Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022)
Edited by Maria Chiara Leva, Edoardo Patelli, Luca Podofillini, and Simon Wilson
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-5183-4_R25-06-532-cd

Outline of a risk management framework for future transport systems

Surbhi Bansal,

Proactima, Norway. E-mail: surbhi.bansal@proactima.com;

Caroline Metcalfe

Proactima, Norway. E-mail: caroline.metcalfe@proactima.com

Roger Flage

University of Stavanger, Norway. E-mail: roger.flage@uis.no

Henrik Bjelland

Proactima & University of Stavanger, Norway. E-mails: henrik.bjelland@uis.no

Anders Jensen

Proactima & University of Stavanger, Norway. E-mail: anders.jensen@proactima.com

Willy Røed

Proactima & University of Stavanger, Norway. E-mail: willy.roed@proactima.com

Future transport systems, through the application of cooperative intelligent transport systems (C-ITS) promises safety improvements, increased efficiency of the road network and reduced climate impact. The benefits are hinging on increased automation and autonomous vehicles. Replacing humans with machines offers superior performance on repetitive and information-intensive tasks. Individual, inter-vehicle and dynamical understanding of the traffic pattern will lead to inter-vehicle adaption of behavior and reduce reaction times and prevent more critical situations from occurring. These benefits do not come about without challenges associated with e.g., automated and human controllers' interactions, algorithms and value judgments, vague system boundaries, vulnerability to malicious acts, regulation and standardization and liability issues in case of accidents. In this paper we outline the relevant contents of a risk management framework to support studies on implementation of future transport systems.

Keywords: risk management, complex socio-technical systems, intelligent transport systems, automated mobility.

1. Introduction

Integrated intelligent transport systems (IITS) is an example of what new combinations of advanced technology can enable. In its simplest form, it is about creating step-by-step improvements in our current transport system, for example by developing more advanced driver support systems that better enable the individual driver to avoid and handle challenging situations. In a more extreme form, it is about developing systems that completely change the way the transport system is built and used. We can imagine that transport will be a service we buy. Today's drivers will be the future's passengers. Replacing humans with machines offers superior performance on repetitive and information-intensive tasks. Individual, inter-vehicle and dynamical understanding of the traffic pattern will lead to inter-vehicle adaption of behavior and reduce reaction times if critical situations occur. IITS is the key to such a disruptive change.

These benefits do not come about without challenges. The nature of human-machine interactions will change, challenging cognitive capabilities of human controllers (Norman 2015; Merat & Lee, 2012; Biondi, Alvarez & Jeong, 2019). Judgments based on values and situations, previously attributed to drivers, will become

integrated in algorithms. System boundaries will fade, as autonomous machines become tightly coupled, amongst themselves and other parts of the society (Perrow, 1999). Malicious actors will be able to take advantage of cyber vulnerabilities and initiate major cascading events (Sou et al., 2022; Liu et al., 2020; Rayin, 2018; Yagdereli et al., 2015). Implementation of innovative systems challenge conservative regulations, standardization processes and diverging stakeholders' values (Geistfeld, 2017; Claybrook & Kildare, 2018).

Accidents involving partly autonomous vehicles already raise questions about ownership of consequences and liabilities. Currently, there is intense interest in research, standardization, and piloting of new technology to identify use-cases, societal opportunities and benefits, ethical dilemmas, hazards, etc. of future transport systems.

Existing risk management approaches are criticized (e.g. Leveson 2011) for not treating new and complex systems holistically, and thus unfit to explore the risks of software-controlled socio-technical systems. Our overall aim is to develop a framework to support studies on implementation of future transport systems, by integrating strengths of both traditional risk management and systems thinking. In this paper we report on our current findings towards an adapted risk management framework. Traits of socio-technical systems in general and intelligent transport systems are identified and described.

In section 2 we describe the iterative design method of developing the framework. Section 3 contains a brief overview of system's characteristics. Section 4 include a description of the adapted framework, while section 5 highlights some parts of its application on a simple example. Section 6 includes a discussion and, finally, there are some concluding remarks in section 7.

2. Method

Our framework design process is inspired by McMeekin et al. (2020), cf. Figure 1. The approaches combined include adapting existing methods and guidelines, employing experience and expertise, literature review, iterative development and refining & validating through piloting/trialing. The resulting framework is a product of existing risk management literature, past experiences, and knowhow about IITS systems together with a framework development methodology.

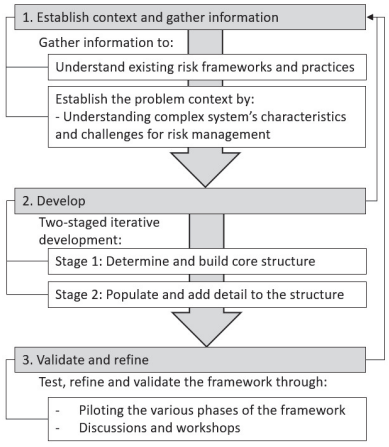

Figure 1 Framework development methodology

Step 1 involves *establishing the context and gathering information*: An understanding of the current practices and existing risk management frameworks is established. Industrial standards and frameworks consulted for this purpose are ISO 31000:2018 (2018), NS 5814 (2021) and the IRGC risk governance framework (Florin and Bürkler, 2017) and their main features, limitations and challenges are benchmarked. Understanding is built around complex systems (representing the future transport system). Key characteristics are identified, sorted, and integrated.

Step 2 includes *development*: Iterative development of the risk management framework. The first stage builds the core structure of the framework (three main phases). It is inspired by the widely adopted ISO 31000 standard and assumes a top-down, iterative, and incremental approach for managing risks of complex socio-technical systems. The features benchmarked in the previous phase are incorporated into the core structure. In the second development stage, the core structure is populated with details by logically implementing the solutions to the challenges of complex systems' characteristics identified previously.

Step 3 is about *validation and refinement*: The framework is tested, evaluated and refined by piloting its phases. Several rounds of internal discussions and workshops were also conducted. The feedback from the evaluation exercise is used to advance the framework in subsequent iterations.

3. System characteristics and threats

3.1. System characteristics

IITS systems share some common or at least often-present characteristics. The review of characteristics here is based on reports from a knowledge-building internal workshop. In the workshop, an initial set of characteristics were listed in a brainstorming session, followed by a structuring/clustering of system characteristics, resulting in the following list:

- Complexity: Decompositional, interactive, dynamic, and non-linear.
- Structural characteristics: Scalable (size, shape, prevalence, type), hierarchical and emergent properties/emergence, openness (vague boundaries) and multiple actors/stakeholders
- Intentionality and adaptability
- Novel (sometimes one of a kind)

Leveson (2011) identifies four types of complexities as one of the reasons differentiating simpler systems of the past from today's systems. These are briefly described and discussed for their implications for risk management:

Decompositional complexity involves a lack of consistency between the conceptualized system model and its actual structure. Then, reductionism or breaking complexity into most basic parts is not meaningful for framing high-level problems such as safety and security. Reductionist approaches can overlook system's underlying behavior, structure, and organization.

Interactive complexity is about the nature and scale of interactions among system components (e.g., physical components, networks, stakeholders, etc.). Stakeholders can raise interactive complexity when framing the risk problem, given the variety in their roles, expectations, and risks. They perceive the system from different (and often conflicting) viewpoints, whose integration is a big challenge.

Dynamic complexity relates to system changes over time because of internal or external factors. These changes, whether as developments or degradations, cause relevancy issues for problem framing, hazard & threat identification, setting safety margins, etc. Describing the system's long-term dynamics is equally demanding.

Non-linear complexity is the lack of obvious cause and effect relationship to explain system behavior. The presence of a combination of long value chains makes problem framing, understanding system behavior and placing barriers effectively beyond the ability of a single domain's expert.

Additionally, our internal workshop identified issues related to *scalability* and *novelty*.

Scalability is the ability to increase or decrease a system's performance to cater to changing demands (such as changing resource or functionality needs). This along with the aspects of size, shape and type should be estimated appropriately or else one risks underestimating the system's attack surface and selecting inappropriate measures of risk treatment(s).

Novelty is about the uniqueness about the system due to a lack of previous experience. One-of-a-kind systems lack previous characterizations, suffer from poor problem framing and uncertain scope. Novelty often presents newer risks requiring non-traditional means of assessment and treatment. Analysts might make weak assumptions in the process.

Table 1. Example of results from workshop on challenges and solutions

Framework phase: Planning – Problem framing	
Challenges	Systemic behavior: reductionist approaches are usually inappropriate. Emergent properties: "safety", "security", "sustainability", etc. Challenging to be precise and concrete when the perspective is large and includes many elements. Abstract models and concepts not necessarily appropriate for analyses.
Solutions	Frame the problem as a system problem, not a component problem. Clarify system perspective. Define system, sub-systems, components, and systems-of-systems. Clarify scope of work and any assumptions. Whose problems are we solving? Identify stakeholders: how would they frame the problem differently than originally considered? What views have not been included? Document this for transparency. Iterative development of problems and analyses.

While there are many more challenges, these complexities can majorly impact risk assessment, treatment, validation, and communication.

For instance, for risk communication, these complexities make it difficult to establish a reasonable level of risk understanding, disseminate information comprehensible for all stakeholders and ensuring a high level of trust.

Held together with the generic risk management frameworks identified, challenges and associated solutions related to each characteristic were identified in another workshop. An extract of the resulting table is shown in Table 1.

3.2. Threats and vulnerabilities

An exhaustive list of threats against and vulnerabilities of IITS systems cannot be listed here. This is not only due to space constraints, but also due to the ubiquitous challenge of completeness in risk identification and since, while typical for such systems, all the identified threats may not be relevant for all specific systems.

Nevertheless, interconnectedness, extensive digital value chains, software control, human-machine interfaces, etc., are example of common traits of the systems, which underpins specific hazards driving the design of this framework. Generally, there is a need to include both unintentional (e.g., extreme weather and electricity shortage), unwanted intentional (e.g., specification errors in software, unforeseen system adaptions and software updating) and malicious intentional threats (e.g., cyber-attacks and sabotage).

In addition to events or scenarios the systems are subjected to, hazards could also relate to *lack of system control*, e.g.: failure to maintain safety constraints, inconsistency between process behavior and process models, and lack of information about system state to update process models (Leveson et al., 2004).

The characteristics described in section 3.1 have implications for system vulnerabilities. The non-linear complexity characteristic implies, for example, that it may be difficult to assess vulnerability as the link between a given threat and the consequences is poorly known. The same applies for novel systems, due to lack of experience with operating similar systems.

The structural characteristics imply, for example, an interconnectedness such that different consequences will exhibit dependence or association, and that a single threat may lead to consequences in several parts of the system.

Finally, the intentionality and adaptability are especially associated with human and social aspects, which may have both a negative and positive effect on the system vulnerability. Intentional malicious acts from within the system represent a considerable threat to future transport systems. On the other hand, human adaptability within the system will be able to react to events that occur and reduce negative consequences.

4. Adapted risk management framework

Our aim is to develop a framework to assist risk management practitioners in various problematical situations associated with future transport systems. It should provide a direction of thinking flexible enough to understand, assess and manage risks of complex systems in general. The framework should not be confused with a method or process, that is a defined set of steps to be taken to achieve our goal.

The framework is structured into the three phases: plan, assess, and manage, iterated across in a top-down fashion.

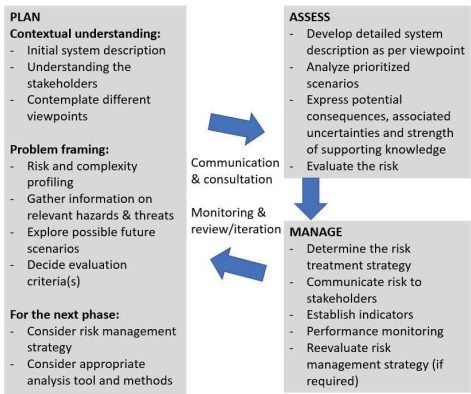

Figure 1 Suggested risk management framework

4.1 Planning phase

The basis is to understand the major elements that influence the assessment, such as the system and its complexities, the involved stakeholders, and the risk problem.

Our starting point is that understanding these elements needs simultaneous development. System description and/or risk problem may, for instance, depend on stakeholders' viewpoints.

The initial description provides guidance on what information is needed to complete a more detailed system description within the assessment phase and profile the system's complexities against each complexity factor in Section 3.1. This profiling helps to communicate the different types of system characteristics that influence the strategies and methods used to manage the risk of the system.

We regard stakeholders and "possible futures" as different viewpoints/contexts for the assessments. Identification and understanding of stakeholders, their viewpoints, and the values that they want to protect is central. Regulatory agencies and associated system requirements are one example of relevant "stakeholders". We introduce foresight techniques or scenario thinking as relevant tools to explore possible futures.

By choosing a viewpoint or viewpoints for the assessment, the system will be analyzed from various perspectives, over various assessments, allowing for a better understanding of the system's complexity.

The hazard and threat information gathered does not need to be an in-depth collection at this step, but enough to help the assessor develop understanding of the problem, which is important in deciding the evaluation criteria in correspondence with the way risk is assessed.

The next step is to create a risk problem profile. The dimensions include some characteristics suggested by Aven (2014) and our own suggestions from practical experience of working with clients. The six dimensions are: ambiguity among stakeholders, familiarity of the risk problem, time and budget constraints, risk appetite, the potential for extreme consequences and the uncertainty related to the consequences.

By considering the risk problem profile alongside the stakeholder participation the risk management strategy(s) can be determined. Such strategies could be: follow and ensure compliance with current standards, a risk-informed approach, a robustness or resilience-based strategy, a discursive strategy or a combination of these strategies. See Aven (2016) for more information.

Finally, the risk analysis methods are selected. The term "risk analysis" here is used in a broad sense, where the interest is assessing possible (future) consequences and their uncertainties using the most relevant methods and techniques given the problematic situation, stakeholders' viewpoints, the problem profile, the system's complexity, and the analyst's competence. The results of the selected methods also need to able to be evaluated within the chosen criteria.

4.2 Assessment phase

A detailed system description is developed that is relevant to the viewpoint(s) and method(s) of the analysis decided upon in the planning phase. Note that there might be different system descriptions and different assessment methods depending on the viewpoint selected.

Initial potential scenarios to be analyzed may emerge from the planning phase and the prioritization is determined based on the selected viewpoint/perspectives(s) and the risk management strategy(s). Additional scenarios will emerge during the iterative process of the risk management framework, and the prioritization will be re-evaluated. The potential consequences related to the prioritized scenarios are then expressed, along with the associated uncertainties and the associated knowledge of which the analysis assumptions are based on. The risk problem can then be evaluated in the context of the prioritized scenarios.

4.3 Management phase

Once the assessment of the risk has been carried out, risk evaluation is used to decide upon what the risk treatment strategy(s) are. The risks need be communicated to the targeted/relevant stakeholder in a way which addresses their needs and understandings. Performance monitoring indicators should also be established to monitor if the risk treatment strategies are having the desired outcome in the long run and that the values which the stakeholders want to protect are being protected. Finally, the risk management strategy(s) are re-evaluated.

5. Example of application on an autonomous robotic cleaning machine

We now briefly describe some results from using the framework's *planning phase* on a pilot study. The purpose is mainly to illustrate our development of "risk problem" understanding.

Originally, it was perceived as a technical design problem. During the process, risk associated with the implementation process became more central.

In the pilot, a Norwegian municipality is considering a machine learning driven autonomous road cleaning robot to replace the existing manual road cleaning as a pilot project. The robot has sensors and cameras that provide data to its algorithm governing operations such as target area mapping, navigation, conducting road cleaning for dry waste collection and dumping operations autonomously. The pilot project's key operational and technical specifications are anonymized to preserve confidentiality.

An initial understanding of the system was obtained through discussions and available documentation. This was followed by stakeholder mapping workshop which saw participation from different stakeholders (system integrators, operator, road authorities, municipal body, contractors, etc.). Using inputs from the workshop, stakeholder assessment and value assessment was conducted and consequently the viewpoint of the road regulatory authorities (high impact, high influence stakeholder) was selected for the first iteration round. However, the stakeholder mapping and assessment exercise revealed important insights early on. It was found that the public, as a stakeholder, was missing from the conversation. In a socio-technical system such as this, the people of the community would be impacted most by the direct and indirect consequences of a poorly implemented technology in their immediate vicinity (e.g., parking lots, shopping arena, roads, etc.). While the public may not be able to directly impact or influence the outcome of this pilot significantly, their participation is crucial for building a holistic contextual understanding. Similarly, inputs from insurance industry's players were missing and they can play a major role in establishing trust for this technology in the society.

Without understanding their needs, concerns and pains, the risk management can be narrow in its scope. One might fail to identify important hazards and threats and develop an incomplete risk picture for a stakeholder group. For instance, what novel hazards/threats can this robot present for special attention groups such as older citizens and physically impaired people?

This has implications for the treatment phase as well. A system-level consideration reveals that important measures such as an incident logging system and grievance addressal system are missing. Clarity is needed on the role of the police, who would usually be the immediate point of contact for the affected public if an incident were to happen. How will they handle such cases, do they have access to incident footage, etc.? Given the absence of an insuring party, how would the incident liability be resolved, who reimburses the affected people? Such questions are clearly important for managing the risk of such dynamic and novel systems. From the risk communication perspective, the public needs to be aware on how to interpret this technology, its implications, their role around it, handling emergency scenarios, etc.

When interpreting the political aspect, scenarios around people losing road cleaning jobs to autonomous machines may escalate in the future. New emerging risks such as data privacy and citizen security issues can also be raised. Such scenarios should be identified and analyzed using a systems approach following a discursive strategy.

6. Discussion

6.1 Fundamental design of the framework

The overall goal for the development of this framework is to make risk management practitioners more capable of adding value to the processes of innovating, designing, and implementing new and complex transport systems. From this practical standpoint it was considered important to maintain familiarity with known frameworks, while also keeping the framework flexible to a broad set of approaches to measure safety or risk. Consequently, the framework builds on the known structure of ISO 31000, involving the major steps of *planning*, *assessing*, and *managing*. This choice may indicate a strong connection towards risk assessments as the preferred tool within the framework. Risk assessments will play a major role, but we also acknowledge the strong link towards systems theoretical safety approaches, such as Leveson's STAMP (Leveson, 2011). An important difference between risk approaches and systems theoretical approaches is that the former uses events, or scenarios, as key elements of the analysis, while the latter highlights analyzing of control structures. Both approaches are designed to support decisions regarding the prevention of

future losses in social-technical systems, whereas the risk-based approach are also designed to manage opportunities of *taking risk*. Our definition of risk is broad, encompassing *future consequences of the activity and associated uncertainties* (Aven, 2014). As systems theoretical approaches are intended to prevent future, i.e. uncertain, losses, through better enforcement of safety constraints, we argue that it falls under our understanding of risk. Further development of the framework, through more piloting, will investigate any semantical and practical inconsistencies that may still exist.

6.2 System challenges and framework design

The framework addresses *decompositional complexity* by incorporating an overtly iterative and top-down approach following a plan-do-check-act sequence. The attention is on acquiring relevant information and knowledge discovery about system configuration (sub-system, hierarchies, interfaces, components, actors, etc.) that emphasizes on systematic determination of several aspects:

- Incremental system description.
- Stakeholder and worldview mapping.
- Clarify the high-level emergent properties.
- Open-ended management strategy early on.

To manage *interactive complexity,* emphasis has been placed on stakeholder mapping/assessment and value assessment early in the planning phase. This step identifies and assesses all the system stakeholders for their impact, influence, needs and system viewpoints and ultimately visualize actors in relation to each other. Prioritizing stakeholders and strategizing their management as per their role, values, and stakes in the complex system lifts the risk management's focus to a higher system- level thinking where an attempt to understand the underlying structure, mindset and goals is made.

Dynamic and *non-linear complexities* are served best employing a combination of scenario and systems thinking. Once stakeholders and their values are prioritised on degree of importance, a scenario thinking is applied to determine which scenarios can cause pains in different phases of the system's lifespan. Using this as an input, the scenarios are prioritised and analysed iteratively using an appropriate systems approach to assessment, such as STAMP by Leveson, (2011).

The framework focuses on describing the system incrementally to manage *scalability*. First in the planning phase, and then iteratively enriching our understanding in the assessment phase. This is done employing different system viewpoints (with respect to shape, size, configuration, time horizon, etc.) and constructing multiple visualizations for comprehensiveness, if required.

Novel systems may require novel tools for information discovery and regulation may be lacking. Suitability of the risk assessment tool/methodology is often overlooked in this regard. The framework sets a specific step for careful selection of the tool(s) and methodology(s) in the subsequent phases based on its strengths, weaknesses, limitations, and suitability for the context.

An overall iterative approach, that goes into detail incrementally is useful in general for managing the above complexities and their challenges. With each subsequent run, the effort and resources are diverted towards solving granularities of subsequently critical aspects as they become visible. This combined with a top-down approach counters the traditionally reductionist way of understanding the system.

6.3 Feasibility of the framework

Currently, the framework rests heavily upon theoretical considerations and less upon practical pilot studies. From this point on, our intention is that the shaping of the framework mostly will come from practical application through pilot studies and projects for clients. This reflects that this is an iterative design process. This also include determining and reflecting upon relevant quality criteria, i.e. how should we measure that the framework adds value to a problematical situation? Considering that we are dealing with future consequences of dynamic socio-technical systems, the framework cannot be validated in the ordinary sense of the word by comparing predictions with historical or experimental data. Work remains on these issues, but we suggest establishing trustworthiness by systematically addressing the quality criteria for qualitative research, such as credibility, transferability, dependability, and confirmability (Shenton, 2004; Guba, 1981; Njå et al., 2020).

7. Conclusion

Our findings suggest future transport systems are recognized by several complexity factors which makes us question the appropriateness of existing risk management methods. Based on the general traits of complex IITS, an adapted risk management framework is suggested and will be developed further through the "SIITS project". The final version of the suggested risk management framework needs to include guidance on a broad set of attributes, e.g., the significance of different scientific perspectives; definition of context, purpose and problem for the study; clarification of the study's scope, e.g. what system level(s) to consider; understanding the risk managers' role in the innovation team and process; characteristics and specific hazards of intelligent transport systems; identification of stakeholders' values, and; include relevant tools for analysis and visualization and communication of results.

Acknowledgement

This paper is partly funded by the Research Council of Norway through the PILOT-T research program. The authors are grateful for the insightful comments from our team members in Proactima and our partners in the SIITS project. We also greatly appreciate the ideas and comments from five anonymous reviewers on a previous version of this paper.

References:

Aven, T. (2014). *Risk, Surprises and Black Swans: fundamental ideas and concepts in risk assessment and risk management*. Routledge.

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research 253(1),*Page 1-13.

Biondi, F., Alvarez, I. & Jeong K-A (2019). Human-vehicle cooperation in automated driving: A multidisciplinary review and appraisal. *International Journal of Human-Computer Interaction, 35(11), pp. 932-946.*

Claybrooke, J. & Kildare, S. (2018). Autonomous vehicles: No driver…no regulation? Science 361(6397)., pp. 36-37.

Florin, M.-V. and Bürkler, M. T. (2017). *Introduction to the IRGC Risk Governance Framework.* Lausanne: International Risk Governance Center.

Geistfeld, M.A. (2017). A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation. *California Law Review, vol. 105.*

Guba, E.G. (1981). Criteria for assessing the trustworthiness of naturalistic inquiries, Educational Communication and Technology Journal 29, 75–91.

International Organization for Standardization (ISO 31000), (2018). *Risk Management*

Leveson, N. Daouk, M., Dulac, N., & Marais, K. (2004). A Systems Theoretical Approach to Safety Engineering. Aeronautics and Astronautics Dept. Massachusetts Institute of Technology.

Leveson, N. G. (2011). *Engineering a safer world: Systems thinking applied to safety* (p. 560). The MIT Press.

Liu, N., Nikitas, A. & Parkinson, S. (2020). Exploring expert perceptions about the cyber security and privacy of Connected and Autonomous Vehicles: A thematic analysis approach. *Transportation Research Part F, 75(2020), pp. 66-86.*

McMeekin, N., Wu, O., Germeni, E., & Briggs, A. (2020). *How methodological frameworks are being developed: evidence from a scoping review.* BMC medical research methodology, 20(1), 1-9.

Merat, N. & Lee, J.D. (2012). Preface to the special section on human factors and automation of vehicles: Designing highly automated vehicles with the driver in mind. *Human Factors 54(5), pp. 681-686.*

Njå, O., Sommer, M., Rake, E.L. & Braut, G.S. (2020). Societal Safety - Analysis, Management and Evaluation (in Norwegian). Oslo: Universitetsforlaget.

Norman, D.A. (2015). The Human Side of Automation. In Meyer G. & Beiker, S.: Road Vehicle Automation 2. Springer.

Norsk Standard (NS 5814). (2021). *Requirements for risk assessment.*

Perrow, C. (1999). Normal Accidents: Living with High-Risk Technologies (First Published by Basic Books 1984). Princeton, New Jersey: Princeton University Press, 1999.

Raiyn, J. (2018). Data and cyber security in autonomous vehicle networks. *Transport and Telecommunications, 2018, 19(4), pp. 325-334.*

Shenton, A.K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. Education for Information 22 (2004) 63–75.

Suo, D., Moore, J., Boesch, M., Post, K. & Sarma, S.S. (2022). Location-Based Schemes for Mitigating Cyber Threats on Connected and Automated Vehicles: A Survey and Design Framework. *IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 4, April 2022.*

Yagdereli, E., Gemci, C. & Aktas, A.Z. (2015). A study on cyber-security of autonomous and unmanned vehicles. *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology 2015, 12(4), pp. 369-381.*