vehicle, and possibly stopping the vehicle are controlled by the vehicle AI. The user interaction with the self-driving vehicle becomes a multi-sensory whole-body experience and full-body interaction.

This interaction involves subtle psychological mechanisms creating positive or negative expectations external to the vehicle and internal during use.

An example: When you have an experience with an

elevator, it is the subtle psychological mechanisms that create the overall impression. Odor, sounds, how it moves, the pressure in your ears, tactile properties of push buttons, and how the door opens and shuts. This is an interaction with the elevator itself. In addition, it is the context, i.e., the waiting area, the building the elevator is in, seen from the outside, which affects expectations and affective, emotional preferences or dislikes associated with trust.

Waymo has taken interaction design one step further to create trust in highly automated vehicles when the driver is removed from the vehicle [30]. Waymo accepts that user interaction with the self-driving vehicle is a multi-sensory whole-body experience with full-body interactions. When arriving, since there is no human driver, the voice takes over some of the former driver's tasks, like announcing the arrival and reminding them not to forget anything in the car. Sound is also used to comfort people when they enter the car. The use of ambient sound helps users to feel more at ease. Further, Waymo recognizes that transparent visual communication of what the vehicle sees and where it intends to drive is crucial for establishing trust. The most prominent communication happens via the two screens mounted on the headrests. Waymo has developed a tool that uses the camera feeds of the car to highlight what the sensors on the vehicle are seeing. The essential information is displayed as a feed from the cameras transformed into an abstract animated map. Cognitive and emotional trust is related both to technology and psychology. Interior design and user communication are subtle and overt psychological attributes of emotional trust enabled by technology. Design attributes of highly automated vehicles will reduce uncertainty and enhance experienced control and a feeling of caretaking in a transparent way.

3 COMMUNICATING SAFETY, SECURITY AND TRUST

This section is based on the guidelines for risk communication published by the US agency SAMHSA [23]. Communication to the public related to risks has four components – (1) what are the risks, (2) how likely are they to occur, (3) what have we done to prevent them, and (4) what should you do if they occur anyway? We will give some short comments to each of these components below.

- What are the risks? First – tell no lies and do not cloud the truth, you ***will*** be found out sooner or later. If it is something you do not know, say so. If done properly, informing people of existing risks will not scare them but build confidence.
- How likely are they to occur? Do not use statistical terms, such as "The probability of this event is 10^{-6}" Many people will not understand this. Saying "It will occur to 1 in a million" will not help much either – people will think "that one could be me". Most people tend to personalize risk in the same way as safety analysts de-personalize it. This is also a question of trust, and we already have a trust-case for autonomous buses.
- What have we done to prevent them? This is where the safety case comes in. The safety case represents our arguments about why we think the system is safe and what we have done to be able to reach that conclusion.
- What should they do if an accident occurs? There need to be emergency instructions available in all the autonomous buses.

The four items in the list above should also be discussed on the service provider's homepage or app and be easily available to the public. This homepage or app should also contain information such as "No accidents reported for the last X months". It should be possible for the public to post questions related to safety there. In addition to the issues discussed in the list above, the bus service provider should have a home page or app where people can ask safety-, trust- and security-related questions. The questions and their answers should be available to everyone. This will show that you have nothing to hide and will also show how you plan to handle possible problems.

4 THE COMPLETE PICTURE

4.1 The link between safety and security

There is a strong link between being safe and being secure. If the system is not secure, it is probably not safe. But there can and will be parts of the vehicle's safety system that are distinct from security. Some mechanical and electrical systems can still work autonomously from software control. Cyber security threats change faster than safety threats. Some similarities exist between ISO 26262 [8] and ISO/SAE 21434 [9], e.g., plans for safety and security, culture, responsibility, configuration, and impact analysis. There might also be some gains when combining safety and security for the completeness of the relevant analysis.

4.2 The link between safety and trust

Trust differs from Safety in that trust cannot be estimated but can be ***based*** on previous experiences – own and others. The goal of the TrustMe survey is to try to understand people's perception of the term's "safety" and "trust", not to reach a final, scientific definition of the two terms. This understanding is important when we want to communicate with potential customers of self-driving buses. Two examples of short responses from the survey are

- Having trust refers more to your own experience and feeling of safety
- Being safe is a more objective evaluation of whether you are in danger or not

Some of the responses were rather lengthy, e.g.: "To me, having trust means that you have an innate belief that this thing/person is correct/safe/logical, and you wouldn't have the need to question it since you have experienced it to be true. You feel a complete calmness and safeness.

You give up your critical thinking about the person/thing since you have put your trust in it. It hasn't let you down or given you any evidence that this trust was put in a bad place".

There was no general agreement on the description of safety and trust [8]. The survey tells us that trust has wider interpretations than safety – six categories vs. four categories. The most frequent category for Trust is "feeling comfortable (Table 1 below), followed by "relying on somebody" while the

most frequent category for Safety is “objective evaluation, flowed by "not being in danger” Alternatively, we can say that: *Having trust* is if *you believe* that the risk is worth taking, i.e., a subjective evaluation while *safety is* whether or not a thing *is dangerous* for people, i.e., an objective evaluation.

Table 1: Trust and safety results

Trust	N	Safety	N
Feeling comfortable	15	Objective evaluation	14
Relying on somebody	14	Not in danger	13
Belief	9	Feeling safe	11
By choice	4	Handle accidents	6
Subjective evaluation	4		
Building confidence	2		

4.3 The complete picture

In order to gain acceptance for self-driving buses (AV), there are four groups that must be considered – each with its own needs and requirements: the road traffic authorities, the safety assessors, the AV passengers, and the rest of the public, such as pedestrians and people riding bicycles. In all cases, trust, reliability, and safety will come into play but in different proportions. Suppose we consider all the worries raised by ten persons or more out of the TrustMe survey’s 54 respondents. In that case, the common requirements for all three groups are that the AV shows predictable driving and safe speed and follows all traffic regulations. They all need to trust the bus’ handling of traffic situations but in different ways. These results are supported by the results of four TrustMe focus groups.

- The road traffic authorities and the assessors' main concern is safety, compliance with relevant standards, and reliability. Their acceptance of AVs is a two-step process – first approval for testing in real traffic, and after that, a final approval and certification before it can enter the streets in real traffic. The reliability assessment and the safety case are the most important documents. The reliability assessment is needed to know the problem frequencies, while the safety assessment is needed to understand the size of the consequences.
- The bus passengers – their main concern is trust, i.e., do we trust an AV? Safety and reliability are also important but only as long as they influence trust. According to the TrustMe survey, their main requirements are that the AV is tested and certified, that it has a good track record, seat belts, and is comfortable. In addition, the AV should communicate with the passengers in an efficient and pleasant way.
- The general public – their main concern is their own safety. However, this is a highly diversified group containing, among others, pedestrians, people on bicycles and people in ordinary cars. An earlier survey done by the TrustMe project shows that common requirements for cyclists and pedestrians are that the AV keeps a good distance to pedestrians and cyclists, that is, signals early if it intends to change lane or change direction and that the AV can “see” cyclists and pedestrians.
    - The special requirements for pedestrians are that the AV stops at pedestrian crossovers and that the AV is marked as self-driving.
    - For cyclists, the special requirements are that the AV is marked with lights for better visibility, that there are separate lanes for AVs, and that it is programmed to handle unpredictable driving from cyclists.

To sum up – we need reliability [8 part 5, 24] and safety to get the self-driving bus certified [25], and we need safety analysis to convince the general public that it is safe to move around in an area used by AVs – that they “see” the pedestrians and cyclists and take precautions not to run them over. The AV’s passengers are concerned that the AV is tested and certified. All in all – we need safety and reliability information to build a safety case for the public and a trust case for the AV users.

Note that pedestrians and cyclists only are concerned with situational trust and system performance. Only the AV passengers are concerned with all three components of the trust case – see fig 2.

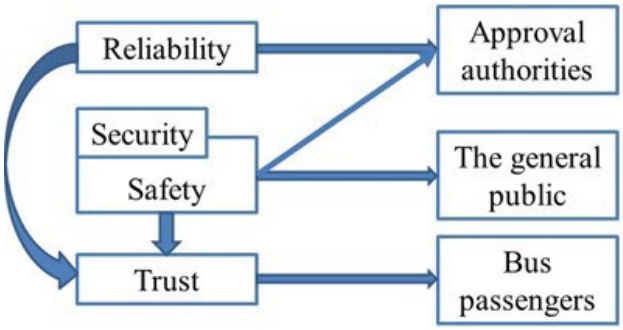

Figure 2: Trust case and the related components.

Acknowledgments

This work has been supported by The Norwegian Research Council, Project name "TrustMe", project number: 309207 - IPOFFENTLIG19.

REFERENCES

1. T. Myklebust, T. Stålhane and S. Wu. Agile safety case for vehicle trial operations. PSAM16 Hawaii 2020
2. T. Stålhane and T. Myklebust. Trust and acceptance of self-driving buses. ESREL 2022, Dublin.
3. ISO/IEC TR 24028:2020, Information technology - Artificial intelligence - Overview of trustworthiness in artificial intelligence.
4. J. Kontio, L. Lehtola and J. Bragge. Using the Focus Group Method in Software Engineering: Obtaining Practitioner and User Experiences. Proceedings 2004. International Symposium on Empirical Software Engineering (ISESE'04)
5. T. Myklebust and T. Stålhane. The Agile Safety Case.

ISBN 9783319702643. Springer International Publishing. February 2018.
6. T. Myklebust, T. Stålhane, G. D. Jenssen and I. Haug. TrustMe, we have a safety case for the public. ESREL 2021 Angers France
7. T. Stålhane and T. Myklebust. Trust Case and the link to safety case. SAFE 9th International Conference on Safety and Security Engineering. Rome, Italy 2021-11
8. ISO 26262:2018 series. Functional safety for road vehicles
9. ISO/SAE 21434:2021 Road Vehicles - Cybersecurity
10. ISO/PAS 21448:2019 Road vehicles - SOTIF
11. EN TS 50701: 2021 Railway applications - Cybersecurity
12. BSI PAS 1881:2022 "Assuring the safety of automated vehicle trials and testing - Specification"
13. IEEE P7001:2022 Standard for Transparency of Autonomous Systems
14. ISO/IEC TR 24027:2021-11 Bias in AI systems and AI aided decision making
15. ISO/IEC TR 5469:draft 2022 Functional safety and AI systems
16. UL4600:2022. Standard for Safety for the Evaluation of Autonomous Products
17. J3016:202104. Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles
18. IEC TR 62443-2-3:2015 Patch management in the IACS environment
19. Stålhane, T and Malm, T.: Risk Assessment - Experts vs. Lay People, ESREL 2016
20. Frederiksen, M.: Trust in the face of uncertainty: a qualitative study of inter-subjective trust and risk. Dept. of Sociology and Social Work, Aalborg University
21. Perrow, C.: Normal Accidents, 1984, pg. 326
22. Hoff, K.A and Bashir, M: Trust in Automation: Integrating Empirical Evidence on Factors That Influence Trust, Academy of Management Annals. September 2, 2014
23. Risk Communication Guidelines for Public Officials. SAMHSA Publication No. PEP19-01-01-005. Rockville, MD, Substance Abuse and Mental Health Services Administration, 2019.
24. https://ec.europa.eu/growth/sectors/automotive-industry/technical-harmonisation/faq-type-approval-vehicles_en
25. Norwegian trial Law: LOV-2017-12-15-112
26. G. Costantino, M. D. Vincenzi, and Ilaria Maeucci. In-Depth Exploration of ISO/SAE 21434 and its correlations with existing standards. IEEE Communications Standards Magazine • March 2022
27. E. Glikson, A. W. Woolley (2020). Human trust in artificial intelligence. Review of empirical research., March 2020.
28. I. Petterson and W. Ju. Design Techniques for Exploring Automotive Interaction in the Drive towards Automation. DIS '17: Proceedings of the 2017 Conference on Designing Interactive SystemsJune 2017 Pages 147–160
29. F. Eyben, M. Wollmer, T. Poitschke, B. Schuller, C. Blaschke, B. Farber, and N. Nguyen-Thien. Emotion on the road—necessity, acceptance, and feasibility of affective computing in the car. Advances in Human-Computer Interaction. Vol. 2010, Hindawi Publishing Corporation.
30. R. Powell R. "Trusting Driverless Cars. How Waymo designed an experience that reassures riders every step of the way", March 2019. (accessed on 02/07/2022). https://design.google/library/trusting-driverless-cars/
31. Jisun Kim et al. Partially automated driving hRas higher workload than manual driving: An on-road comparison of three contemporary vehicles with SAE Level 2 features. Human factors and ergonomics in manufacturing & service industries. Wiley 2022

BIOGRAPHIES

Thor Myklebust
SINTEF Digital, Trondheim, Norway

e-mail: thor.myklebust@sintef.no

Senior researcher, Safety&Security. His experience is in certification of products and systems since 1987. Myklebust has participated in several international committees since 1988. Member of safety (IEC 65), the IEC 61508 committee and railway (CENELEC/TC 9). He has co-authored three books and published more than 270 papers.

Tor Stålhane
NTNU, Trondheim, Norway

Email: stalhane@ntnu.no

Professor emeritus. He started his career in compiler development. He then moved on to safety and reliability, did a PhD in applied statistics and has since then been working on safety analysis of software-intensive systems. He has co-authored five books, all related to safety.

Gunnar Deinboll Jenssen,
SINTEF Community, Trondheim Norway

e-mail: gunnar.d.jenssen@sintef.no

Senior Research Scientist. Jenssen's experience covers 30 years' in safety and mobility research. PhD in Roads and Transport Engineering. Master's in psychology. He has been responsible for several projects related to Automated Driving. He has contributed to four books and published more than 200 papers.