Safety Architecture Overview Framework for the Prediction, Explanation and Control of Risks of ERTMS

Katja Schuitemaker[1(✉)], G. Maarten Bonnema[1], Marco Kuijsten[2], Heidi van Spaandonk[3], and Mohammad Rajabalinejad[1]

[1] Department of Design, Production and Management, University of Twente, Enschede, The Netherlands
{k.schuitemaker, g.m.bonnema, m.rajabalinejad}@utwente.nl
[2] Safety Department, NS, Utrecht, The Netherlands
marco.kuijsten@ns.nl
[3] Safety Department, ProRail, Utrecht, The Netherlands
heidi.vanspaandonk@prorail.nl

Abstract. The proposed framework includes modelling of interfaces between risk analysis, risk evaluation and scenario's representing flows of safety information of the European Railway Traffic Management System (ERTMS). In this study, we propose a functional framework combining safety data generation, data processing and structuring, definition of interactions and finally, the creation of customized representations in order to predict, explain, and control risks. Through literature review and ERTMS applicability, we develop a safety architecture overview framework. The comprehensive overview of the safety architecture can illustrate the main interactions between government, regulations, company management, technical and operational management, physical process and activities, and environment. Explicit representation delivers insight, stimulates striving for completeness, and leads to consistency of the safety analyses.

1 Introduction

The European Railway Traffic Management System (ERTMS) is subject to an increasing number of stakeholders [1], open specifications [2], and split-responsibilities [3]. Many and varied interactions among the individual components are approached proactively and qualitatively where little time and pressure towards cost-effectiveness can inadvertently lead to generating adaptive responses [4]. In previous study [5], the effects of the safety case regime, interoperability, deregulation and dynamic specifications on the ERTMS have been researched at the Dutch national level. This study concluded that achieving an interoperable and safer railway system by implementing ERTMS appears not to be straightforward for three key reasons:

- The safety case argument involves descriptions and observations including various explanations and interpretations from stakeholders.

E. Bonjour et al. (Eds.): CSD&M 2018, *Complex Systems Design & Management*, pp. 145–156, 2019.
https://doi.org/10.1007/978-3-030-04209-7_12

- For the Dutch situation, the absence of a central designer [6] and overarching safety decision-making processes between railway and train transportation lowers the degree to which the parties succeed in harmonizing various processes.
- An increased number of actors has caused a lack of insight into cross-border information.

These challenges require improvements in resilience, more awareness and increased sensitivity for interrelationships between hazards and risks, but even more: joint comprehension of the safety architecture and creation of cross-discipline understanding.

In this study, we create a safety architecture overview framework representing structured scenarios including hazards, consequences, RACs, risks and decisions in various layers. We model interfaces between scenarios, risk analysis and risk evaluation so that stakeholders are able to verify data origin, argumentation route, and application. Also, we argue that the proposed framework addresses the explained challenges through combining safety data generation, data processing and structuring, definition of interactions, and finally the creation of customized representations in order to predict, explain, and control risks.

Section 2 provides an overview of ERTMS and state of the art of safety models aiming at modelling elements of the safety architecture. The methodology is discussed in Sect. 3. Section 4 explains the creation of the safety architecture overview framework and how this complies with the challenges described above. These results are discussed in Sect. 5. Section 6 summarises the results, draws conclusions, and explains future work in order to test the proposed framework.

2 Background

ERTMS is a command, control, signalling, and communication system for railway management and safe regulation. It is composed of two technical components: (1) European Train Control System (ETCS): the Automatic Train Protection (ATP) system that makes sure trains do not exceed safe speeds or run too close together and (2) Global System for Mobile Communications – Railways (GSM-R): helps to provide communication for voice and data services.

The Dutch House of Representatives took an official preferential decision in 2014 that included a phased implementation of ERTMS. The Commission Implementing Regulation (EU) 402/2013 concerns the regulation on a Common Safety Method (CSM) for risk evaluation and assessment (CSM RA). This regulation is mandatory for railway duty holders in Europe, including the Netherlands. The safety of ERTMS should comply with the European Norm (EN) 50126, 50128, 50129 and 50159. Typical safety assessment methods for safety case creation used in railway industry, but also in other industries such as offshore, nuclear plants, and air traffic control are the Preliminary Hazard Analysis (PHA) and Hazard and Operationally studies (HAZOP). For these analysis, it is important to first define causal scenarios: potential sequences of events of an initiating event that could lead to a potential dangerous scenario.

Stakeholders involved with the creation of the safety case are the Dutch Ministry of Infrastructure and the Environment (I&W), the Dutch infrastructure provider (ProRail), and train operating companies such as the Dutch railways (NS). Next, the safety case must show that the correct management for controlling safety is in place. For the Dutch ERTMS, this management system refers to the safety management systems (SMS) of both ProRail and NS.

In short, ERTMS is subject to the influence of the Dutch House of Representatives, the application of the CSM and EN5012x, the SMS of the infrastructure provider and train operating companies, multiple technical components, trains operating on tracks, and of course, the consideration that ERTMS is an important link in the ambition to ensure the passengers and shippers view the railway system as an attractive mode of transportation. This indicates active layers in the area of government, regulations, company management, technical and operational management, physical process and activities, and environment. These levels of decision making that are involved in risk management and control hazardous processes, are explained in [7].

2.1 State of the Art

Model-Based Systems Engineering (MBSE) allows systems engineers to create the system structure and behaviour using interrelated models. MBSE is mostly used for creating the system description, and safety is often considered as a dependent attribute. On the other hand, for the missing link between MBSE and safety, several models for safety analyses have been developed.

Multiple languages have been established for safety annotation, for example the Goal Structuring Notation (GSN) [8], AltaRica [9], EAST-ADL [10], and SAML [11]. GSN is a graphical notation, using hierarchical goal structures to document the safety case. In AltaRica, the expression is in the form of a collection of Node possessing hierarchical structures, focussing on computation of dysfunctional models. EAST-ADL is an architecture description language intended to support the development of automotive embedded software. One of its extensions concerns dependability and captures information related to safety. A SAML model combines discrete probability distributions and non-determinisms.

Some studies have used SysML for safety argumentation. Safety models that are system-oriented, are often using SysML, or a modified language based on SysML. MéDISIS, using SysML for PHA and FMEA, focus more on reliability [12]. Some models use SysML for safety modelling, but not on the safety analyses itself. Examples are SafeSlice focussing on requirements and inspections [13], a model focussing on requirements [14], SafetyMet focussing on compliance with standards [15], a model focusing on the certification process [16], and O&SHA focussing on requirements and on the integration between SE and safety [17], though O&SHA does create operational views and defines a safe functional architecture. Belmonte and Soubiran [18] use both DSML (which is based on SysML) and AltaRica for the creation of PHA and FMEA. MSA is based on a combination of RobotML, AltaRica and OpenPSA for the Fault Tree Analysis (FTA) [19]. HiP-HOPS uses EAST-ADL and Boolean expressions for FTA and FMEA [20]. Some of these models zoom in on scenarios or hazardous flows. However, none of these models focus on both detailed characterisation of the evidence

underlying the safety case, and customisation of risk analysis and risk evaluation representations for enabling communications between safety stakeholders.

3 Method

This study and the design of the Safety Architecture Overview Framework is carried out in four successive steps, though execution of step three and four are iterative.

- Step 1. Translate need/requirements to a top-level use case diagram. The resulting use cases can be considered as top-level functionalities of the framework and related to system requirements.
- Step 2. Decompose to a set of functions. The functions explained in the use case diagram are decomposed to a set of functions. Per top-level functionality, we define input and output.
- Step 3. Finding solutions. For each functionality, literature review is combined with ERTMS application in order to find suitable solutions.
- Step 4. Evaluation on functionality and compatibility between solutions. This step is interrelated with step 2 and 3, because this evaluation can suggest a change of flow or solutions that contradict one another.

The first two steps are executed through following the Design Research Methodology (DRM) described by [21]. Step 3 and step 4 are executed through following the systematic search with the help of classification schemes described in Engineering Design by [22]. This approach is shown in Fig. 1.

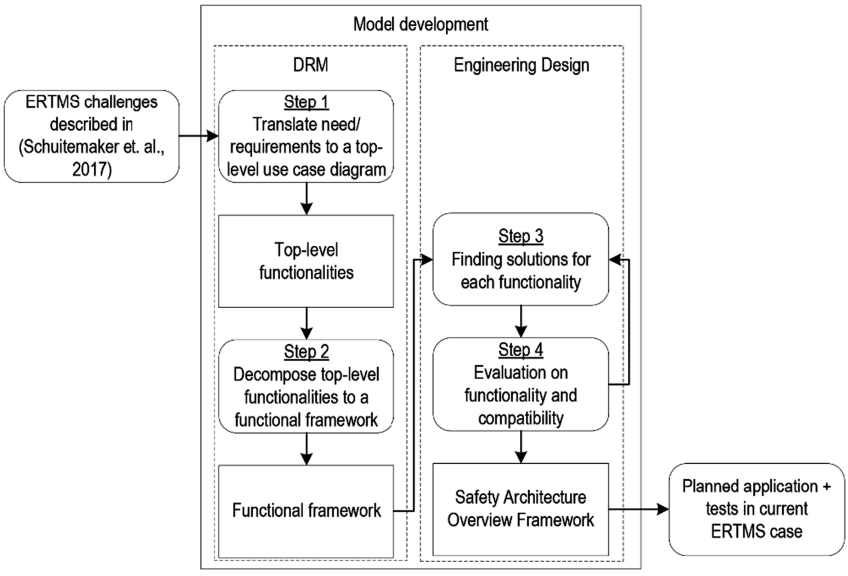

Fig. 1. Approach used for this study

4 Results

The aim of this study is to create a framework that addresses an interdisciplinary approach on both the social and technical level, and shows how parts interact and fit together. First we define interdependencies between entities and top functionalities of the framework. Next, we explain how actors are interacting with the framework. We explain each functionality in more detail and how these can be realised.

4.1 Top Functionalities

According to EN50126 (The Specification and Demonstration of Reliability, Availability, Maintainability and Safety), in order to supply relevant input, safety analysis must be performed by, at the minimum, a safety expert (key individuals or domain experts who understand the system under consideration) and a safety manager (has the responsibility over the risk assessment and ensures the traceability of safety related decision-making). For the creation of the total safety architecture, an integrator should create an integral coherence of the claims, arguments and evidence and the interdependencies between them. The task of this so-called "safety architect" is to define a complete, comprehensive and defensible argument.

For the interdependencies between entities, the use case diagram in Fig. 2 represents top functionalities of the framework, how an overview can be created, and how actors are interacting with the framework.

For the explanation of Fig. 2, the risk assessment approach requires analyses where hazards, risks, and mitigations are identified by following guidelines and logical reasoning of experts during requirements engineering and design. This data must be processed to create comprehensive information and avoid specialist terminology and linguistic ambiguity. Next, in order to consider the safety for the ERTMS as well as the safety for subsystems, it is important to clarify boundaries and relationships. Structuring the safety information evaluates and clarifies trade-offs between analyses. Technological risks must be understood within their context, where there are many active entities like actors, organisations, authorities, government, etc. Finally, stakeholders have various interests and various viewpoints, depending on the structure from which the process is viewed. To take into account these viewpoints, we need to customize the view to be analysed.

4.2 Safety Architecture Overview Framework

The proposed framework for creating the safety architecture overview combines generating and processing of safety data, structuring of information, defining interactions, and creating customized representations.

Data generation refers to the creation of data from risk assessment performed by safety experts. For identification of links between hazards and accidents, consequence analysis is often performed. For the generation of RACs of the Dutch railway system, this means that risks should be reduced to as low as reasonable practicable (ALARP). A risk matrix approach is used in conjunction with an ALARP based approach to risk reduction. Depending on the safety analysis phase, data can consist of hazards,

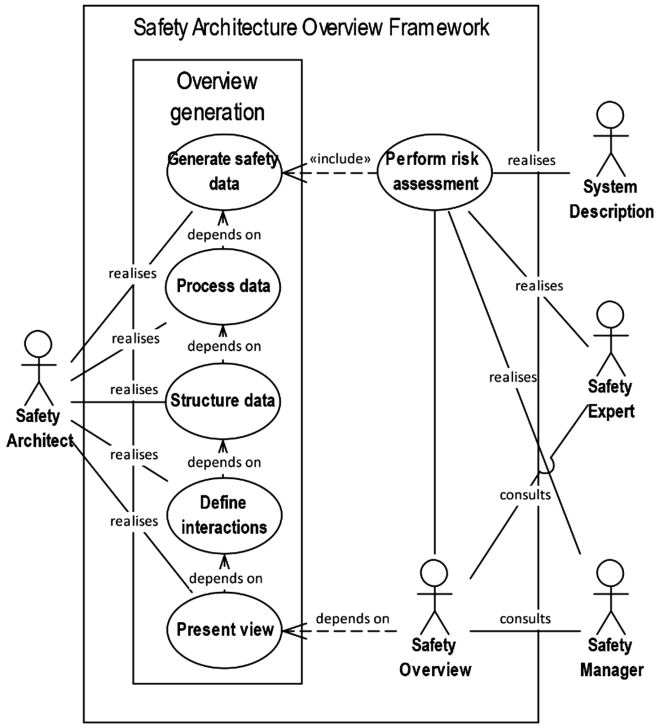

Fig. 2. Use case diagram representing top functionalities of the safety architecture overview framework.

consequences, risk matrices including tolerability limits, ALARP evaluations and decisions. This data is still in the form of raw data, obtained through oral sessions generated in real-time or documentation.

Data processing concerns the translation of raw extracted data from stakeholders, to valuable information. For the purpose of detailed characterisation of the evidence underlying the safety case, and customisation of safety analysis representations, GSN is not suitable. For the purpose of enabling communications between safety experts, safety architects, and safety managers, EAST-ADL, AltaRica and SAML are not well-known and do not focus on information presentation for these stakeholders. The Systems Modeling Language (SysML) is a more standardized and institutionalised language and has been shown to improve development communication during system design [23]. SysML also provides principles for partitioning and layering modules, which are crucial for structuring data and defining interactions. To be able to create valuable information from raw data, we need to select, abstract, and synthesize information:

- Select data. The process of collecting required and recommended data.

- Abstract data. We translate informal raw data to a formal language that creates common understanding. Next, we filter information to prevent information overload, and to deal with safety complexity.
- Synthesize information. The fitting together of parts or elements to produce new effects and to demonstrate that these effects create an all over order [22]. Grouping indicates that elements belong together based on some common characteristic. In this function, filtered information is labelled (stereotypes) according to their type.

This processing from raw data to interpretive safety information is shown in the activity diagram in Fig. 3.

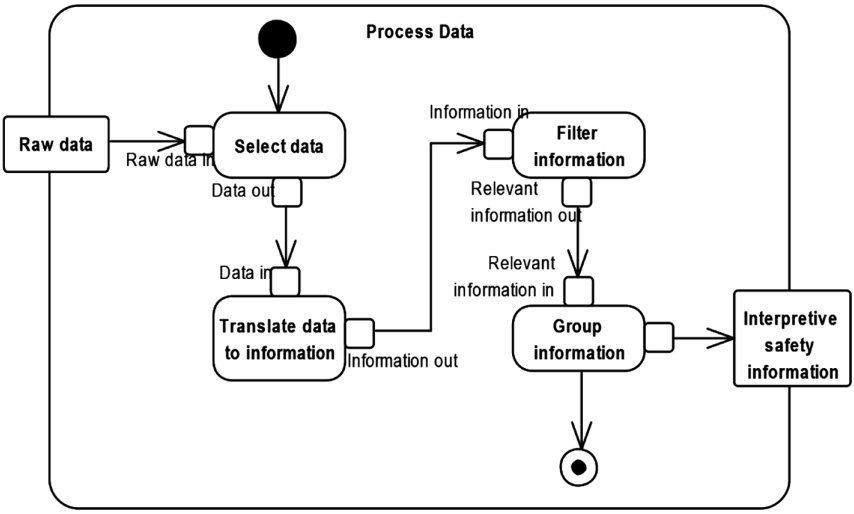

Fig. 3. Activity diagram representing the processing of safety data to interpretive safety information.

In PHA, high-level system hazards are identified inductively by asking "what if this component fails", and hazard are also identified deductively by asking "how this could happen". Scenario-guided hazard analysis is to be structured around the flows within a system. For example, each HAZOP contains complex chains of flow of information, and each flow can have hazardous effects. As for identification of hazards, their causes, and their effects, the focus within this framework is on the properties and behaviours of flows in the system.

A typical methodology for scenario identification is ETA; Cause-Consequence Analysis in particular may also be applied to identify scenarios. Causal analysis aims to identify the logical sequences of hazardous events that may lead to an undesirable effect (EN50126). Typical causal analysis techniques are FTA and FMECA. The use of inductive and deductive safety analyses results in downstream and upstream flows, see Fig. 4.

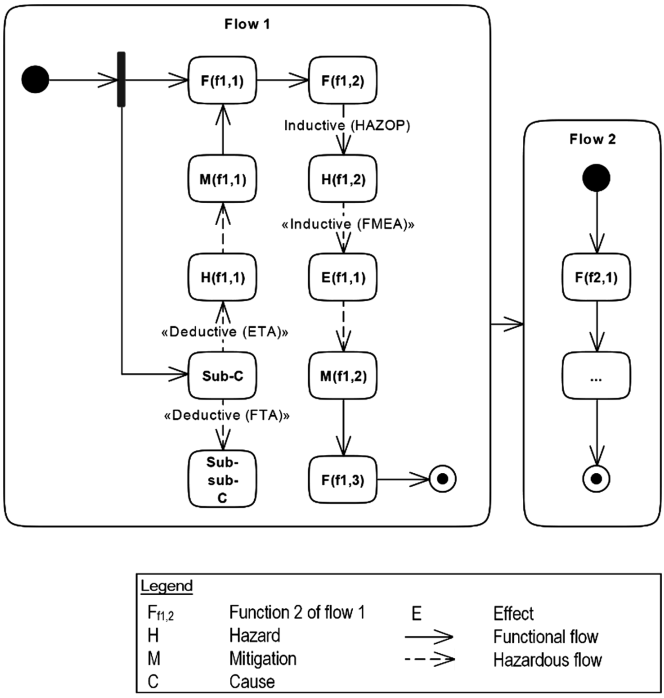

Fig. 4. Activity diagram of the flows representing safety analyses performed in the safety architecture overview framework.

As for ERTMS and moreover, the Dutch Railway industry, the safety case approach is applied to construct an argument that the system is adequately safe for a given application in a given environment. In accordance with the safety case, the structure upon which the Safety Architecture Overview Framework is built consists of:

- Claims. A conclusion or premise to be demonstrated. For example, that the system is safe to operate.
- Evidence. References that can be a result of a safety analysis. For example, FTA's or FMEA's.
- Arguments. Set of inferences between claims and evidence.

As for the example in Fig. 4, flow 1 includes some hazards (resulting for example from a HAZOP) for which mitigation M(f1, 1) and M(f1, 2) are applied in order to reduce the risk. For this reason, one can claim that execution of Flow 1 is acceptably safe.

The *definition of interactions* includes the identification of all factors that contribute to a failure. According to EN50126, the definition of the operational context is necessary to evaluate the risks specific to a hazard within its accident scenario. Identification of causal scenarios allows architects to discover interactions between various flows and layers such as human, technological, organisational and external, that might contribute to the failure at the system output. Each element of the scenario is allocated

to one of the earlier explained 6 layers (government, regulations, company management, technical and operational management, physical process and activities, and environment). It is intended that each layer is considered when generating causal scenarios. We model these layers in SysML as partitions that share content. Each partition represents one of the six layers. Its content can be allocated accordingly.

For the *presentation of views*, graphic presentation exposes the interrelationships of system events and their interdependence upon each other. By visualisation, we make boundaries of safety decisions explicit, and reveal patterns such as links, inferences, and contextual relationships, that would be otherwise hard to find. In order to understand the overall safety level of ERTMS, various views of its safety architecture have to be investigated:

- Risk analysis overview. This overview includes the top-level safety architecture including risk analysis elements such as top-claim, argument and supporting evidence.
- Risk evaluation overview. This overview includes expected total risks to which the user is exposed in the form of likelihood and severity. Through consulting this view, the user is able to evaluate the integral risk analysis architecture and make judgements about the overall safety level of ERTMS.
- Scenario analysis detailed views. This view includes the scenario to be analysed. It represents combinations of flows including safety functions, hazards, consequences and mitigations and layers. This view is important for more in-depth analysis of a scenario.

5 Discussion

Some benefits of the Safety Architecture Overview Framework have been shortly explained in earlier sections. Though, there are some specific added values and challenges that require more explanation. First, the abstraction reduces complexity and emphasizes the system under consideration. This can be useful in collaborative work and should reduce ambiguity. In order to predict, explain and control risks, it is of primary importance to find a balance between concreteness and abstraction. Main challenge is to extract data without losing essential information necessary for defining the architecture. Second, incorporating structure allows better partitioning. This modelling of interfaces also allows that parts can be independently produced. Structuring the safety architecture eliminates vagueness in descriptions and clarifies tradeoffs among analyses. Third, the risk decision-maker requires an understanding of social and political issues, technical issues, management issues, and communication issues. An overview of risk analysis, risk evaluation, and detailed view of layered scenarios will improve readability and comprehension [24].

As for compatibility between top-level functionalities of the framework, hazard identification should be systematic and structured, which means taking into account factors such as system boundaries, interactions with the environment and modes of operation and environmental conditions. SysML incorporates the advantages of systematic structure of object- and process-oriented methods, which can easily describe

the connection and data exchange among systems [23]. There is evidence that SysML proved its value in other safety models (see Sect. 2 about background). Information interpretation depends on information structure. Structuring information improves readability and comprehension, contributing to the creation of representations, and essential for the quality of data generation. Also, the scenarios in various layers require structure of causal relationships between the scenarios. Finally, the origin of a failure can come from decisions made earlier in the process. Complex systems come to be in the interaction of components. Baxter explains that undesirable events are simplistically seen as the result of organisational findings [25]. For these reasons, it is important to define the interactions between earlier explained layers.

6 Conclusion

The proposed framework combines safety data generation, data processing and structuring, definition of interactions and finally the creation of customized representations in order to predict, explain, and control risks by various safety experts, safety architects and safety managers.

For safety data generation, data will come from scenario-guided hazard analysis, consequences from causality analysis, risk matrices including risk acceptance criteria, and ALARP evaluations and decisions that influence the safety analyses. The focus of the Safety Architecture Overview Framework is on the properties and behaviors of functional flows and hazardous flows of the system under consideration. The structure upon which the framework is built consists of claims, evidence and arguments. The identification of causal scenarios allows safety experts, safety architects and safety managers to discover interactions between various flows and layers. Graphic representation exposes the interrelationships of events and their interdependence upon each other. By visualization, we make boundaries of safety decisions explicit, and reveal patterns such as links, inferences, and contextual relationships, that would be otherwise hard to find. The views consist of: a risk analysis overview, a risk evaluation overview, and a detailed view of scenario analyses. These views can illustrate the main interactions between the various layers and system components. Also, it is possible to illustrate the criticality of each layer and subcomponent. Explicit representation delivers insight, stimulates striving for completeness, and leads to consistency of the safety analysis.

In terms of acceptance, factors that would be of interest to the stakeholders for adoption of the framework are described in [5]. These are, among other things, more awareness and sensitivity for interrelationships between hazards and risks, but even more: comprehending the safety architecture and creating cross-discipline understanding. In response, we plan to test this framework in a real-life Dutch railway case that, at this moment, is setting up their risk analyses and evaluations.

References

1. Alexandersson, G., Hultén, S.: The Swedish deregulation path. Rev. Netw. Econ. **7**(1), 1–19 (2008)
2. European Union: Commission Decision of 25 January 2012 on the technical specification for interoperability relating to the control-command and signaling subsystems of the trans-European rail system. Off. J. Eur. Union **55**, 1–51 (2012)
3. UNIFE: UNISIG, An industrial consortium to develop ERTMS/ETCS technical specification. http://www.ertms.net. Accessed May 2018
4. Rajabalinejad, M., Martinetti, A., Dongen, L.A.M.: Operation, safety and human: critical factors for the success of railway transportation. In: Systems of Systems Engineering Conference, pp. 1–6 (2016)
5. Schuitemaker, K., Rajabalinejad, M.: ERTMS challenges for a safe and interoperable European railway system. In: Proceedings of the Seventh International Conference on Performance, Safety and Robustness in Complex Systems and Applications, pp. 17–22 (2017)
6. Stoop, J.A.A.M., Dekker, S.: The ERTMS railway signaling system: deals on wheels? An inquiry into the safety architecture of high speed train safety. In: Proceedings of the Third Resilience Engineering symposium, pp. 255–262 (2008)
7. Svedung, I., Rasmussen, J.: Graphic representation of accident scenarios: mapping system structure and the causation of accidents. Saf. Sci. **40**, 397–417 (2002)
8. Kelly, T.: Arguing safety a systematic approach to managing safety cases. PhD Thesis (1998)
9. Arnold, A., Point, G., Griffault, A., Rauzy, A.: The AltaRica formalism for describing concurrent systems. Fundam. Informatica **40**(2), 109–124 (1999)
10. Cuenot, P., Chen, D.J., Gerard, S., Lönn, H., et al.: Towards improving dependability of automotive systems by using the EAST-ADL architecture description language. In: Architecting Dependable Systems IV. Lecture Notes in Computer Science, vol. 4615, pp. 39–65 (2006)
11. Güdemann, M., Ortmeier, F.: A framework for qualitative and quantitative formal model-based safety analysis. In: Proceedings of the 12th IEEE International Symposium on High-Assurance Systems Engineering (HASE), pp. 132–141 (2010)
12. Cressent, R., David, P., Idasiak, V., Kratz, F.: Designing the database for reliability aware model-based system engineering process. Reliab. Eng. Syst. Saf. **111**, 171–182 (2013)
13. Falessi, D., Nejati, S., Sabetzadeh, M., Briand, L., Messina, A.: SafeSlide: a model slicing and design safety inspection tool for SysML. In: Proceedings of SIGSOFT FSE, pp. 460–463 (2011)
14. Sabetzadeh, M., Nejati, S., Briand, L., Evensen Mills, A.: Using SysML for modeling of Safety-critical software-hardware interfaces: guidelines and industry experience. In: IEEE 13th International Symposium on High-Assurance Systems Engineering, pp. 193–201 (2011)
15. De la Vara, J.L., Panesar-Walawege, R.K.: SafetyMet: a metamodel for safety standards. In: International Conference on Model Driven Engineering Languages and Systems, pp. 69–86 (2013)
16. Biggs, G., Sakamoto, T., Kotoku, T.: A profile and tool for modelling safety information with design information in SysML. Softw. Syst. Model. **15**(1), 147–178 (2016)
17. Mauborgne, P.: Operational and system hazard analysis in a safe systems requirement engineering process – application to automotive industry. Saf. Sci. **87**, 256–268 (2016)

18. Belmonte, F., Soubiran, E.: A model based approach for safety analysis. In: International Conference on Computer Safety, Reliability, and Security, pp. 50–63 (2012)
19. Yakymets, N., Dhouib, S., Jaber, H., Lanusse, A.: Model-driven safety assessment of robotic systems. In: Intelligent Robots and Systems, pp. 1137–1142 (2013)
20. Sharvia, S., Papadopoulos, Y.: Integrating model checking with HiP-HOPS in model-based safety analysis. Reliab. Eng. Syst. Saf. **135**, 64–80 (2015)
21. Blessing, L.T.M., Chakrabarti, A.: DRM, a Design Research Methodology. Springer, London (2009)
22. Pahl, G., Beitz, W., Feldhusen, J., Grote, K.H.: Engineering Design, a Systematic Approach. Springer, Berlin, Heidelberg (2003)
23. Wang, P.: Civil Aircraft Electrical Power System Safety Assessment: Issues and Practices. Butterworth-Heinemann (2017)
24. Brussel, F.F., Bonnema, G.M.: Interactive A3 architecture overviews. Proc. Comput. Sci. **44**, 204–213 (2015)
25. Baxter, G., Sommerville, I.: Socio-technical systems: from design methods to systems engineering. Interact. Comput. **23**, 4–17 (2011)