REPORT SIITS

WORKPACKAGE 1

New challenges for risk management of the future Integrated Intelligent Transport System (IITS)

Methods and Tools

SIITS

proactima

Client:	Contact person:
Workpackage 1	Surbhi Bansal

Abstract:

This report provides a brief overview of new challenges for managing the risks and vulnerabilities of the future transportation system. These challenges differ from those of the traditional systems due to more complexities, connectedness, autonomy, and interactions involved. The future transport system will involve multi-disciplinary collaborations from different domains to deliver safe, sustainable, and effective services to the Norwegian society. The identification of these challenges stresses on the need to adapt our current risk management methods.

Key word	IITS, risk management, challenges, mobility, methods
Report no.	1073996-RE-003
Author(s)	Surbhi Bansal
Confidentiality	Open
Revision no.	01
Date revised	17.10.2023
Pages	18

Rev.no.	Date	Reason for revision
00	16.05.2022	For internal review
01	17.10.2023	Final version

Prepared by	Verified by	For SIITS
Surbhi Bansal	Torgrim Huseby	Anne-Kari Valdal

Table of Contents

Abbreviations

Short form	Expanded form
ADAS	Advanced Driver Assistance Systems
AV	Autonomous Vehicle
C-ITS	Cooperative- Intelligent Transport System
FMEA	Failure Mode Effect Analysis
GDPR	General Data Protection Regulation
IITS	Integrated Intelligent Transport System
ISO	International Organisation for Standardisation
ITS	Intelligent Transport System
KPI	Key Performance Indicator
OECD	Organization for Economic Co-operation and Development
RVA	Risk and Vulnerability Analysis
SoS	System of Systems
V2I	Vehicle- to- Infrastructure
V2P	Vehicle- to- Pedestrians
V2V	Vehicle- to- Vehicle

Summary

IITS, the future of mobility, promises several benefits (such as safety, sustainability, and efficiency). It attempts to deliver these through integration among multiple novel ITS technologies. This not only disrupts the existing business models but also encourages new interactions among actors and stakeholders. Consequently, the future of mobility is complex and fraught with uncertainties and risks. This report explores the new challenges faced while managing risks associated with future IITS and underscores the need for updated risk management methods. The report begins by defining future IITS and enlists limitations associated with aspects of the risk management process (such as scoping, risk analysis and communication). It then highlights the shortcomings of traditional risk management tools and methods in understanding potential adverse outcomes of these complex systems. It addresses the need to account for the diverse stakeholder landscape and the absence of reliable validation methods. Overall, these insights demand reevaluating the current risk management practices, thereby, forming a strong basis for incorporating improvements systematically and logically.

The main finding of this report is that current risk management methods, although effective in the past, fall short when dealing with the evolving and complex nature of systems such as IITS. Thus, we suggest the need to modernize and evolve the current risk management framework to one that adopts a more iterative, holistic (systems thinking) and top-down approach. This will better equip risk managers to handle the multifaceted risks and uncertainties inherent in the future transport systems.

1 Introduction

1.1 Background

The future IITS

IITS is the system integrating various ITS technologies and services to optimize transportation systems and improve overall mobility. ITS technologies are enabled using dynamic- and present-situation related data/information from other entities (ISO 17427-2:2015). It comprises a dynamic and distributed computing environment with computing units in vehicles, roadside infrastructure, mobile devices, and central systems. It can be referred to as a system of systems (SoS). An important characteristic of such a SoS is that it consists of several interoperable systems (ISO, 17427-3: 2015). An *interoperable* system comprises of two or more systems that can exchange and use the exchanged information in a heterogeneous network (Geraci et al., 1991). Interoperability, i.e., seamless communication and cooperation among technologies is a complex issue. It requires enablers such as standards & protocols, data exchange, regulations, security, etc. In short, it requires technical-, organisational- and policy-related efforts. Given these characteristics, the future mobility system is a complex one. According to Johansen and Rausand (2011), 'complexity' refers to a state of difficulty in determining the output of a system based on knowledge about individual inputs and given our current knowledge base. The complexity grows with the number of installed systems (Bossom & Jesty, 2009) or number of integrated ITSs in this case. This threatens its effectiveness, manageability, maintainability, extendibility, refurbishment, and overall costs (Bělinová et al., 2010). At a broader level, the concerned stakeholders face challenges (such as ensuring safety, privacy, and security) arising from the interconnectedness and interoperability among systems.

General characteristics of IITS

The table below lists some of the elements of IITS and its characteristics.

Table 1 Features and characteristics of IITS.

#	Element	Characteristic
1.	Component	Multiple, dynamic, inter-connected and evolving (smart infrastructure, intelligent vehicles, regulations, technology, etc.)
2.	Agents	Intelligent, interacting (human and non-human)
3.	Information flow	High-speed, high volume, challenging to track
4.	Information processing	High-speed computations for real-time decision-making
5.	Interactions	Human-human, human-machine, machine-machine (growing)
6.	Stakeholders	Several, diverging interests, differing objectives
7.	Scalability	Highly scalable with no upper- limits

As per the table:

- the system comprises multiple dynamic components, including smart infrastructure, intelligent vehicles, regulations, and technology, which continuously evolve.
- Intelligent agents, both human and non-human, interact within the system.

- Information flows rapidly and at a high volume, making tracking its flow and ensuring quality as a challenging task.
- High-speed computations are used for real-time decision-making.
- Various types of interactions occur, including human-human, human-machine, and machine-machine. The number of machine-to-machine interactions are only growing in such systems.
- Stakeholders have diverging interests and objectives.
- The system is highly scalable with no upper limits.

The societal handling of risk (from 1950s) using conventional risk management has been a success story in almost all OECD countries (Murray & Lopez, 1996). This success has been well documented (Renn et al., 2022). Conventional risks (such as occupational accidents, traffic accidents, deaths, illnesses) have been reduced successfully following the linear ISO 31000 framework of identifying risks, assessing them, and finally treating them. This traditional methodology falls short in managing the risks of complex systems described so far. The situation is rendered further challenging by risks that are interconnected, non-linear, and often global in nature today. The traditional risk management approaches (methods and supporting tools) have been universally acknowledged for being effective so far. However, these no longer appear sufficient for providing guidance on how to manage emerging and systemic risks for systems with diverse technological interactions, unclear interfaces, and multiple subjective stakeholder perspectives. Today, there is a greater need to involve the stakeholders in risk management if such a system is to succeed. We elaborate on all these challenges in section 3.

1.2 Purpose

The purpose of this report is to address the emerging challenges in the field of risk management posed by complex Integrated Intelligent Transport System (IITS) of the future. As the landscape of transportation evolves as integrated and interconnected systems using advanced technologies, new complexities and uncertainties arise. This demands an evaluation of the effectiveness of the traditionally used risk management methods and tools. This report delves into the fundamental challenges faced in effectively managing the risks of the future IITS. For this, the limitations of the different steps of the risk management framework are discussed, for example, using bottom-up vs top-down approaches for risk assessment. Next, the report sheds light on the inadequacy of visualization tools available to risk managers, underscoring the need for such solutions that enhance their ability to identify, assess, and manage risks of IITS. By addressing these aspects, the report aims to provide inputs to other work packages in the SIITS project that are tasked with developing a more suitable risk management framework for complex systems.

1.3 Scope

This report focuses on exploring the challenges related to methods and tools used for risk management of the future IITS. While the report briefly talks about the nature, characteristics, and workings of complex systems, discussing these further falls beyond the scope of this report. It investigates the fundamental difficulties of understanding and analysing risks in integrated systems (i.e., complex interoperable systems) and strategic challenges in managing a diverse stakeholder landscape.

The report aims to look at both the social and technical aspects, since IITS is a fundamentally a ‘socio-technical’ system. The report also considers different ways to approach these challenges, i.e., bottom-up and top-down. It discusses the problems in visualizing this complex system and inadequacy of visualization tools. In doing so, the focus has been on addressing uncertainties that undermine our system understanding and impairs the ability to apprehend its future outcomes with

sufficient confidence. This eventually raises concerns about reliability and validity of knowledge gained from risk analysis. By addressing these aspects, the report aims to provide a clear understanding of the challenges risk management faces and some insights into what these methods need to address.

2 Method

This study employs three key methods to investigate challenges faced by risk management of the future Integrated Intelligent Transport System (IITS):

1. **Literature Review:** A thorough review of academic articles, research papers, and industry reports forms the basis of understanding the IITS challenges for risk management.
2. **Project partner's lecture and discussions**: Conversations with knowledgeable colleagues and expert project partners provide practical insights into identifying challenges. These conversations facilitated the identification of key challenges, as well as paved way for thinking about perspectives on potential strategies for mitigating risks within the IITS framework.
3. **Lecture Insights:** Valuable perspectives from lectures by project partners enrich our knowledge, offering focused exploration of specific IITS and risk management aspects.

By integrating insights from extensive literature review, project partner discussions, and lecture takeaways, this report aims to deliver a succinct but informed analysis of risk management challenges faced within the evolving IITS landscape.

3 Discussion

The traditional risk management methodology

Risk management entails the ability to making informed decisions and allocating resources wisely. ISO 31000 is a gold standard used by risk managers globally (Dali & Lathja, 2012). This internationally accepted standard presents risk management principles, framework and process as constituting a globally applicable reference guide for any activity, domain, or organisation. It lists the following steps for managing risks (see figure below):

- Establishing scope, context, and criteria
- Conduct risk assessment- consisting of risk identification, risk analysis and risk evaluation and
- Risk treatment

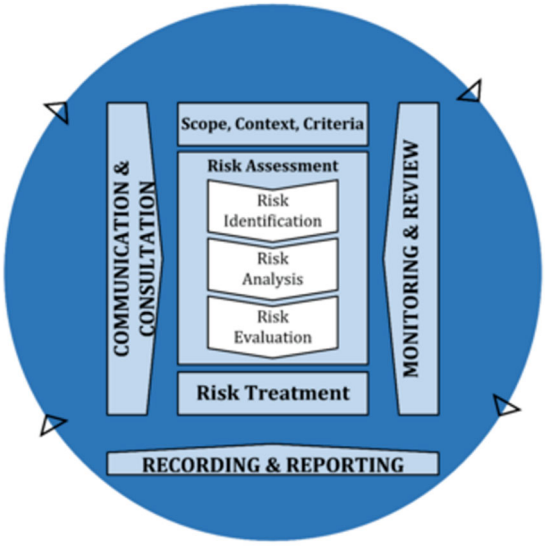

Figure 1 ISO 31000 risk management process

ISO emphasises on conducting the following throughout:

- Continuous monitoring of risk environment & review of framework
- Recording & reporting all developments and
- Communication & consultation with different stakeholders are ongoing and iterative activities carried out throughout the process.

Employing such a routine of above steps has become a familiar norm in the risk field. However, they are not sufficient when dealing with the complexities of today's dynamic and uncertain systems. This section discusses challenges encountered when following such a process in the IITS-context.

3.1 Methodical challenges

3.1.1 Challenges in establishing scope, context, and criteria.

This is associated with the challenges in establishing the scope, context, and criteria; the first step in risk management.

Scope

Scoping means defining boundaries around what will be considered in the risk management process. The system under investigation is one of them. A system is an interconnected set of elements that is coherently organized in a way that achieves some defined objective(s). A system broadly consists of the following (Meadows, 2008):

- Elements (tangible and intangible)
- Interconnections
- Function or a purpose.

The IITS is composed of several transport modes, infrastructure elements, network of spatially spread-out linked nodes, and flow of information, people, and freight. The system is built to serve several defined functions serving several purposes (such as enhancing safety, security, sustainability, effectiveness, etc.).

First and foremost, one needs to identify its key elements, functions, connections & interfaces. All this constitutes the scope of the system under investigation. In the IITS, identifying the elements is perhaps the only easy part. While it may be a challenge per se, it can be relatively easy to lose sight of the overall system perspective when meticulously identifying elements at progressively deeper levels for the sake of thoroughness. This can lead to scope creep, or uncontrolled expansion of system's scope over time that is beyond its original objectives. This can have implications for the overall quality of the exercise.

Next, the system's dynamic interconnections, system behaviour and functions are not so obvious either. ITS technologies are demonstrating increasingly novel and dynamic interactions such vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-pedestrians (V2P), etc., and less of the traditional human-human or human-machine interaction. These interactions are new and interfaces (see interoperability in section 1.1) are difficult to specify within a system boundary (which is often blurry). This makes it challenging to conduct the scoping exercise for a system with unclear/uncertain boundaries (face scope creep). Consequently, it becomes a matter of judgement on which risks are to be managed. Risk managers are prone to unknowingly overlooking the risks that might wrongly appear as 'seemingly non-critical'.

The functions and purposes of a system are even harder to see. One may argue that the purpose of the system is easily identifiable from its stated objectives and goals. However, Meadows (2008) specifically highlights that the purpose of a system is deduced from its behaviour and not from rhetoric or stated goals. For instance, in theory, an Advance Driver Assistance System (ADAS), aims to increase the safety of driving and parking activities, but its behaviour determines its true objective function. Furthermore, in a system as large as the IITS, risk managers are challenged for comprehensively identifying functions for the scope. The functions are often quite heavily interconnected (one-to-one, one-to many and many-to-many) and interdependent on each other. Understanding these interconnections and interdependencies is crucial. Selective addressal (or rejection) of functions can have undesired ripple effect on others. Validating that all relevant system aspects are adequately covered is an overall challenge. Leaving out seemingly inconsequential functions from scope can diminish the effectiveness of risk treatment.

One way of dealing with a large-scale complex system is to start by identifying (and later assessing) events that can threaten the reliability of the system's performance (Selvik & Signoret, 2020). This requires a systems-perspective to risk visualization, known as *systems thinking*. In systems thinking, the world is imagined as a collection of feedbacks (feedback loops and delayed effects), balancing, and reinforcing with differing strengths, causing complex behavioural patterns (Meadows, 2008). Adopting such a perspective helps in viewing the system as a whole and not as collection of individual components. Acknowledging interconnections, loops, emergent properties and cause-effect relationships implies lesser chances of excluding relevant aspects from the system's boundary.

Establishing the context is outlining the broader environment (of external and internal factors) within which an entity (or stakeholder) operates. Clarifying and understanding the context right in the beginning of the process can be easy when dealing with small and well-understood systems. But this is difficult in the IITS-context due to the presence of several interacting stakeholders. Each stakeholder has its own goals, concerns, and context. Then the challenge is which of these context(s) should be chosen? A single context can only provide limited insights on the factors governing a small portion of the system. Then how can multiple contexts be established for risk analysis? Which ones are most relevant? These challenges resurface when setting the criteria for evaluating and prioritising risks. Different stakeholders prioritise different values and thus, have different decision-making criteria to evaluate their risks on.

3.1.2 Challenges in visualizing system properties

Once, the relationships/interconnections in the system are identified, one should associate different functional, parametric, and emergent properties to the system's response behaviour. This is in line with Rouse (2015) who outlines that the two main concepts for understanding complex systems is by determining:

(1) dynamic response of the system as a function of its properties, and
(2) uncertainty of system's state (for controlling the complex system).

Emergent properties are unexpected behaviours that stem from interaction between the components of an application and their environment (Johnson, 2006). They are important from the risk perspective. These properties are not predictable from the properties of individual components. Hence, they can add uncertainty about the system's future state by violating safety requirements. This is referred to as the *emergent risk*. *Systemic risk* is another type of risk pertaining specifically to complex systems. It refers to the risk of breakdowns in an entire system, as opposed to breakdowns in individual parts or components and is evidenced by co-movements (correlation) among most or all parts (Kaufman & Scott, 2003). The interdependencies influencing the system performance such that fragility (dependencies) in the systems is a main reason that systemic failures occur (Venkatasubramanian, 2011). As already mentioned, IITS is a highly interconnected and integrated system, it is prone to the risk of failure in these interactions, connections and dependencies, materialising into emergent and systemic failures and disasters.

These properties are difficult to predict while analysing them to predict future systemic failures is even more challenging. For example. Marini et al., (2021) discusses the phenomenon of coordination of autonomous vehicles (AVs). This pertains to what is known as the coordination risk. In an environment of autonomously driven cars, where multiple AVs are interacting with each other and road users, the interactions give rise to the risk of lacking coordination, i.e., inability to coordinate their movements to properly handle both vehicle's access to shared resources. The risk is that if the vehicles fail to coordinate with each other, for instance at an intersection, it can cause accidents, lead to traffic flow inefficiencies and congestions. All this can happen in spite of individual autonomous systems functioning properly.

Another challenge appears, as per Renn et al., (2022), when dealing with systemic risks. It relates to understanding what factors are shared between how risks are generated (cause-effect relationships) and how they are managed (risk-governing system in place). One needs to identify the important factors that contribute to the risk and distinguish them from the unusual patterns that might not matter (Renn et al., 2022).

Thus, traditional risk analysis methods employing reductionist approach (breaking down system to its parts that are assessed step-by-step) for doing all this, will clearly fall short by analysing just the individual component/actor behaviour. Instead, the approach of the assessment should be towards

combining knowledge of system-level interactions and resulting system properties. Renn et al., (2022) go one step ahead by suggesting adding empirical knowledge to the overarching system characteristics (and properties) for truly improving the understanding of the systems behaviour. This logically leads us to the challenge of choosing an appropriate risk assessment approach.

3.1.3 Bottom-up vs top-down approach for risk management

The choice of approach towards risk management (particularly for risk assessment) is crucial while evaluating the risks of complex IITS. It can greatly affect the practical value of the outcomes derived from the risk analysis.

Bottom-up approach

A bottom-up approach is a reductionist approach focusing on individual elements/processes. Bottom-up approach starts by breaking down system to its base elements and analysing the effect of their individual failures. This is suitable for a system with well-defined boundaries and familiar components. The risk analysts are largely able to comprehend component-level consequences since the system-level perspective is not of significance. A bottom-up approach can be quite resource intensive in terms of the volume of risk assessments that will need to be conducted and data to be managed. Given the typically limited resources available for conducting risk assessments, risk analysts may find it challenging when prioritizing their attention toward the most significant risks and vulnerabilities. Further, Gershenson, (2016) points out in using this approach to risk assessment, one risks discarding the critical knowledge of functional-interactions not visible at element-level. The dynamic response or behaviour of a system cannot be understood just by knowing the elements of which the system is made of (Meadows, 2008).

Top-down approach

For IITS, which is a system with immense complex, fuzzy boundaries, and dynamic interactions, such an approach is deficient. Here, an important risk management objective is to uncover critical failures or deviations (such as at component-, subsystem- or emergent-level) causing system-level consequences. The top-down approach features a broad perspective of the entire system and then drills down to assess risks at various sub- levels. It allows for a holistic understanding of the system's interdependencies and encompassing risks. It is particularly effective when dealing with IITS since it requires a much broader context during risk evaluation. A top-down approach can be effective to maintain a system-level focus when dealing with large, complex, and evolving systems.

Nevertheless, a bottom-up approach can prove valuable for concentrating efforts on particular system areas where vulnerabilities are probable and demand a more thorough examination. Thus, an iterative employment of bottom-up approach (based on needs of the analysis) while keeping an overall top-down approach can be the most optimal blend.

3.1.4 Risk communication in a complex stakeholder landscape

Risk and crisis communication is a part of risk management, which can be understood as a technical field applying probabilities to articulate and recommend prevention and mitigation strategies—at the technical, organizational, and individual level (Bourrier & Bieder, 2018). However, Slovic (2000), through numerous studies, finds that different social actors hold different risk perceptions, depending on their position/role in society. This relates to the issue of varying and subjective risk perception. The more the number of stakeholders, the more complex this landscape becomes. In fact, addressing different complex systems such as health-care delivery, sustainable energy, financial systems, urban infrastructures, and national security requires knowledge, skill, and participation from many disciplines, including systems science and engineering, behavioral and social science, policy and political science, economics, and finance, and so on (Rouse, 2015). All

these disciplines project their unique principles and theories to perceive and operate within the system. All these perspectives are important to present a holistic view. But how should this knowledge be communicated to all the stakeholders?

The future transport system would have numerous stakeholders in sub-systems (see figure 2 below). Different participating stakeholders would practice a varying degree of influence on the system to achieve their objectives. For example, the regulatory authorities have vested interests to impose stricter data privacy guidelines while the autonomous technology developers would prefer greater access to user data to improve the performance of their auto-navigation system. The general users would, in turn, be conscious about their personal data being shared with the insurance companies and so on. This renders the stakeholder landscape as being quite complex for managing different aspects (economic, functional, social, environmental, etc.). Lack of trust due to a one-way communication (from experts to the receivers) can further complicate risk communication (Bourrier & Bieder, 2018). Thus, failure to build and ensure trust in such a system through proper and targeted risk communication, would be one of biggest factors challenges its success.

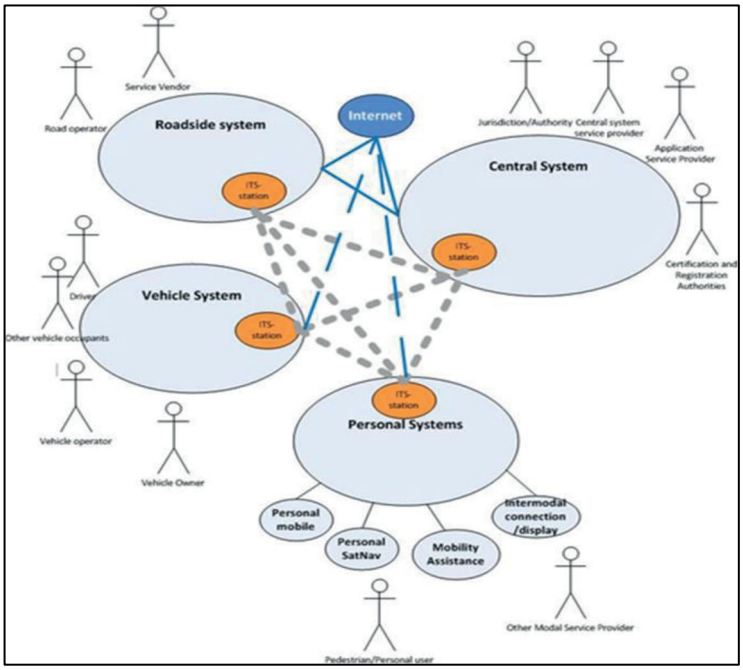

Figure 2 Functions and actors in ITS, Source: ISO 17427-2

Each actor/stakeholder expects a different set of goals, values, and utilities from the IITS (see figure above and section 3.1.2). They will also hold a limited specialized system knowledge depending on its function, application, or associated responsibility and hence perceive the system differently. Their needs and expectations can be opposing. In such a scenario, risk and vulnerability communication needs to be effective, clear, and unbiased since, the information flow (e.g., about resources, incentives, and consequences) will feed into their respective decision points and trigger actions accordingly. The varying (and often limited) nature of stakeholder's understanding makes it challenging to use a common mode of system visualization and information dissemination. Then one will need to prioritize the stakeholders. But which stakeholder's perspective should be used to communicate risks? What is the optimal balance between common- and stakeholder-specific risk information? How do we ensure quality and timely information dissemination that caters to all the critical stakeholders? All these are challenges for the risk communication.

3.2 Challenges related to analysis methods & tools

3.2.1 Background

As discussed in section 3.1.1, systems thinking is the process of understanding how things influence one another within a whole and represents an approach to problem solving, that views 'problems' as components of an overall system (Rouse, 2015). To a large extent this is about 'visualising' or forming a mental image of the overall system.

Visualization, a process or act of creating these mental concepts, is a form of 'computer-aided seeing' of information embedded in data (Chen & Luciano, 2013). *It involves constructing a system model by abstracting and showcasing the most relevant components, actors, and functionalities.* The goal of visualization is to aid our understanding of the collected data/knowledge by leveraging the visual system's highly tuned ability to see patterns, spot trends, and identify outliers (Heer et al., 2010). However, when we apply this understanding of visualisation to risk management, it should not be limited to just data analysis or computer-generated graphs. Visualisation has significance for each step of risk management, for instance:

- Scope, context, and planning- visual representations of system boundaries, visualising diverse set of stakeholders and their interests.
- Risk assessment- Visualising cause-and-effect in models for conducting analysis of risk/threat scenarios, visualising risk appetite to gauge against pre-defined risk criterion.
- Risk treatment- Visualisation can help in developing risk treatment strategies or plans and monitor effectiveness of barriers.

Section 3.2.3 talks about some of the fundamental insufficiencies of traditional visualisation tools that will need to be overcome to help in adequately visualising the future IITS's risk management.

Utne et al., (2008) addresses challenges of using simplistic risk and vulnerability analysis for evaluating the critical infrastructure. Complexity from combination of old and new technology, interdependencies among parts of society, varying risk perception between stakeholders, lack of statistical data for relevant incidents, fast rate of development in infrastructure are some of the major challenges facing risk and vulnerability analysis (RVA) methods. These are further discussed below.

3.2.2 Challenges for analysis methods

To capture the possible failure events that could cause critical system failures in complex systems, one should look beyond the traditional barrier thinking, where an assumed set of individual and independent components protects the system from going down (collapse) (Selvik & Signoret, 2020). But what kind of risk analysis methods aids in applying such a thinking during the risk analysis? Clearly, there are issues concerning efficacy, capability and relevance of traditional risk analysis methods in the IITS context. These are discussed below:

How can the undesirable outcomes of events be predicted?

The mobility sector is undergoing a socio-technical transition. The system is becoming dynamic, automated, has large-scale deployment of services across all road transport categories (urban and rural with covering a range of complex situations) to ensure interoperability, security, and system availability (Lu at al., 2018). Such a state-of-the art system consists of multi-layered architecture, with interconnected functions spanning multiple modes of transport. This exponentially expands the range of state space the system can be in the future. Some of the risks (emerging and systemic risks section 3.1.1) require comprehending and estimating the effects of exploited vulnerabilities or

events in one part of the system emerging as consequences for other connected (or even unconnected) sub-systems, stakeholders, or elements. This is challenging to do when using the simplistic risk assessment techniques (such as FMEA, fault-tree, event tree, etc.) that have a reductionist approach of focusing only on the technical weaknesses in individual components. Further, the consequences can be of social, economic, or political in nature. The traditionally used risk analysis methodologies are do not suffice for these emerging needs.

How should the validity of the risk analysis results be ensured?

Given that the IITS system is fast growing and changing, the risk & vulnerability analysis can quickly become outdated. At what point does the risk analysis results cease to be valid for the evolving system? Risk managers are faced with this and many more related questions such as:

- How can analysts validate the results of the risk analysis?
- Keeping a track of the relevant changes and developments in this sector is hard enough. Moreover, how often should these changes (as invalid assumptions, new developments, transition in business models) be assessed to reflect in the analysis?
- What kind of indicators (or KPIs) are useful for tracking system performance, safety and security aspects. How does one account, for example, impact of changes in technology & infrastructure, evolving data protection laws, complicated cybersecurity threat profile, adapting human behavior, etc.?

3.2.3 Insufficiency of traditional visualization tools

Listed below are some of the missing aspects that need to be addressed by traditional visualisation tools:

- The IITS is a modern system generating volumes of data at high velocity, that will need to be represented comprehensibly.
- The visualisations will have to offer the ability to offer to view information that caters to specific perspectives of the users.
- The visualisations should be able to represent the interconnected nature of risks and not provide fragmented understanding of system portions.
- Unlike static tools (e.g., risk matrices), the visualisation tools of the future IITS should be able to offer real-time analysis & updates supporting quick decision-making. Ideally, the tools should be able to evolve their visualisations with the risks it is communicating.
- These should provide a secure and collaborative interface among users.

4 Conclusion & recommendations

The success of future IITS rests on interactions, relationships, communication, and trust. These are difficult to manage. The conventional risk management framework, while effective in the past needs to be adapted to manage these emerging and novel challenges that from the nature of a dynamic socio-technical system that is continuously evolving. Difficulties in balancing comprehensive with resource limitations during planning (scope, context and criteria), challenges of connecting the appropriate system properties to explain and apprehend its future behaviour, communicating risks to a diverse set of stakeholders are just some of the challenges that have started to emerge when managing the complex IITS. One needs to account for changes in autonomous elements, evolving infrastructure and interplay of complex technologies, and the limitation of a linear regime of

traditional risk management process is a major drawback when trying to assess the system risks. There is a need to adapt and transition towards embedding a *top-down, iterative* and *systems thinking* approach in the risk management framework.

References

A. Geraci, F. Katki, L. McMonegal, B. Meyer, J. Lane, P. Wilson, J. Radatz, M. Yee, H. Porteous, and F. Springsteel. (1991). IEEE standard computer dictionary. IEEE Press.

Bělinová, Z., Bureš, P., & Jesty, P. (2010). Intelligent transport system architecture different approaches and future trends. In Data and Mobility (pp. 115-125). Springer, Berlin, Heidelberg.

Bossom, R., Jesty, P. (2009). Using the FRAME Architecture for Planning Integrated Intelligent Transport Systems. In: ITS Prague 2009, Prague

Bourrier, Mathilde, & Bieder, Corinne. (2018). Risk Communication for the Future. Springer International Publishing AG. https://doi.org/10.1007/978-3-319-74098-0

Chen, M., and Luciano F. (2013). "An analysis of information visualisation." Synthese 190.16 3421-3438.

Dali, A., & Lajtha, C. (2012). ISO 31000 risk management—“The gold standard”. EDPACS, 45(5), 1-8.

Gershenson, C. (2016). Improving Urban Mobility by Understanding its Complexity. arXiv preprint arXiv:1603.04267.

Jeffrey, H., Bostock, M., and Ogievetsky, V. (2010). "A tour through the visualization zoo." Communications of the ACM 53.6: 59-67.

Johnson, C. W. (2006). What are emergent properties and how do they affect the engineering of complex systems?. Reliability Engineering and System Safety, 91(12), 1475-1481.

Johansen, I.L., Rausand, M. (2011). Complexity in risk assessment of sociotechnical systems. In: Proceedings of the 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference, pp. 2274–2283. Curran Associates, Helsinki.

Kaufman, G. and Scott,K.E. (2003). “What Is Systemic Risk, and Do Bank Regulators Retard or Contribute to It?” The Independent Review 7, no. 3: 371–91

Lu, M., Turetken, O., Adali, O. E., Castells, J., Blokpoel, R., & Grefen, P. W. P. J. (2018, September). C-ITS (cooperative intelligent transport systems) deployment in Europe: challenges and key findings. In 25th ITS World Congress, Copenhagen, Denmark (pp. 17-21).

Mariani, S., Cabri, G., & Zambonelli, F. (2021). Coordination of autonomous vehicles: taxonomy and survey. ACM Computing Surveys (CSUR), 54(1), 1-33.

Meadows, Donella H. (2008) Thinking in systems: A primer. chelsea green publishing.

Murray, J. L., & Lopez, A. D. (1996). The global burden of disease. A comprehensive assessment of mortality, and disability from diseases, injuries, and risk factors in 1990 and projected to 2020. Harvard, MA: Harvard University Press.

Renn, O., Laubichler, M., Lucas, K., Kröger, W., Schanze, J., Scholz, R.W. and Schweizer, P.-J. (2022), *Systemic Risks from Different Perspectives. Risk Analysis*, 42: 1902-1920. https://doi.org/10.1111/risa.13657

Rouse, W. B. (2015). Modeling and Visualization of Complex Systems and Enterprises : Explorations of Physical, Human, Economic, and Social Phenomena, John Wiley & Sons, Incorporated.

Selvik, J. T., & Signoret, J. P. (2020). Risk Management of Complex Systems: Understanding the Difference Between Systematic and Systemic Failures. In Engineering Assets and Public Infrastructures in the Age of Digitalization (pp. 128-136). Springer, Cham.

Slovic, P. (2000). The perception of risk. London: Earthscan

Utne, I. B., Hokstad, P., Kjølle, G., Vatn, J., Tøndel, I. A., Bertelsen, D., & Røstum, J. (2008, March). Risk and vulnerability analysis of critical infrastructures-The DECRIS approach. In SAMRISK conference, Oslo.

Venkatasubramanian, V. (2011). Systemic failures: challenges and opportunities in risk management in complex systems. AIChE J. 57(1), 2–9

+47 4000 1933

POST@PROACTIMA.COM

PROACTIMA.COM