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 models for the inclusion in a safety assessment framework for efficient transport

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
NTNU, Trondheim, Norway

ABSTRACT: This paper presents the experiences from applying SysML models 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 paper introduces the SafeT project as context of the work and presents experiences on the application of SysML for the conceptual system design of the new securing work areas application. The paper also discusses whether SysML models fit the SafeT framework's objectives.

1 INTRODUCTION

The SafeT project 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). Figure 1 illustrates which phases of EN 50126 that is within the scope of the current SafeT work and this paper, annotated by a dark grey rectangle.

The current focus 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, requirements specification and safety demonstration of the system under consideration, throughout the system's lifetime.

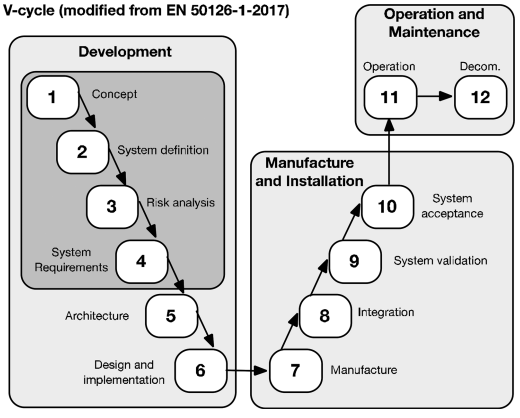

Figure 1. Scope of paper and relationship to EN50126.

2 RELATED WORK

International safety standards, such as EN 50126, provide requirements and guidance on how to carry out safety demonstration and assessment. 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 SafeT 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.

Next, many past projects that relate to the topics of SafeT are briefly introduced. The OPENCOSS project provides a common language for both safety-case and standards-based approaches for certification. The CHESS project seeks to improve Model Driven Engineering practices and technologies to better address safety, reliability, performance, robustness and other extra-functional concerns while guaranteeing correctness of component development and composition for embedded systems, and offers a modelling language and editor. The CHESS modelling language and editor is a collection-extension of subsets of standard OMG languages such as UML (UML), MARTE (MARTE) and SysML (SysML).

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-oriented structure of a guided transport system. The SaferCer project (Björnander, 2012) provides a generic process model for integrated certification and development of component based systems, including an overall picture of the development and verification of components and systems. ASCOS (Roelen, 2014) focuses on safety and certification of new aviation operation and systems, including advices on methods and tools for safety based design. ModelMe! (Falessi, 2011) provides a tool-supported traceability framework where the tool automatically extracts the safety-related slices of SysML design models.

Another approach is the AltaRica Language (Griffault, 1998). AltaRica 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, 2013; 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 CONCEPTUAL MODELLING

3.1 *The role of models*

An important aspect of SafeT is the role of system modelling in the RAMS process defined in EN 50126, in particular for supporting the risk assessment process and the identification of safety requirements. An example of a modelling task related to the RAMS life-cycle phases is the introduction of the system under consideration in a model at the railway system level (phase 1). In phase 2, the model can be refined as necessary to support the description of system objective, mission profile, boundaries and external interfaces and interactions. In phase 3, the model can be further refined to support the establishment of the risk model, followed by a refinement in phase 4 to support the specification of requirements and application conditions for the system under consideration. In addition to the system models, there is also a need to establish risk models that capture the relations between the different hazards, causes, barriers, accidents, and consequences identified in the hazard identification performed at the different system levels. SafeT looks into the possibilities to enhance the system and risk modelling tasks by the appropriate application and combination of techniques evaluated against a set of criteria derived from the relevant standards.

SafeT intends to support the implementation of EN 50126 by giving guidance on what kind of models can be used, and how they can be utilized, in the life cycle phases within the standard. In this paper, we focus on the application of models. In another paper, we focus on the risk assessment part (Skogvang, 2018). An important research problem in the SafeT project is how the use of models throughout the life cycle of a system can be integrated in a way that facilitates the overall safety demonstration and assessment. The models will serve different needs, related to the analysis of system, risk, requirements, etc. SafeT aims at arriving at a set of techniques that covers the modelling needs in the different life cycle phases, with a current focus on the first four phases aimed at establishing the requirements specification. Some examples of the prospective use of models are:

- describing and analysing the static structure of a system and its constituent parts, down to the system level and the level of detail necessary to support analysis, independence demonstration, etc.;
- describing and analysing the behaviour of a system, internally as well as through its boundaries;
- describing and analysing a system's interaction with its environment, and how it affects, and is affected by, agents involved in its operation;
- supporting the activities involved in risk assessment and hazard control, including the identification of hazards at all system levels, their causes and possible consequences;
- supporting the derivation of the safety requirements needed to handle the hazards at the overall system level as well as technical hazards at any system level; and
- communicating the different design and risk aspects, as well as the safety argumentation as such, to the different stakeholders involved.

3.2 *Requirements to models*

To facilitate the selection of design and risk models, an initial set of 58 requirements to be fulfilled by the models is established within SafeT. The requirements were derived by reviewing the process requirements in the CENELEC standards EN 50126, 50128 and 50129 (CENELEC 2017, 2011 and 2003). The set of requirements acts as the evaluation criteria supporting the selection of techniques to be used in the development of the desired models. The identified modelling needs were reformulated in terms of requirements to the models as such and categorised as requirements concerning

- Structure: to model the static aspects of a system at any system level, e.g. the possibility to support any hierarchy of system levels, and describe any system level at the appropriate level of detail without introducing unnecessary detail and complexity at other system levels;
- Behaviour: to describe the dynamic aspects of a system at any level, e.g. the possibility to show how the behaviour and state of a system depends on, and changes with, the functionality of its sub-systems and components;
- Interaction: to describe the reciprocal impact between a system and its environment, e.g. the possibility to show how the environment can influence, or be influenced by, the system, including anything to which the system connects mechanically, electrically or by other means;
- Risk: to carry out the risk assessment and hazard control, e.g. the possibility to facilitate the identification of hazards associated with the system and events leading to these hazards, the determination of the risk associated with the hazards, and the identification of possible further safety requirements needed to reduce the risk to an acceptable level, at any system level;
- Requirements: to identify and specify safety requirements, e.g. the possibility to provide the details necessary to explain and understand the requirements to the functions to be provided by the system, as well as any additional requirements that are necessary to ensure proper functioning, including contextual and technical requirements;
- Design: to analyse the safety aspects of a design, e.g. the possibility to identify the need for, and analyse the effectiveness of, safety functions or any other barrier; and
- Quality: to assure clarity, unambiguity, consistency, etc., e.g. the possibility to review the models for completeness of the identified safety requirements.

For each requirement, SafeT provided an explanation to guide the application of the requirement on models to be used in the RAMS life cycle. An example is shown in Figure 2.

Requirement: The models must support the breakdown of a system into its constituent parts, in terms of system, sub-systems, and components.
Explanation: A system generally consists of a hierarchy of subsystems and components, each of which can be understood as a system itself. It is therefore meaningful to speak about the different levels of a system, and represent these levels in such a way that the details presented for each level are adequate for this level. Furthermore, it should be possible to study the details at any system level by recursively opening up the system model down to the subsystem or component of interest.

Figure 2. Example of a requirement and its explanation.

3.3 *The use of models in the RAMS life cycle*

The 58 requirements to models reflect needs identified from an analysis of the tasks to be performed in the different phases of the RAMS life cycle. The requirements can therefore relatively easily be interpreted in this context by describing how they apply to the modelling needs in the first ten RAMS phases. The different requirements were gradually introduced along with possible procedures and flow charts. Concerning modelling, the concept phase can be carried out in accordance with the following procedure:

1. Describe the needs and how these are met today without the system.
2. Make a first informal description of the system and its environment.
3. Make a first model of the system and its environment.
4. Define the aspects to be analysed, including the aspects defined in EN 50126.
5. Select an aspect for analysis.
6. Analyse the aspect, refining the model to make it adequate for the analysis.
7. If necessary, refine the model to make it represent the analysis result adequately.
8. Repeat from step 5 for the remaining aspects.

The RAMS life cycle is initiated with the concept phase. The main objective of the phase is to investigate the overall system and its environment, confined to (1) scope, context and purpose, as well as (2) physical, interface, legislative and economic issues. This means that there already is some idea of a "system under consideration", and some idea of the functionality that shall be offered, and most likely some constraints. The purpose of a model in this phase would therefore be to facilitate this investigation. Even if the system has not yet been defined in a proper sense, it will usually be possible to introduce the system as a black box, and concretize the aspects to be investigated. It might already in this phase even be possible to decompose this black box into a set of connected subsystems, each with its specific scope, context and purpose.

Requirements posed to models in this phase demand the ability of the models to support different needs, for example:

- support the breakdown of a system into its constituent parts, in terms of system, sub-systems, and components;
- facilitate the treatment of systems, sub-systems and components as black boxes, for which the details on architecture, design and implementation can be kept out of consideration, evaluating functions and hazards only at the boundaries;
- describe the system as contained in its operational environment;
- show how the environment can influence, or be influenced by, the system, including anything to which the system connects mechanically, electrically or by other means;
- show how man and organization can affect, or be affected by, the operation of the system;
- use clear and intelligible means of description, such as formal notation for logical functions, natural language for introductions, justifications and representations of intentions, graphical representations of examples, semantic definition of graphical elements, and directories of specialised words;
- be possible to communicate to the different stakeholders;
- be understandable in themselves;
- be understandable to the prospective user.

4 APPLYING SYSML

The Concept phase and System definition phase are focused on preparing the conceptual system model. The model acts as an input to the Risk analysis phase (see Figure 1). The first activity of the Risk analysis phase is the Hazard Identification (HI). This was the focus of a workshop in the SafeT project (see section 4.5) using the model-based description of an example case described in section 4.1.

Related to the use of models, two questions were investigated: (1) whether the modelling technique selected on the basis of theoretical considerations (the identified requirements to models based on the standards) is also practical for phase 1 and 2, and (2) whether the model-based description prepared is practical for the hazard identification activity.

4.1 *The securing work areas case*

In order to realistically evaluate existing techniques and develop the SafeT framework, the project chose a case example based on a concept of a new solution for securing work areas (Sivertsen, 2014). The problem concerns the need to protect maintenance workers from accidents caused by the interference with the railway traffic. The concept involves the development of a software-based system for securing the work areas from such interference. The basic requirements to such a system are to identify the workers' position correctly, effectively block the correct work area, and prevent a premature unblocking of this work area.

In the proposed solution (see Figure 3), a safety guard uses a smartphone both for the interaction with the train dispatcher and for identifying the works areas under consideration. The smartphone contains a dedicated application with functionality

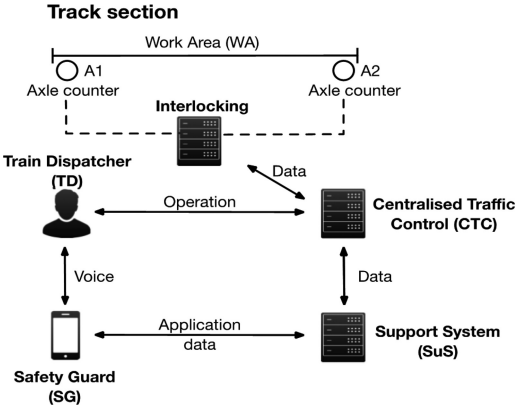

Figure 3. The securing work areas case.

to manage the securing and releasing of the work areas. Some of the characteristics of the functionality are:

- The main Safety Guard (SG) selects the functions from the application on his smart phone, e.g. secure a Work Area (WA).
- The scanning of the associated QR-code of a WA identifies both the SG and the WA.
- The application communicates with the Support System (SuS), which communicates with the Centralised Traffic Control (CTC) and other applications.
- The SuS supervises the associated protocols.
- The SuS supervises the secured WAs, and prevents the Train Dispatcher (TD) from prematurely unblocking them.

4.2 *SysML*

UML (Unified Modeling Language) was initially selected to be applied for modelling in phases 1 and 2 as it fulfils all of the related requirements to models in these phases. However, UML's focus is on supporting software analysis and design, while the system in our example case is not limited to software. Another important consideration was that the first RAMS phases are carried out at a higher system level ("the railway system level"), requiring a focus on the system as such and not merely on its software. Hence, we used SysML (Systems Modeling Language) instead which supports system engineering.

SysML is an extension of a frequently used subset of UML, and thus is expected to comply with most of the requirements to models that UML complies with. A SysML model is usually developed in a tool that stores the model entities with their characteristics and relations. The model entities can then be used in diagrams to present graphical views on specific aspects, e.g. structural or behavioural aspects.

Because of this unified model in the core of UML and SysML, they can be considered as a single but complex modelling technique. Furthermore, they offer different kinds of diagrams where each kind can be considered as a modelling technique in itself.

4.3 *Modelling the conceptual design*

Within the concept phase, modelling of the system and its environment with respect to the following aspects are required: (1) scope of the system, (2) (application) context of the system, (3) purpose of the system, and (4) environment of the system (anything that could influence, or be influenced by, the system, including people and procedures). All of these aspects are expected to be considered in the context of RAMS performance. The system definition phase requires extending the model with:

- functions and elements which need to be considered in the risk assessment;
- interfaces and interactions with the physical environment, other systems, humans, and other organisations;
- operational requirements influencing the system, including a description of conditions, constraints, logistics;
- existing safety measures and assumptions that determine the limits for the risk assessment.

The modelling was performed by an IT and dependability specialist with some experience in UML modelling, using a tool. A short textual description of the proposed system was the input to the modelling, and was analysed according to the needs of the two phases described above. The models were developed in an iterative process including consultation with the system owner.

Diagrams were prepared for a HAZOP workshop, e.g. Block Definition Diagrams (**BDD**) about Work Area and related concepts (see Figure 4), Internal Block Diagrams (**IBD**) about the internal communication and interfaces of the Support System (see Figure 5), Use Case diagrams (**UC**) of the main functions of the Securing Work Area application, State Machine diagrams (**STM**) about the registerable states of a Work Area (see Figure 6), and Sequence Diagrams (**SD**) about the main functions of the application.

4.4 *Using the models to meet the needs of the concept phase and the system definition phase*

The concept phase modelling needs can be mainly fulfilled by using BDDs and IBDs since those needs

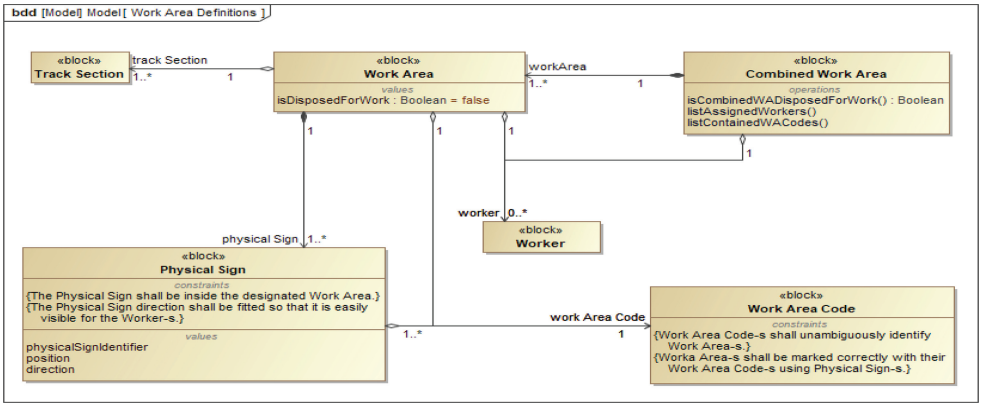

Figure 4. Example BDD defining the work area and related concepts.

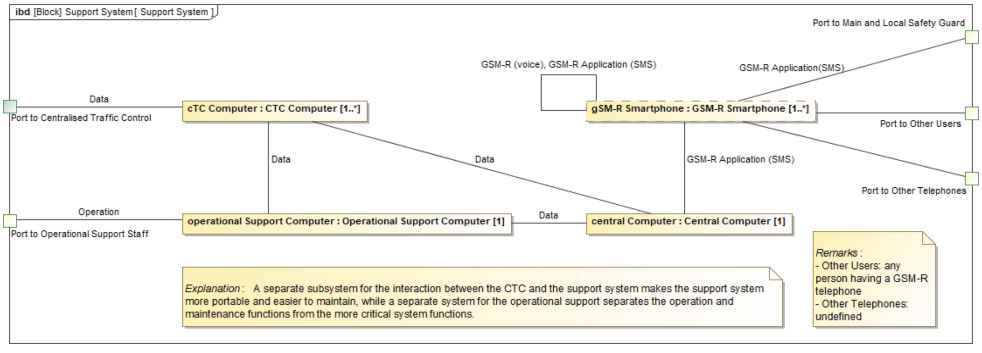

Figure 5. Example IBD of the internal structure of the support system.

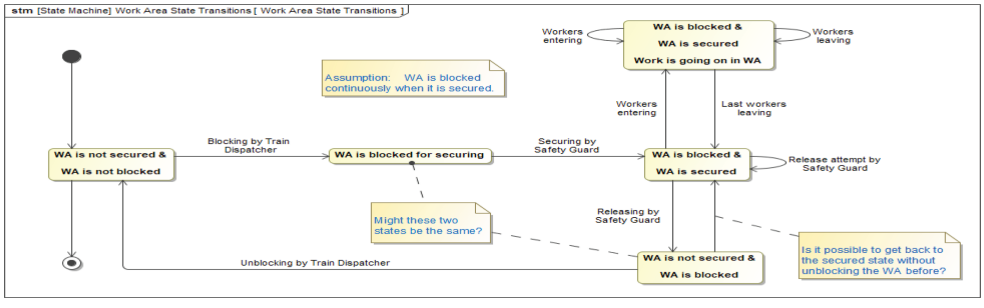

Figure 6. Example STM with the different states of a work area from the securing point of view.

require to represent the system with its elements and environment, and their static, conceptual relations. BDDs can depict an ontology. For example, the BDD in Figure 4 identifies the main concepts connected to work area in the proposed solution, their relevant characteristics, and their relations. IBDs can visualize internal structure, lines of communication and interfaces. For example, the IBD in Figure 5 depicts the internal structure of the Support System with it interfaces. The central computer communicates with the applications via its GSM-R receiver and transmitter; the operational support computer is used by the operational support staff to operate the system; the CTC computer ensures the correct interaction between the central computer and the CTC system. Another SysML diagram type not utilized by us is the Requirement Diagram (REQ) which could have

been useful for embedding the requirements in the model if a structured requirement specification had been available.

The system definition phase modelling needs can be partially fulfilled by using all 5 mentioned diagram types. BDDs and IBDs can be used when the system is further detailed (i.e. elements and interfaces in the system definition description). UC and STM diagrams as well as SDs are useful for depicting the dynamic, behavioural aspects (i.e. functions and interactions). For example, Figure 6 presents an STM with the different states of a Work Area from the securing and releasing functions point of view. This diagram shows for example that the states of the Work Area (as seen by the system) were unclear between "before securing"/"after releasing" and when it was "secured". Whether these states ("WA is blocked for securing" and "WA is not secured & WA is blocked") are the same, whether a transition from the second directly back to the state of "WA is blocked & WA is secured" is possible, triggered lots of discussions in the workshop.

Operational requirements were mostly not included in the model, but they can be added through REQ diagrams and by defining constraints. Existing safety measures were not specifically identified as such in the model, they were depicted as regular parts of the diagrams. However, there are suggestions in this direction, for example extending UC and SD for safety and security considerations (e.g. Misuse Cases, Failure Sequence Diagrams, Misuse Sequence Diagrams; an overview can be found in (Raspotnig, 2014)). Assumptions were either depicted as notes in the diagrams (e.g. see Figure 6), or as constraints. In summary, SysML has the potential to fulfil the needs of the concept and the system definition phases with respect to the requirements to models connected to these phases.

One experience was that the modelling process *helped identifying unclear and missing parts* of the case description which were necessary to develop an understanding for persons not familiar with the planned system. It is quite hard for a person involved in a task to evaluate what pieces of information are necessary for understanding the task by another person with different expertise working on another aspect of the task. The necessary amount of information is usually underestimated, which is also reflected by the related system descriptions. Modelling helps overcoming this gap but it does not guarantee the completeness of the information provided.

Another experience was that modelling with SysML sometimes demands more details than available or expected in the conceptual design phase. In other words, it *might be hard to draw the line between the conceptual design* (defining the "what") *and detailed design* (defining the "how"). For example, the conceptual design might stop at the level where the actors and systems of the New Solution are identified, maybe including the subsystems of the Support System. However, including the SWA App in the model required some further details since it resides in the software part of the Smartphone, which is a subsystem of the Support System. SafeT will need to specify clear criteria or guidelines regarding the detailing of models at the different phases of the development of a planned system.

4.5 *Using the models in a HAZOP workshop*

Two workshops utilizing HAZOP for hazard identification (HI) were organized, one using only a textual description as input and the other using a model-based description as input. The hazard identification related experiences of the workshops are presented in paper (Skogvang, 2018). Here, we focus on the modelling related experiences from the model-based workshop. A description utilizing the diagrams with limited text and explanation of the modelling language, was sent out one week before the workshop.

Even though modelling helped identifying unclear and missing parts from the modeller's perspective, it gave no guarantee that these identifications covered every necessary detail for HI. This became clear since the workshop participants had many questions outside the scope covered by the model but important nevertheless for their understanding of the context and for identifying hazards. A conclusion is that, for a better coverage of the hazard identification, relevant details in the model and the diagrams are desired. This could be achieved for example by a preparatory workshop focusing on eliciting such information, or by involving a RAMS expert in the modelling.

Constructs in models can become complex, and so their visualization. According to the experiences in the workshop, after a certain level of visual complexity (e.g. when not the whole diagram can be shown at once or if it is shown then it becomes unreadable), understanding of the diagram and following the track of thought becomes cumbersome. One related problem was following the flow of logic in SDs when branches and parallel activities were involved. Modularization might help with this issue.

During the workshop, an example of the physical outline was drawn ad hoc as an illustration which was used a lot in the discussions. This suggests that a physical outline diagram could be part of the model. SysML has no obvious means for this, therefore another modelling technique might be required as support. Another consideration is that modelling specific, representative cases (e.g. application of the planned system at a specific work area) might be a necessary supplement to the

general model of the planned system. In our case, a specific, representative train station could be considered. The model-based description also missed some information, e.g. preconditions of the main functions of the software application, necessary for understanding how the system was intended to work. A question related to this is whether the workshop would have been able to process and utilize the information requested by the participants (defined terminology and roles, description about the old and current solutions, etc.). This needs to be taken into account when considering the use of models with other techniques. SafeT needs to prepare guidelines on how to use HAZOP in combination with specific SysML diagrams.

5 CONCLUSIONS

In this paper we have elaborated on the experiences on using SysML diagrams as support for the concept and system definition phases. To the question of whether the modelling technique selected on the basis of theoretical considerations is also practical for the two first phases, we can answer affirmatively based on the experiences. The concept phase modelling needs can be fulfilled by using BDDs and IBDs since those needs require representing the system with its elements and environment, and their static, conceptual relations. BDDs can depict an ontology. The system definition phase modelling needs can be partially fulfilled by using all five mentioned diagram types.

However, further investigations and fitting guidelines will be necessary. Whether the model-based description prepared was practical for the hazard identification activities were not concluded, but the HAZOP workshop suggests that the use of SysML models requires good preparation of the HAZOP, and the participants should be familiar with such modelling to benefit from the models.

ACKNOWLEDGMENT

The SafeT project is funded by the Norwegian Research Council (project number 257167/O80) and Bane NOR, and has beside 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 project, https://altarica.labri.fr/wp/ (Accessed Apr 10, 2017).

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

Björnander, S., Land, R., Graydon, P., Lundqvist, K., Conmy. P. 2012. A Method to Formally Evaluate Safety Case: Arguments against a System Architecture Model. *IEEE Computer Society. WoSoCER2012.*

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.

CHESS project: http://chess-project.ning.com (Accessed Apr 10, 2017).

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. et al. 2011. Safeslice: a model slicing and design safety inspection tool for SysML. *In SIGSOFT FSE, pages 460–463.*

Gran, B. A. et al. 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. et al.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. et al. 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.

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

Lund, M. S. et al. 2010. Model-Driven Risk Analysis. The CORAS Approach. *Springer.*

MARTE project, http://www.omgmarte.org/.

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

OPENCOSS project, http://next.opencoss-project.eu/node/2 (Accessed Apr 10, 2017).

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

Raspotnig, C. et al. 2018. Coordinated Assessment of Software Safety and Security—An Industrial Evaluation of the CHASSIS Method. *To be published in Journal of Cases on Information Technology (JCIT) Vol. 20, Is.1.*

Roelen, A.L.C. et al. 2014. Risk models and accident scenarios in the total aviation system.

SafeCer project: http://www.safecer.eu/ (Accessed Apr 10, 2017).

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

Skogvang, Ø. et al. 2018. Evaluating approaches for hazard identification for the inclusion in a Safety Assessment Framework for Efficient Transport. *To be presented at ESREL 2018.*

SysML, http://www.omgsysml.org/.

UML, http://www.uml.org/.