Safety and Reliability – Safe Societies in a Changing World – Haugen et al. (Eds)
© 2018 Taylor & Francis Group, London, ISBN 978-0-8153-8682-7

Evaluating approaches for hazard identification for the inclusion in a safety assessment framework for efficient transport

Ø. Skogvang, R.K. Opsahl & S. Solibakke
Safetec Nordic AS, Norway

P. Karpati & A.A. Hauge
Institute for Energy Technology, Halden, Norway

T. Sivertsen
Bane NOR SF, Oslo, Norway

B.A. Gran
Institute for Energy Technology, Halden, Norway
Norwegian University of Science and Technology (NTNU), Trondheim, Norway

M.A. Lundteigen
Norwegian University of Science and Technology (NTNU), Trondheim, Norway

ABSTRACT: This paper presents the experiences from applying hazard and operability analysis (HAZOP) as support for establishing the safety requirements specification of a new safety-related railway application. The new railway application is a software based system for securing work areas, meaning it prevents railway traffic in areas along the track allocated to maintenance. The experiences are collected within the Safety Assessment Framework for Efficient Transport (SafeT) project managed by Bane NOR. Bane NOR is the government agency that owns, operates and develops the Norwegian railway infrastructure. The objective of the SafeT framework is to offer a systematic, reusable way for creating system wide conceptual design models and based on them, creating a common risk model, which in turn will facilitate safety assessment, establishing the requirements specification, and safety demonstration of the system under consideration. The experience collected on applying HAZOP is done through two workshops with different formats on the documentation. The objective was to collect guidance on how HAZOP can be supported in the SafeT framework.

1 INTRODUCTION

The project "Safety Assessment Framework for Efficient Transport" (SafeT) aims at developing a framework that supports the implementation of EN 50126 (CENELEC, 2017) and thereby of the Common Safety Methods for Risk Assessment (CSM RA) (EU, 2013) in the railway industry, in particular how the railway infrastructure may support efficient transport.

This paper presents ongoing results from the case studies, while the results from the modelling is presented in another paper (Karpati et al, 2017). Figure 1 illustrates which phases of EN 50126 that is within the scope of the current SafeT work and both papers, annotated by a dark grey rectangle. Some of the related work (chapter 2) is therefore relevant for both papers, and the case (chapter 4)

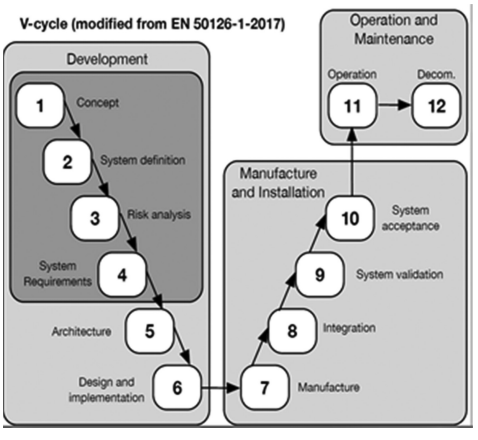

Figure 1. Scope of paper and relationship to EN50126.

is applied throughout the SafeT project. The aim of the paper is to show differences, advantages and disadvantages for two different approaches for hazard identification, applied on the new safety-related railway application.

The current focus in the SafeT project is on the development phases 1 to 4 of EN 50126. In these phases of a systems life cycle, Bane NOR takes a lead role in the development while successive development phases to a large extent are outsourced. The SafeT framework intends to support the development of the core artefacts within the system life cycle. In the early stages of the life cycle, in the part of the framework that concerns the in-house conceptualisation, the core artefacts are: 1) the conceptual system design model; 2) common risk model; and 3) requirements specification.

The main objective of the SafeT framework is to offer a systematic, reusable way for creating system wide conceptual design models and based on them, creating a common risk model, which in turn will facilitate the safety assessment and safety demonstration of the system in focus, throughout the system's lifetime.

2 RELATED WORK

International safety standards, such as EN 50126, provide requirements and guidance on how to carry out the assessment process. Although most safety standards often view the safety of a system as a function of the reliability of its components, little guidance is provided on how to derive safety requirements and acceptable risk for components whose failure rates are not known. Particularly, it is often difficult to derive safety requirements for logical components such as the software. The problem can be formulated from a consideration of the following two important tasks in the development of safety critical systems: (1) *establishing the requirements to the system*, and (2) *ensuring that the system fulfils these requirements.* The safety requirements should be established through risk assessment and hazard analysis, and fulfilled through the use of techniques and measures adequate for the risk level. The framework proposed in the project has much of its inspiration from theoretical aspects of international safety standards such as IEC 61508 (IEC 61508). The novel part of the framework is fivefold: reusability, modularity, unification, transparency and argumentation.

In the following, a number of past projects that relate to the topics of SafeT are briefly introduced. However, most of them relates to the need of establishing models and providing support for a safety case, see related work presented in the other Safe-T paper (Karpati et al, 2017).

The EU funded project MODSafe provides a risk analysis method purposed to combine potential hazards, safety requirements and functions, and link these elements to a generic functional, and object structure of a guided transport system. ASCOS (Roelen, 2014) focused on safety and certification of new aviation operation and systems, and included among other advices on methods and tools for safety based design. ModelMe! (Falessi, 2011) provides a tool-supported traceability framework where the tool for example automatically extracts the safety-related slices of SysML design models (SysML).

The AltaRice Language (Griffault, 1998) is an object-oriented modelling language dedicated to performance evaluation of complex systems. The main motivation for its creation was the difficulty to design, to share and most importantly to maintain safety and reliability models such as fault trees, event trees, Markov chains or stochastic Petri nets. The application and further development of the language is a continuous research activity at NTNU (Legendre, 2017).

Of relevance is also CORAS (Lund, 2011; Gran, 2004) which provides a methodology for model-based risk assessment integrating aspects from partly complementary risk assessment methods and state-of-the-art modelling methodology.

The SafeT project has also reviewed a number of ongoing and past industrial experiences among the project partners related to the use of design and risk models to facilitate the safety assessment and demonstration of complex systems. Some of the challenges observed in these projects have also been reported earlier within aviation (Gran, 2007). Finally, the CHASSIS method (Raspotnig, 2018) utilizes UML use cases and sequence diagrams with HAZOP guidewords to integrate safety and security considerations for early requirements determination.

3 APPLYING DIFFERENT APPROACHES FOR HAZARD IDENTIFICATION

3.1 *The role of the hazard identification*

There may be a number of different motivations for performing a hazard identification. Among them are avoiding loss of value, life and property, optimizing performance and reducing costs. The motivation for studying hazard identification in the SafeT project is to make sure that relevant hazards associated with development and use of software are evaluated, risk mitigation is in place, and the methods used for hazard identification are applicable and useful, with a basis in case studies that are carefully selected together with Bane NOR.

The purpose and method of a hazard identification and operability study (HAZOP-study) is well described in the literature, for example in *Risk assessment* (Rausand, 2011) and *IEC 61882:2016 (HAZOP studies)* (IEC 61882). The hazard identification and operability study is performed by a group review using structured brainstorming to identify and assess potential hazards. The group of experts starts with a list of tasks or functions, and next uses keywords such as none, reverse, less, later than, part of, more. The aim is to discover potential hazards, operability problems and potential deviations from intended operation conditions. Finally, the group of experts establishes the likelihood and the consequences of each hazard and identifies potential mitigating measures. The analysis covers all stages of project life cycle. In practice, the name HAZOP is sometimes (ab)used for any "brainstorming with experts to fill a table with hazards and their effects". Many variations or extensions of HAZOP have been developed.

Hazard identification can be defined as the process of identifying and listing the hazards and accidents associated with a system (DEF-STAN 00-56, 2007). There are numerous different definitions of the term *hazard* described in standards and the literature. In the following, we will combine the definitions used in EN 50126 and EN 50129 and define hazard as "*a physical situation or a condition that can lead to an accident*".

3.2 *Hazard identification in the RAMS lifecycle*

Throughout the European Union, railway signalling and interlocking projects are carried out on the basis of the CENELEC standards EN 50126 (CENELEC 2017), 50128 (CENELEC 2011) and 50129 (CENELEC 2003). The set of standards provide a consistent, European approach to the management of reliability, availability, maintainability, and safety, denoted by the acronym RAMS. In order to demonstrate that a technical system is safe to take into use and suitable for its intended application, the CENELEC standards require that the system under consideration is described and analysed in its intended context, in particular with respect to its relationship to hazards that can occur in this context and how these hazards can be controlled through the system design. This requires good models of both system design and risk that capture the relations between the different system levels and between hazards, causes, barriers, accidents, and consequences. Of particular importance to the safety demonstration is the utilization of common risk models that include the results from the hazard identifications at the different system levels, from an overall railway system down to the separate subsystems (Sivertsen, T. 2016). The use of models to support the safety management is central to SafeT, which therefore focuses on criteria for the choice of modelling techniques and how they can be combined, adapted and further developed to satisfy the modelling needs. These needs are associated to the analyses at the different system levels and its context, the risk associated to the application, and the requirements established to control this risk.

Hazard identification, operability studies, analysis and evaluation of the risks are key activities in phase 3, but they are also relevant for all the following RAMS-phases, shown in Figure 1, and in accordance with 50126-1 (CENELEC 2017):

#	Phase
1	Concept
2	System definition and operational context
3	Risk analysis and evaluation
4	Specification of system requirements
5	Architecture and apportionment of system requirements
6	Design and implementation
7	Manufacture
8	Integration
9	System validation
10	System acceptance
11	Operation and maintenance
12	De-commissioning and disposal

As part of continuous improvement work as described in the ISO 9000-family of standards (ISO 9001), identification and evaluation of potential hazards should also be done as a continuous activity throughout the system's whole life cycle. For all steps and phases, there may be numerous hazards that can compromise the RAMS performance of the system.

4 CASE EXAMPLE DESCRIPTION

4.1 *Introduction to the case example of securing work areas*

The introduction of axle counters for train detection necessitates a new solution for securing work areas. The current solution, on track sections without axle counters, is to use a contact magnet to induce a short circuit in a manner similar to how an axle of a train induces a short circuit and thereby is detected. The short circuit induced by the contact magnet triggers a state change in the interlocking that prevents the train dispatcher from locking routes through the affected section until the contact magnet is removed by the safety guard.

In the proposed solution for securing work areas (see Fig. 2 and Fig. 3), a safety guard uses a

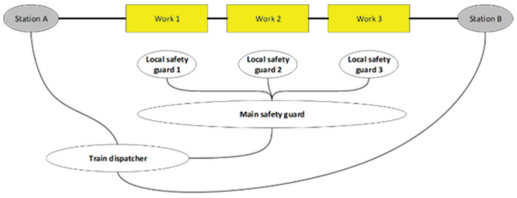

Figure 2. Work areas and roles.

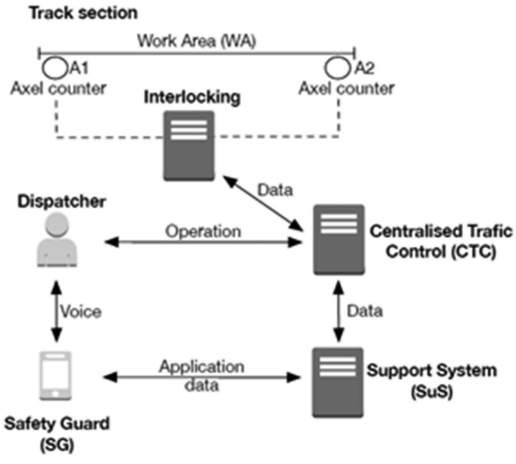

Figure 3. The securing work area case.

smartphone to interact with the train dispatcher. Besides allowing voice communication with the train dispatcher, the smartphone also contains a dedicated application with functionality to manage the securing and releasing of work areas.

In the Norwegian infrastructure, the train detection has usually been performed with different variants of track circuits. Axle counters were introduced in the infrastructure just a few years ago, and gradually replace the existing track circuits.

Irrespectively of the train detection system used, there is a need to protect workers along the track from trains unintentionally moving into the work area. A work area is a track section (possibly more than one track) that can be disposed for work, without any trains entering or leaving the area (Figure 2). The work area and the surrounding tracks can be protected by points, derailers, main signals, shunting signals, and regulations.

While the train dispatcher in either case has the possibility to block the work area, a basic safety principle in Norwegian railway operation is that the workers should be able to prevent the train dispatcher from unblocking the work area before the work is finished. Basically,

- the workers' position must be correctly identified;
- the correct work area must be effectively blocked; and
- the work area must not be unblocked prematurely.

One of the challenges with the introduction of axle counters has been that the existing methods to secure the work area no longer worked. This applies both to the correct identification of the workers' position and to the barriers against hazards caused by premature unblocking of the work area. Since a track circuit short-circuits when a train is present in the track section, the presence of trains can be imitated by short-circuiting the track circuit with other means, viz. the *contact magnets*. In this way, the workers along the track can indicate their position to the train dispatcher, who can block the section to prevent trains from entering. The contact magnet furthermore works as a barrier to hazards caused by premature unblocking of the area (trains entering the work area), since the track section is considered occupied by the interlocking.

The current solution in Norway for securing the work area when axle counters are used for the train detection involves removing a physical key for the relevant work area from its lock when the train dispatcher has blocked the work area and released the key. The train dispatcher is prevented from unblocking the work area until the safety guard has put the key back. While this certainly works, the solution is both expensive and inefficient due to the need for additional physical equipment along the track, and physically interlocking this with the signalling system. There is therefore a need for a system that can replace the current use of physical keys.

This is the background for the invention of the concept described in the next section.

4.2 *A concept of a new solution for securing work areas*

The concept involves the development of a software based system for safe interaction and supervision related to the protection of maintenance workers from accidents caused by the interference with the railway traffic. The solution is planned to require no other physical measures in the infrastructure than simple marking along the track in terms of a barcode or QR-code identifying the work area.

The proposed solution for securing work areas (see Fig. 3) consists of a software-based solution whereby a safety guard uses a smartphone to interact with the dispatcher. Besides allowing voice communication with the dispatcher, the smartphone also contains a dedicated application with functionality to manage the securing and releasing of work areas.

The safety guard identifies the work area by scanning the code on site. This identification of the work area is required at certain steps in the operation. Some of the characteristics of the functionality are:

- The main safety guard selects the functions from the application on his smart phone.
- Scanning the work area identifies both the safety guard and the work area.
- The application communicates with the support system, which communicates with the CTC and other applications.
- The support system supervises the protocol associated to each function.
- The support system supervises the secured work areas, and prevents the train dispatcher from prematurely unblocking the work area.

The solution gives several advantages, like less intervention in the infrastructure, no physical key to be kept and replaced, more convenient inspection, improved safety locally, additional functionality, larger flexibility, and simpler maintenance.

For simplicity, the interfaces between the operational support staff and the other roles are not shown in the figures. The operational support is not mentioned in the descriptions of the main functions, but a separate analysis of the support functions should be part of a complete analysis of the system. The responsibilities of the operational support include

- correcting errors or operational problems;
- keeping the support system updated with respect to information about known faults or operational problems; and
- keeping the support system data updated.

For the purpose of the risk assessment at the railway system level, all the functions can be described by considering only the interfaces between the applications and the safety guards, between the applications and the support system, and between the support system and the CTC.

Twelve main functions have been specified for the system (T. Sivertsen, 2014):

1. Log in: Logging into the system, thereby getting access to the other main functions.
2. Log out: Logging out of the system, thereby being prevented from using other functions before a new login.
3. Join: Enrolling in a work area, thereby preventing the safety guard in charge to release the work area.
4. Resign: Withdrawing from a work area, thereby allowing the safety guard in charge to release the securing of the work area.
5. Secure: Securing a work area, thereby preventing the work area from being unblocked.
6. Release: Releasing a secured work area, thereby allowing the work area to be unblocked.
7. Set time: Setting the time available for work in a work area, thereby allowing an automatic countdown of the time available.
8. Time: Reading the time available for work in a work area, thereby facilitating management of work in the work area.
9. Status: Reading the status a work area, thereby facilitating management of work in the work area.
10. Takeover: Requesting takeover of responsibility for a work area.
11. Full takeover: Requesting takeover of another safety guard's responsibilities.
12. Overview: Overview of the work areas the safety guard is in charge of or enrolled in.

For each of these functions there is a list of tasks that is performed by one or more of the involved actors in the process of securing and releasing the work areas, as showed in Figure 3.

5 TESTING TWO ALTERNATIVE APPROACHES FOR HAZARD IDENTIFICATION ON THE CASE

In order to evaluate the importance of the system description in relation to the result of an analysis, two alternative system descriptions were applied in two different HAZOP workshops with different participants.

The aim was to evaluate if different ways of presenting the system would result in different findings. In the first workshop, the basis for preparation and discussion was a graphical model of the system, while the other used a textual description. The same type of competence was present in both workshops, however, not represented by the same individuals.

The participants in the two workshops were mainly academics, with theoretical knowledge of the new and current system and of different approaches for risk assessment. There were no participants with practical experience with using the existing system for securing work areas, or other roles involved when performing such tasks. Most participants were familiar with the railway infrastructure in general and had experience with the HAZOP technique. All participants in the workshop where familiar with the new concept for securing work areas, through either the graphical representation of the system or the textual description.

5.1 *HAZOP based on a graphical model*

As preparation, a description of the case utilizing SysML diagrams with limited text and explanation

of the modelling language was sent out to the participants one week before the workshop. In the workshop the participants had many questions outside the scope covered by the model, there were also questions related to the meaning of some of the modelling symbols. During the workshop, an example of the physical outline was drawn ad hoc as illustration, and it was used a lot in the discussions. The facilitator had guidewords on hand, but they were not applied actively, as the participants constantly came up with new questions related to system achitecture or potential problems. The HAZOP resulted in the identification of two hazards, a large number of potential hazards and potential situations leading to down-time. The large number of the identified potential hazards was due to uncertainty and lack of detailed system procedures.

5.2 *HAZOP based on a textual description*

A textual description of the case was provided in advance as input to the HAZOP workshop (a summary of the textual description is given in chapter 4.1). The participants had one week to familiarize themselves with the textual description of the system before the workshop.

The following guide words were used in the meeting: early, late, before, after, wrong place, missing and wrong. The guidewords were not used actively for each function, but were presented on a separate marker board throughout the whole workshop. Each of the main functions was discussed in the HAZOP workshop, in accordance to the order given in chapter 4.2.

5.3 *Experiences from testing the two approaches*

A textual description is, compared to a model description, a well-known and common way of presenting systems for most people. A textual description may therefore be less time consuming to understand and is easy to present in a meeting. However, the textual description was not detailed enough to present the system logic and all the preconditions in depth. Hence, an illustration including the sequence of main functions and roles involved in each function was made by one of the participants in the workshop.

The illustrations were found to be useful complements, and indicated that the textual descriptions alone were not able to provide sufficient information. In specific, it was found that understanding the correct sequence of functions performed by the different roles was critical to the hazard identification, and this was not easily covered and captured by the textual description.

Constructs in models can become complex and thus their visualization as well. According to the experiences in the workshop based on graphical models, the models became difficult to understand after a certain level of visual complexity (e.g. when it is no longer possible to present the whole system in *one* single and readable screen diagram), it becomes more difficult to find support in the visual representation). One specific related problem was following the flow of logic in diagrams when branches were involved. Modularization of the visual representation added to the textual descriptions (if meaningfully possible) might help here.

Both workshops included a physical description in addition to the text or models provided on beforehand. This suggests that a physical outline diagram could be part of the models, or an addition to textual descriptions. Another consideration is that modelling or describing specific, representative cases (e.g. application of the planned system at a specific work area) might be a necessary supplement to the initial descriptions of the planned system. In our case, a specific, representative train station could be considered.

Even though participants in both workshops helped identifying unclear and missing parts, both workshops pointed to a number of potential hazards due to uncertainty about how the system was intended to work. Some of these details were contained in only one of the descriptions, but a number of descriptions were missing in both workshops, for example: preconditions of the main functions of the securing work area app, defined terminology and roles, description about the old and current solutions etc. A question related to this is whether the workshops would have been able to process and utilize the information requested by the participants. This needs to be taken into account when considering the use of HAZOP. In particular, there is a need to find models supporting the balance between the two considerations: giving sufficient descriptions, but not drowning the participants in details.

Based upon one workshop with models, we cannot conclude on the question of whether the model-based description prepared is practical for the hazard identification. There were, as described above, many other influences in the workshop independent from the modelling. However, it is clear that SafeT will need to prepare guidelines on how to use HAZOP in combination with specific SysML diagrams. Another question is if other models could have provided the same.

The two workshops came up with the same hazards. The only differences lay in how they were identified in the two workshops. This is in accordance to what one should expect. Since the textual and graphical descriptions were based upon the same source of knowledge within Bane NOR, differences in the assessment would typically point to

flaws in one of the descriptions. Another reason for having the same results is that the two workshops had rather homogenous group of knowledge and experiences. None of the groups had participants with practical experience, such as train dispatchers or safety guards. This is also illustrated by the high number of potential hazards. It is assumed that by having additional competence in the workshop, some of these potential hazards would be closed as not possible, while others would be confirmed. One interesting observation is that most of the potential hazards are not closed by just adding the graphical and the textual description. The uncertainty lies in what is not presented in any of the two workshops. If the experiment would have included only one HAZOP, we could falsely have concluded that the solution was simply to add the graphical or the textual description.

Both for the model based and the text based descriptions there is a need to supplement the descriptions by all the following different visualisations, to compensate for their inherent advantages and disadvantages:

- High-level visualisations—everything on one drawing.
- Modularised visualisations—to explore the details where and when needed.
- Sequences—to get necessary understanding on the order and timing of activities and tasks.
- Visualisation of interactions: man–machine/technology–organisation–environment.

A conclusion from this is that a better coverage of relevant details for the hazard identification could have been included in the model and the diagrams. This could also have been achieved by a preparatory workshop focusing on eliciting such information, or by involving a RAMS expert in the modelling beside the system modeller and the system owner.

There are several sources of uncertainty in the conclusions relating to relevant hazards identified in the two workshops. The uncertainty related to the sum of competencies covered by the participants in the workshop is crucial. That means that whatever approach, the sum of competencies is of great importance. It is not possible to compensate for lack of competence by choosing the other approach, or adding more time for each participant's preparations.

Applying these two approaches to the case identify basically the same hazards. This means that the conclusion is not that one of the approaches is preferable. On the contrary, both approaches give different nuances and different perspectives, resulting in a broader risk picture, which may be useful when it comes to communicating, evaluating and mitigating the risk.

How sensitive these findings may be to the chosen case is not investigated. This means that if the case was a totally different one, we do not know whether the two approaches would end up with similar hazards. Anyway, the findings in the HAZOPs from the two approaches, and the findings from the comparison of the two approaches, both indicate that the case is complex enough for an experiment like this.

When introducing new technologies or new applications of existing technologies, it is important to assess the risk by using not only one approach, but rather apply different approaches to get a broader understanding of the potential hazards.

6 CONCLUSIONS

In this paper we have elaborated on the experiences on using a graphical model presented as SysML diagrams in comparison with an ordinary textual description as a basis for hazard identification.

The model-based description is a practical and useful supplement for the hazard identification activities, but the HAZOP workshops point out that the use of SysML models requires good preparation of the HAZOP. SafeT will need to prepare guidelines on how to use HAZOP in combination with specific SysML diagrams. The participants should be familiar with such modelling to benefit from the models. A textual description is a mode of communication that most of the potential participants in the HAZOP workshop will be familiar with and trained in on beforehand. Graphical models, pictures and drawings are necessary and useful supplements for getting a broader understanding on the case that is subject for analysis.

ACKNOWLEDGMENT

The SafeT project is funded by the Norwegian Research Council (project number 257167/O80) and Bane NOR, and has participation by Bane NOR and IFE, also participation from Indra Navia AS, Avinor, Solvina AB, Safetec Nordic AS, NTNU, VTT and Beijing Jiaotong University.

REFERENCES

AltaRica, https://altarica.labri.fr/wp/ (Accessed Apr 10, 2017).

ASCOS project: https://www.ascos-project.eu/ (Accessed Apr 10, 2017).

CENELEC, EN 50126-1:2017. Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS).

CENELEC, EN 50128:2011. Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems.

CENELEC, EN 50129:2003. Railway applications – Communications, signalling and processing systems – Safety related electronic systems for signalling.

DEF-STAN 00-56, 2007. Safety management requirements for defence systems, parts 1 and 2.

EU, 2013. EU COMMISSION IMPLEMENTING REGULATION (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009.

Falessi, D., Nejati, S., Sabetzadeh, M., Briand, L. and Messina, A. 2011. Safeslice: a model slicing and design safety inspection tool for SysML. *In SIGSOFT FSE, pages 460–463.*

Gran, B.A., Hauge, A., Winther, R., Lavik, L. 2007. Some challenges and solutions assessing the safety of ATM systems, *In Risk, Reliability and Societal Safety, ESREL 2007, Aven & Vinnem (eds), Taylor & Francis Group, pp 2113–2120.*

Gran, B.A., Fredriksen, R., Thunem, A.P.-J. 2004. "An Approach for Model-Based Risk Assessment". *In Proc. Computer Safety, Reliability, and Security (LNCS 3219). Heisel, M. Liggesmeyer, P., Wittmann, S. (Eds). Pp 311–324.*

Griffault, A., Point, G., Rauzy, A., Signoret, J.P. and Thomas, P. 1998. The AltaRica Language. *In Lydersen and Hansen and Sandtorv ed., Proceedings of European Safety and Reliability Conference, ESREL'98.*

IEC 61508:2010. Functional safety of electrical/electronic/programmable electronic safety related systems.

IEC 61882:2016. Hazard and operability studies (HAZOP studies) – Application guide.

ISO 9001:2008 Quality management systems – Requirements.

Karpati, P., Hauge, A.A., Sivertsen, T., Gran, B.A. 2017. Evaluating models for the inclusion in a Safety Assessment Framework for Efficient Transport. *To be presented at ESREL 2018.*

Legendre, A., Lanusse, A., Rauzy, A. 2017. Toward model synchronization between safety analysis and system architecture design in industrial contexts. *In LNCS 10437.*

Lund, M.S., Solhaug, B., and Stølen, K. 2011. Model-Driven Risk Analysis. The CORAS Approach. *Springer-Verlag Berlin Heidelberg.*

MODSafe project: http://www.modsafe.eu (Accessed Apr 10, 2017).

Raspotnig, C. 2014. "Requirements for safe and secure information systems". *PhD thesis.*

Raspotnig, C., Karpati, P., Opdahl, A. L. 2018. Coordinated Assessment of Software Safety and Security – An Industrial Evaluation of the CHASSIS Method. *To be published in in Journal of Cases on Information Technology (JCIT) Vol. 20, Is. 1.*

Rausand. 2011. Risk Assessment: Theory, Methods, and Applications, ISBN: 978-0-470-63764-7.

Roelen, A.L.C., Verstraeten, J.G., Speijker, L.J.P., Bravo Muñoz, S., Heckmann, J.P., Save, L., and Longhurst, T. 2014. Risk models and accident scenarios in the total aviation system.

Sivertsen, T. 2014. Concept of a New Solution for Securing Work Areas, EHPG 2014, Røros, Norway.

Sivertsen, T. 2016, Validation of safety requirements within railway signalling and interlocking, Enlarged Halden Programme Group Meeting, Scandic Fornebu Hotel, Norway, 8th – 13th May, 2016.

SysML, http://www.omgsysml.org/ (Accessed Dec 12, 2017).