*Safety and Reliability of Complex Engineered Systems – Podofillini et al. (Eds)*
*© 2015 Taylor & Francis Group, London, ISBN 978-1-138-02879-1*

# An integral safety approach for design of high risk products and systems

M. Rajabalinejad, G.M. Bonnema & F.J.A.M. van Houten
*University of Twente, Enschede, The Netherlands*

ABSTRACT: To make the world a safer place while adapting high-end technologies, engineers have to address societal concerns about the safety of emerging high-tech systems. While adapting services provided by technology, people concern about their safety. It seems that engineers are struggling to control the fast-growing technology. From another perspective, the safety toolbox seems to be outdated as there are issues that cannot be addressed by inherited nature of the commonly used tools. As systems become more complex and more autonomous, the safety-toolbox requires improvements to catch up new developments. This paper sheds light on societal concerns on safety issues, discusses commonly practiced design methods for dealing with safety, and suggests an integral safety approach. While the application range of this subject is indeed very broad, this study keeps its focus on the industrial design discipline.

## 1 INTRODUCTION

In the world of high risk technology, safety becomes more and more important for human societies. Smart and autonomous products are operating beyond the boundaries of a specific system (Jamshidi 2011). More and more complex systems and systems of systems are emerging, and there is a challenge for engineers to ensure safety of these systems. This rather fast technological development is subject to societal concerns (see for example (Harvey & Stanton 2014, Perrow 2011). Recent warning of Stephen Hawking about the future of artificial intelligence clearly reflects this societal concern when he says "Artificial intelligence could be the worst thing to happen to humanity" (Woollaston 2014).

Humanity has been always demanding safety against dangers and now against new technologies (Hansson 2009). Safety is a ubiquitous term which comes more and more into societal attention. Industrial safety, medical safety, organizational safety, safety of sociotechnical systems, safety of system of systems etcetera are a few examples presenting this concern from different perspectives which can be equally important. The increasing complexity of systems demands a multi-disciplinary approach to address safety concerns. For example, a public transport sector uses civil, information, industrial and organizational infrastructures to deliver services to the society. Needless to say that all these infrastructures should operate safely to deliver safe services; safety is below on Maslow's pyramid (Maslow 1943). Yet safety definition differs from one discipline to another. Besides, integration of two safe disciplines does not necessarily imply safe-operation. For example, if using a mobile phone is safe and driving a car is safe, it doesn't imply that driving a car while using a mobile is safe. This integration may result in a situation that the system does not fail but it does not operate safely. Another example of this situation happened in a train accident in the Netherlands in 2013 where a passenger with poor vision took a wrong door for leaving the train. This resulted in injury where neither a hardware nor a software failure was reported. Such a system behavior follows design flaws or system complexity. One, therefore, may conclude that increasing complexity of systems leads to more unexpected behaviors. This results in doubts if the engineers are able to control the fast-growing technology.

The points discussed above reflect some concerns have to be addressed primarily by "system designers" because they can more effectively tackle these issues. It is not convincing to only apply the available tools. Thus the question is how to address these issues? To start answering this question, we first discuss the commonly practiced approaches, recent developments and conclude the need for an integral safety approach.

## 2 SAFETY AND COMMONLY PRACTICED APPROACHES

### 2.1 *Performance triangle*

In a highly competitive market, industry demands a higher performance by emphasizing on three pillars of cost, quality and time to the market as shown in Figure 1 (see for example (Theisens 2014)). In this performance context, safety is implicitly present through quality or cost. In industrial design context, designers pay often a great attention to safety and naturally check their design against safety criteria trying to catch any possible design errors and correct them before production (Hale, Kirwan et al. 2007). Yet is has been observed that the system has failed in unexpected or unpredicted ways, or because the system operators had other ideas about how it was functioning, and there are limited resources for a designer to explore unexpected situations. Furthermore, some designers may consider safety as a system attribute which hinders the performance, imposes extra costs and implies extra features and resources. This has been discussed in literatures as the safety culture (Reiman and Rollenhagen 2014). While trying to improve the safety culture to more explicitly attend to safety issues, we should review the design process and the currently practiced safety-toolbox.

### 2.2 *Engineering design process*

The engineering design process is formulated by several steps starting from analyzing the problem, identifying requirements, generating ideas and concepts, embodying the chosen concept followed by detail design and testing (Pahl, Beitz et al. 2007). Figure 2 shows the roadmap of product design according to (Eger, Bonnema et al. 2013) describing the design process as logical sequence of several phases: preliminary design, design phase, embodiment and detailing phase and implementation phase. In this process, safety is often treated as a requirement must be addressed through the process.


Figure 1. Performance in industrial design is identified by focusing on three pillars of cost, quality and time to the market.

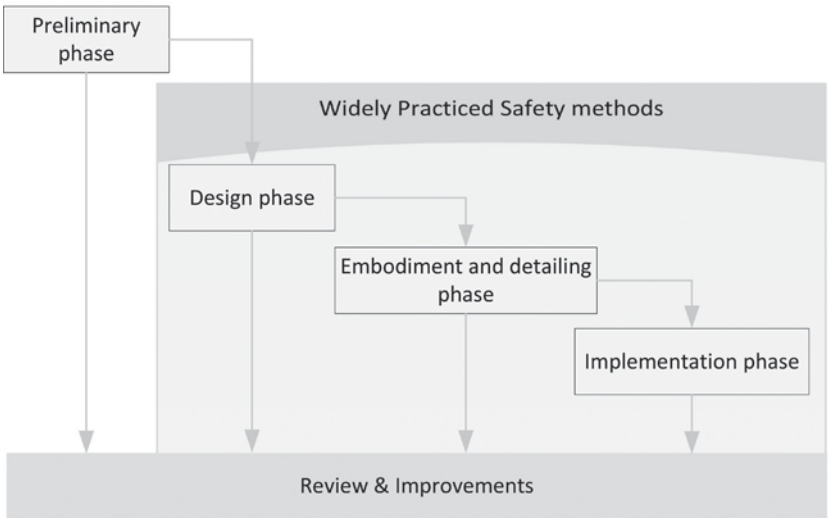


Figure 2. A road map for Engineering Design process adapted from (Eger et al. 2013).

In the design process, a Preliminary Hazard Analysis (PHA) is usually performed to inform stakeholders about possible hazards or risks. Safety techniques are often applied during and after the design phase (see Figure 2) where a concept is already formed. Failure Mode and Effect Analysis (FMEA) is commonly used for exploring the possible failure scenarios, assigning failure probabilities and analyzing its effects or consequences. To represent hierarchy of faults or subsequent events, Fault Tree Analysis (FTA) (Jamboti and Liggesmeyer 2012, Rajabalinejad, van Gelder et al. 2007) or Event Tree Analysis (ETA) are commonly used (Stapelberg 2009). The essence of these methods are based on the component failure; a system failure is presented as a logical chain of events or faults. Methods like Fishbone, Cause & Effect diagram, or Root Cause Analysis focus on the relationship between hazard and possible events. To estimate the likelihood of these events, Probabilistic Risk Assessment (PRA) methods, Bayesian Belief Networks (BBN) or Incident Tree Method (ITM) (Wang, Jiang et al. 2010) may be used. To minimize the expected error or risk, Lean Six Sigma method is utilized.

A common assumption among these methods is that a working system or product does not fail. Furthermore, human error is treated in the same way as a component failure. The implemented methodologies often make no difference between modeling a component or human. In this context, reliability is thought to be similar to safety and the applied tools become incapable of capturing a situation which is unsafe but not initiated with a failure (Fleming 2015).The shortcomings of this assumption is becoming more and more obvious when systems become more complex, and system integration requires special attention. Next section focuses on the commonly practiced approaches in early phases of system design and system architecture.

### 2.3 *Systems engineering and design*

Systems Engineering is a discipline focusing on the design and application of the whole system (integration of system components) as distinct from its parts in order to ensure a working system which satisfies user requirements (Forsberg & Krueger 2007). In systems engineering, life cycle stages are mainly described at concept, development, production, utilization, support and retirement levels. This process treats safety as a system measure that reflects customer/user satisfaction along with other system measures such as performance, reliability, availability, maintainability and workload. Furthermore, it suggests using Failure Modes and Effect Analysis (FMEA), Failure Modes and Effects Critically Analysis (FMECA) or hazard analysis to identify the critical system level requirements (see e.g. (Lopez, Di Bartolo et al. 2010)). When design starts at the architectural level, the focal points are on functional and performance requirements, constraints and interfaces. To derive a logical architecture, the use of modeling languages such as SysML is recommended at this stage.

The committed cost at the concept project lifecycle is less than 10% which increases up to 15% at the design phase. This motivates further investment on early design phases in order to ensure a robust system architecture capable of fulfilling system requirements and ensuring the sharing of consistent and common information across. DoDAF is the architecture framework used in the Department of Defense of United States. This architecture framework focuses on architectural data as information required for making critical decisions and allows architects to visualize this information through consistent models. The Open Group Architecture Framework (TOGAF) also aims to improve the organizational performance typically modeled on four levels of business, application, data and technology. Zachman framework is an ontology based framework which provides a structured views for defining an enterprise (Zachman 1999). Among others, A3AO architecture is a framework that aims to facilitate communication (Borches 2010). In these architecture frameworks, safety is treated often as a requirement which has to be addressed along with other system requirements (Schuitemaker, Rajabalinejad et al. 2015).

## 3 THE PROBLEM

### 3.1 *Safety issues*

Engineered systems demand more autonomy and more power. Along with these two growing demands, complexity of these systems is arising. This system complexity leads to uncertainty in system behavior or performance.

There are situations undefined or unexpected in system design or performance. This uncertainty in performance or behavior can lead to undesired system performance or unpredicted system behavior which leads to safety issues. This process is depicted in Figure 3.

The ultimate scenario portrayed in science-fiction stories or movies portrays situations where technologies become fully autonomous. Then it becomes so powerful which unexpectedly behave as the enemy of human kind.

### 3.2 *The toolbox*

When systems are being created and through different design phases, the primary concerns of design

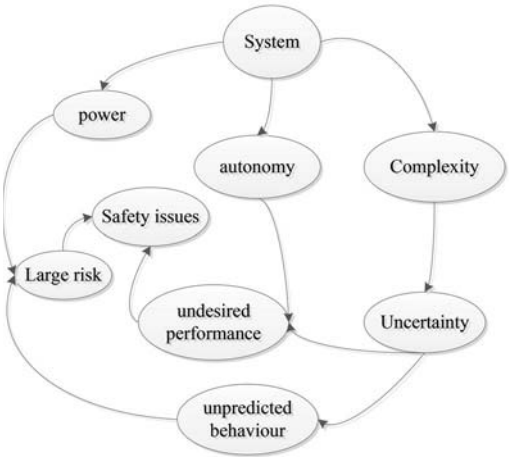


Figure 3. Safety issues of a system shown through an influence diagram.

engineers are fulfilling the requirements. Engineering tools support creating a system which works reliably as discussed in 2. Systems are designed to work as intended and their failure is coming through the components failure or human error. Many of currently practiced tools treat human error similar to a component failure. It means that if the system does not work properly and yet there is no component failure, the failure is undefined! Besides, the arising complexity of systems may lead to undesired performance or unpredicted behavior: a situation that may lead to scenarios where the designers or stakeholders were not prepared for, and they observe this with surprise. Such circumstances may endanger the society.

Furthermore, the available safety tools mainly support fragmented analysis of a system. The safety analysis of system is often field specific. We analyze a system from a certain perspective to design it robust, reliable, fault tolerant and safe. The integration process is rather developed in reliability engineering, and the effect of each component failure at the system level can be seen through a chain of events. Yet, integration of two reliable and perfectly working components may lead to safety issues. The train example described earlier is an example of a working system which is unsafe. The arising complexity of system of systems makes it impractical to use reliability-based safety analysis modelling all the possible combinations of unexpected system behavior.

## 4 TOWARDS SOLUTIONS

Technology rises societal expectations for a higher quality living and for safer living place. Consider for example a flood prone area where the accepted risk level continuously reduces as people expect from technology to provide them better weather forecast and safer/more robust flood defenses (Rajabalinejad and Demirbilek 2013). Furthermore, it becomes easier to share and use worldwide experience in tackling hazards and safety issues. The increasing complexity of systems along with rising expectations for public safety and transparency enforce us to think of developing new approaches to tackle safety issues at the system level for which systems thinking is prerequisite.

System safety looks like a puzzle composed of many parts. To see the whole picture, we need to think about the whole system and not only parts (or disciplines) and implement system thinking (checkland 2000). System thinking has been successfully applied into safety domain by Leveson resulting in System Theoretic Accident Modeling and Processing (STAMP) (Leveson 2012), and it has been tested in different studies (Leveson 2015). Safety thinking starts at early phases of system lifecycle and certainly before having any system architecture. The first step in this perspective is exploring safety-related things. In this process, system stakeholders, system components, system environment, system users and operators, system interfaces, and other adjacent systems are parts of the whole picture. The contribution of these parts in the complete safety picture requires further attention as differences between safety and reliability may confuse system stakeholders (Leveson 2012). Having that clarified, one should see how different system elements influence the system safety. It is desired to define system safety as a key performance indicator so that it can explicitly take a controlling role in systems architecture. Yet definition of objective measures for system safety measures requires further developments (Hale 2009).

Assessment of system safety is not always straight forward. There are many details that influence system safety. Here the devil is in and also beyond the details. Besides, the exceptional performance or condition of some detail component may create unexpected situations. A domino model of safety issues (Khakzad, Khan et al. 2014) or the Swiss cheese model of system flaws (Underwood and Waterson 2014) are example models describing how a chain of events can normally lead to a system failure (Perrow 2011). For system safety, one must pay attention in to system details and processes along with its environment.

Safety concerns are present in system lifecycle and they have to be addressed all along the system life cycle. Safety thinking starts at earliest project phases, yet safety requires continuous screening at different system levels. Dynamism of system evolvement and system environment can influence

system performance and its safety. This implies different safety views at different stages of system life cycle. As a system cannot be created by an individual stakeholder, system safety requires a pluralistic approach which integrates interests and concerns of all stakeholders. For example, the user, operator, and environment may have different safety requirements.

The points discussed above clarifies the needs for an approach which can integrate safety issues and treat them as a whole. A foundation which can integrate the system concerns, dynamism, complexity and plurality. This is further explained through the next section.

## 5 CASE STUDY

Operation of high speed trains in the Netherlands is currently under focus in order to improve its performance. In such a complex system, more than 14 stakeholders cooperate to provide the optimum services for passengers. Through our study, some of the stakeholders were interviewed with regard to their safety perspectives. The following expectations appeared to be of primary importance for them.

- System definition: The need for defining proper system boundaries which comes into the agreement of all stakeholders. This comes as the first step influencing the other considerations with regards to the system operation or performance.
- Chain of events: The effects of possible failure on the system safety and its operation is to be clarified for the stakeholders.
- Hazard management: identification of hazards and its allocation for proper actions.
- Risk identification, monitoring, and management: Hazards and their consequences define risk, which have to be monitored and managed. The total system risk can be defined as a key performance indicator for the system.
- Emergency management: next to hazards and risks, plans and logistics for optimum actions are of relevance for managing emergency situations.

There are currently a number of hazards identified for this system, where every single one may involve more than one stakeholder with different safety considerations. These identified hazards are under the influence of system definition, and changes in system boundaries leads to changes in the number of hazards. Besides, the influences of any possible failure on the operational system demand a systematic approach where the chain of events are recognized and clearly communicated to system stakeholders. Furthermore, quantification of hazards and their consequences should be available and communicable to system stakeholders. Next to these, it is of primary importance to set clear rules for responsible actors in the case of emergency situation. To address these, an integral approach was implemented which we discuss through the next section in further details.

## 6 IMPLEMENTED ARCHITECTURE

The case study, described in the previous section, determined the needs for an architecture that preserves the complete safety-picture of the system while allows the details to be elaborated in real time. This suggests a layered architecture where different system views can be generated and at the same time propagated through a complete model. This requires a meta-model, called the Safety Information Model (SIM), acting as the integral part of the safety system. Such a SIM should be capable of capturing the whole safety context and generating customized views. An integral approach that allows the zoom-in zoom-out feature in real time and is capable of propagating system changes at different levels simultaneously.

As shown schematically in Figure 4, the implemented SIM is composed of two pillars for first modeling the safety information and second communicating customized views. SIM uses models of systems, hazards, accidents, regulations, etc. see e.g. (Cafiso, Di Graziano et al. 2010, Hojati, Ferreira et al. 2013, Wymore 1993).

Furthermore, SIM is capable of generating customized views for stakeholders through A3 architecture. Our experience through this study has proved the advantages of this method for effectively communicating the safety characteristics with stakeholders.

## 7 DISCUSSION

To address the stakeholders' concerns in the case study described through Section 5, an integral approach was implemented and its architecture was described through the previous section. The implemented architecture is based on the safety information model and its A3-views.

The implemented architecture ensures consistency of safety information as there is only one safety model used across the whole system. Furthermore, it increases transparency of system safety as it e.g. clarifies the chain of events for any possible failure. Likewise, this integral approach accommodates stakeholders' needs for identification and management of system hazards and risks.

In addition, task distributions with regards to risk mitigation becomes a part of the architecture, and the monitoring of system safety (and influence of possible actions on the whole system) is observable in real-time.

Customized safety views are produced based on the stakeholders requirements or expectations. An example A3 view is shown in Figure 5. Further details on the components of this view is presented in in (Schuitemaker, Rajabalinejad et al. 2015).

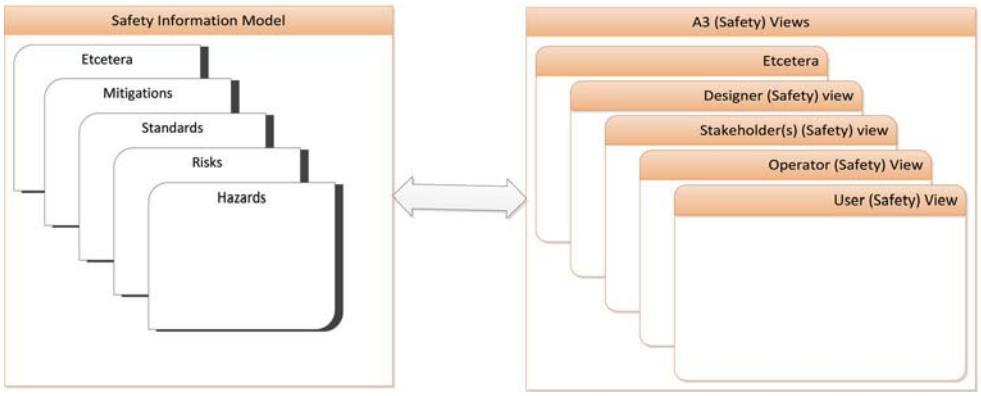


Figure 4. The safety architecture used for the case study.

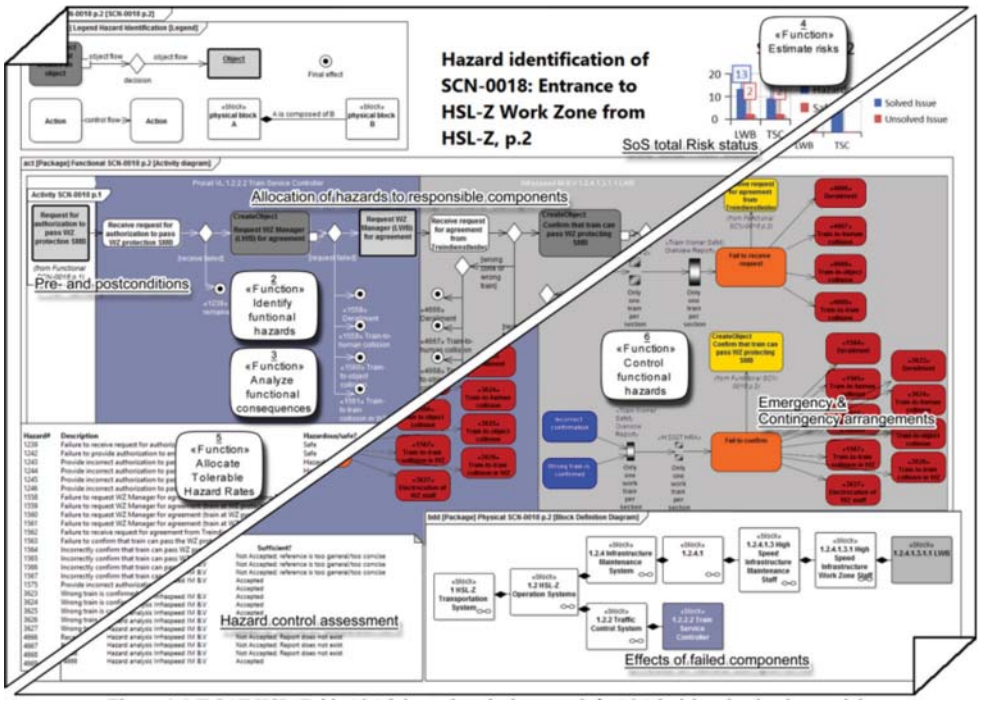


Figure 5. An example A3 overview used to communicate with stakeholders, for further details see (Schuitemaker, Rajabalinejad et al. 2015).

## 8 CONCLUSIONS

Fast growing technology enables complex systems that demand for more autonomy and more power. Undesired performance or unpredicted behavior follow this increasing system complexity which leads to unsafe circumstances. To tackle this, engineers need to renew their safety toolbox. New approaches should support system safety during the whole project lifecycle, integrate different views and concerns of system stakeholders, and be able to brows at different system level from the level to system level. They should be capable of dealing with system dynamism and propagate the influence of any changes simultaneously through the whole system.

Here we share some lessons learnt through a case study of high speed train lines in the Netherlands and we share our approach in dealing with safety concerns of such a complex system. In this paper, we described the architecture of our solution to tackle this growing system complexities. We used the Safety Information Model as an integral part which is capable of generating customized views for the stakeholders. Through this study we learned that the implemented approach can effectively increase consistency, transparency and task distribution with regards to safety issues at the system level.

## REFERENCES


Borches, P. D. 2010. A3 Architecture Overviews. PhD, University of Twente.

Cafiso, S., A. Di Graziano, G. Di Silvestro, G. La Cava & Persaud B. 2010. Development of comprehensive accident models for two-lane rural highways using exposure, geometry, consistency and context variables. *Accident Analysis and Prevention* 42(4): 1072–1079.

Checkland, P. 2000. Soft Systems: Methodology: A Thirty Year Retrospective. *System Research and Behavioral Science.*

Eger, A., M. Bonnema, E. Lutters & Voort M.v.d. 2013. *Product Design*, Eleven International Publishing.

Fleming, C.H. 2015. Safety-driven Early Concept Analysis and Development. PhD, MIT.

Forsberg, K. & Krueger, M. 2007. Systems Engineering Handbook A Guide For System Life Cycle Processes and Activities.

Hale, A. 2009. Why safety performance indicators? *Safety Science* 47(4): 479–480.

Hale, A., B. Kirwan & Kjellen U. 2007. Safe by design: where are we now? *Safety Science* 45(1–2): 305–327.

Hansson, S.O. 2009. *Risk and Safety in Technology. Philosophy of Technology and Engineering Sciences.* A. Meijers. Amsterdam, North-Holland: 1069–1102.

Harvey, C. and Stanton N.A. 2014. Safety in System-of-Systems: Ten key challenges. *Safety Science* 70: 358–366.

Hojati, A.T., Ferreira, L., Washington S. & Charles P. 2013. Hazard based models for freeway traffic incident duration. *Accident Analysis and Prevention* 52: 171–181.

Jamboti, K. & Liggesmeyer P 2012. A Framework for Generating Integrated Component Fault Trees from Architectural Views. 114–121.

Jamshidi, M. 2011. *System of systems engineering: innovations for the twenty-first century.* John Wiley & Sons.

Khakzad, N., Khan, F., Amyotte P. & Cozzani V. 2014. Risk Management of Domino Effects Considering Dynamic Consequence Analysis. *Risk Analysis* 34(6): 1128–1138.

Leveson, N. 2012. *Engineering a Safer World*. Cambridge, Massachusetts, Massachusetts Institute of Technology.

Leveson, N. 2015. A systems approach to risk management through leading safety indicators. *Reliability Engineering & System Safety* 136: 17–34.

Lopez, F., Di Bartolo, C. Piazza, T. Passannanti, A. Gerlach, J. C. Gridelli, B. & Triolo F. 2010. A Quality Risk Management Model Approach for Cell Therapy Manufacturing. *Risk Analysis* 30(12): 1857–1871.

Maslow, A.H. 1943. A theory of human motivation. *Psychological review* 50(4): 370.

Pahl, G., Beitz, W. Feldhusen, J. & Grote, K.H. 2007. *Engineering Design A Systemmatic Approach.* Springer.

Perrow, C. 2011. *Normal accidents: Living with high risk technologies.* Princeton University Press.

Rajabalinejad, M. & Demirbilek, Z. 2013. A Bayesian probabilistic approach for impacts of sea level rise on coastal engineering design practice. *Ocean Engineering* 71: 66–73.

Rajabalinejad, M., van Gelder, P. H. A. J. M., Vrijling, J. K., Kanniing W. & van Baars, S. 2007. Probabilistic Assessment of the Flood Wall at 17th Street Canal, New Orleans. *Risk, Reliability, and Social Safety*. Stavanger, Norway. III: 2227.

Reiman, T. & Rollenhagen, C. 2014. Does the concept of safety culture help or hinder systems thinking in safety? *Accid Anal Prev* 68: 5–15.

Schuitemaker, K., Rajabalinejad M. & Braakhuis J. 2015. A Model Based Safety Architecture Framework for Dutch High Speed Train Lines. *System of Systems Engineering*.USA.

Stapelberg, R.F. 2009. *Handbook of Reliability, Availability, Maintainability and Safety in Engineering Design.* Springer.

Theisens, H.C. 2014. Climbing the Mountain. Amsterdam, Lean Six Sigma Academy.

Underwood, P. & Waterson, P. 2014. Systems thinking, the Swiss Cheese Model and accident analysis: A comparative systemic analysis of the Grayrigg train derailment using the ATSB, AcciMap and STAMP models. *Accident Analysis and Prevention* 68: 75–94.

Wang, W. H.,. Jiang, X. B., Xia S. C. & Cao Q. 2010. Incident tree model and incident tree analysis method for quantified risk assessment: An in-depth accident study in traffic operation. *Safety Science* 48(10): 1248–1262.

Woollaston, V. 2014. Dailymail, Mailonline.

Wymore, A.W. 1993. *Model-based systems engineering*, CRC press.

Zachman, J.A. 1999. A framework for information systems architecture. *Ibm Systems Journal* 38(2–3): 454–470.