SCIENCE • TECHNOLOGY • RESEARCH HIGHLIGHTS • VISIONS
Dissertation
69

An approach for the assessment of safety risks in automated mobile work-machine systems

Risto Tiusanen

VTT

VTT SCIENCE 69

An approach for the assessment of safety risks in automated mobile work-machine systems

Risto Tiusanen

Thesis for the degree of Doctor of Science in Technology to be presented with due permission for public examination and criticism in Festia Building, Auditorium Pieni Sali 1, at Tampere University of Technology, on the 21st of November 2014, at 12 noon.

ISBN 978-951-38-8172-6 (Soft back ed.)
ISBN 978-951-38-8173-3 (URL: http://www.vtt.fi/publications/index.jsp)

VTT Science 69

ISSN-L 2242-119X
ISSN 2242-119X (Print)
ISSN 2242-1203 (Online)

JULKAISIJA – UTGIVARE – PUBLISHER

VTT
PL 1000 (Tekniikantie 4 A, Espoo)
02044 VTT
Puh. 020 722 111, faksi 020 722 7001

VTT
PB 1000 (Teknikvägen 4 A, Esbo)
FI-02044 VTT
Tfn +358 20 722 111, telefax +358 20 722 7001

VTT Technical Research Centre of Finland
P.O. Box 1000 (Tekniikantie 4 A, Espoo)
FI-02044 VTT, Finland
Tel. +358 20 722 111, fax +358 20 722 7001

Grano Oy, Kuopio 2014

Acknowledgements

The strong research interest for the subject of this thesis in industry has made it possible to carry out this research persistently over this long time period. The research and development work in research projects and the practical implementation of the risk-assessment approach and the risk-analysis methods in industrial projects have been carried out in close co-operation with globally operating mobile work-machine manufacturers, their international subcontractors, and final customers as system end users. I am thankful to all co-operating industrial partners and all the industrial exerts with whom I have had the opportunity to work with. Especially I want to thank Sandvik Mining and Construction and Cargotec for the possibility to use the project materials in the case study research.

I am thankful to the Education Fund for granting me an adult education allowance in for altogether five months. This made it possible to take leave of absence and concentrate to examine the four large case projects, analyse the findings, and write part of the manuscript. I am also thankful to the Finnish Work Environment Fund for granting me a scholarship for two months and to VTT Technical Research Centre of Finland for supporting me for writing and finalising the manuscript. The case study research and the review of the latest system safety literature was associated and partly funded by an on-going research project FAMOUS (Future Semi-Autonomous Machines for Safe and Efficient Worksites). The research project is part of FIMECC's (Finnish Metals and Engineering Competence Cluster) research program EFFIMA (Energy and Life Cycle Efficient Machines) and the main financier of the research project is Tekes – the Finnish Funding Agency for Innovation.

The research reported on here was done at VTT in Tampere, first at the Risk and Reliability Management Knowledge Centre and then at the Life Time Management research area. I would like to thank my colleagues Jarmo Alanen, Kaj Helin, Marita Hietikko, Vesa Hämäläinen and Timo Malm who participated and supported the research projects and the case projects related to my thesis work. I am grateful for their valuable contribution to the research and for the open and communicative co-operation over the years. I would also like to thank my fellow doctoral candidates Riitta Molarius and Teuvo Uusitalo and DSc (Tech) Mervi Murtonen for their encouragement and inspirational discussions in our self-

organised peer group. I also like to thank Pirjo Hyvärinen-Kantee and Taina Toivonen for their practical help for the thesis.

Professor Jouni Kivistö-Rahnasto from Tampere University of Technology has been the supervisor for my thesis. I wish to express my sincere thanks to him for the most competent and systematic guidance and advice for the research work and writing of the thesis. In VTT I wish to thank research professor Veikko Rouhiainen who has given me valuable advice for the research and constructive criticism for the manuscript. I would like the thank also DSc (Tech) Risto Kuivanen, DSc (Tech) Markku Reunanen and Lic.Sc. (Tech) Helena Kortelainen who also read the manuscript and gave valuable comments and advice to improve it.

I would like to express my gratitude to Professor Marvin Rausand from Norwegian University of Science and Technology and Associate professor Paul Swuste from Delft University of Technology, who acted as preliminary examiners of my thesis and gave valuable comments and advice to improve it.

On a personal level I am thankful to my children Henri, Marjo and Petri and all my nearest and dearest for their support and encouragement. Especially I would like to thank Aada and Kasper, our dear grandchildren, who bring joy to grand papa's life. Playing board games or sledding down with them made me easily forget the academic contemplation and in fact the whole thesis for a while.

Finally I would like to express my warmest thanks to my beloved wife Leena for her support and understanding during the time I have been writing and processing my work.

Nokia, 27.10.2014

Risto Tiusanen

Academic dissertation

Supervisor	Professor Jouni Kivistö-Rahnasto Tampere University of Technology
Reviewers	Associate professor, Paul Swuste Delft University of Technology
	Professor, Marvin Rausand Norwegian University of Science and Technology
Opponents	Professor, Matti Juhala Aalto University
	DSc (Tech), Markku Aaltonen Finnish Institute of Occupational Health

Contents

List of abbreviations

ALARP	As low as reasonably practical
CAN	Controller Area Network
DoD	United States Department of Defence
E/E/PE	Electrical / electronic / programmable electronic
EUC	Equipment under Control
FMEA	Failure mode and effect analysis
HAZOP	Hazard and operability (a type of study)
HIL	Hardware-in-the-loop (testing)
IEC	International electro technical commission
IPL	Independent protection layer
ISO	International organization for standardization
LHD	Load, haul and dump machine
LOPA	'Layers of protection' analysis
OHA	Operating hazard analysis
PHA	Preliminary hazard analysis
RAMS	Reliability, availability, maintainability, and safety
SE	Systems engineering
SHA	System hazard analysis
SSHA	Subsystem hazard analysis
VNa	Government decree
VTT	VTT Technical Research Centre of Finland

Definitions

Automation	'Automation' in this thesis refers to the use of control systems and information technologies to reduce the need for manual work in production systems and in machinery applications.
Function	A function is a task, action, or activity that must be accomplished if a desired outcome is to be achieved (IEEE 1233:1998, p. 3).
Functional safety	Functional safety is part of the overall safety related to the equipment controlled and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk-reduction measures (SFS EN 61508-4:2010, p. 21).
Harm	Harm is physical injury or damage to health (SFS EN ISO 12100:2010, p. 2) or can refer to physical injury or damage to the health of people or damage to property or the environment (ISO IEC Guide 51 1999, p. 2).
Hazard	A hazard is a potential source of harm. For example, in its origin, it might be a mechanical or an electrical hazard; in terms of the nature of the potential harm, it could be a cutting hazard, a toxic hazard, or a fire hazard (SFS EN ISO 12100:2010, p. 2).
Hazardous event	A hazardous event is an event that can cause harm (SFS EN ISO 12100:2010, p. 2).
Machinery, machine	Machinery is an assembly, fitted with or intended to be fitted with a drive system consisting of linked parts or components, at least one of which moves and that are joined together for a specific application (SFS EN ISO

	12100:2010, p. 1). The term also covers assemblies of machinery that, for reaching the same end, are arranged and controlled so as to function as an integrated whole (Directive 2006/42/EC 2006, p. 27).
Model	A model is a preliminary work or construction that serves as a plan from which a final product is to be made or is used in testing or perfecting a final product. A model can also be a schematic description of a system, theory, or phenomenon that accounts for its known or inferred properties and may be used for further study of its characteristics. See http://www.thefreedictionary.com/model.
Safety engineering	Safety engineering in this study means the efforts supporting designers', manufacturers', end users', and other stakeholders' work to develop and maintain adequate safety in industrial applications.
Safety integrity	The term refers to the probability of an electrical, electronic, or programmable electronic safety-related system satisfactorily performing the specified safety functions under all stated conditions within a stated period of time (SFS-EN 61508-4:2010, p. 35).
System	A system is a combination of interacting elements organised to achieve one or more stated purposes (ISO IEC 15288:2008, p. 6). It is a set or arrangement of elements – people, hardware and software products, and processes (facilities, equipment, materials, and procedures) – that are related and whose behaviour satisfies operational needs and provides for the life-cycle sustaining of the products (ISO IEC 26702:2007, p. 9).
Use-case description	Use-case descriptions are commonly used in software and systems engineering to define the interaction (dialogue) between a user and a technical system as a sequence of steps (Cockburn 2001, p. 53).
Work equipment	A piece of work equipment is any machine, apparatus, tool, or installation used at work (Directive 2009/104/EC 2009, p. 5).
Work site	'Work site' in this thesis refers to an area where a mobile work machine application is located and where the machinery operations takes place.

1. Introduction

Mobile work machines (also called mobile work equipment or just mobile machines) are widely used in industrial work environments such as at construction sites, mines, logistics centres, harbours, terminals, warehouses, and agricultural and forestry work sites, along with many other work tasks, related to, for example, real-estate management and rescue services. Most mobile work machines today are traditional manually operated machines in which the driver (operator) sits in a cabin and controls the machine's movements and operations (see Figure 1).

Figure 1. Mobile work machines.

Mobile work machines are typically diesel-powered or electrically powered and equipped with hydraulic or electric actuating mechanisms such as a boom, bucket, hoist, or gripper. Fully electric versions are used in some applications. The control systems of modern mobile work machines are based on distributed CAN-bus implementations with automated functions, and they can have several modes of operation, from manual to fully automatic functioning.

1.1 The road from machines to automated machinery systems

The trend in development toward automated mobile work-machine systems has continued for about 20 years. Automated functions have been developed to support the machine operator with, for instance, boom handling, hook positioning, lifting, load gripping, and other features to improve work tasks' execution in cases of frequently repeated operations or machine movements. Automated functions of mobile work machines can include, among others, automatic control functions, automatic data collection and transfer, condition monitoring and diagnostics, and automatic information management (for positioning information, work orders, work instructions, warnings, driving assistance, etc.). Remote control for mobile work machines has been developed for, among other purposes, enabling the control of machine movements or machine manoeuvres from a good, safe position at the work site (with line-of-sight control) or to enable the control of the machines from a safe and comfortable environment far from the work site (control by tele-operation) (Uusisalo 2011, p. 12; Vilenius 2007, p. 10). Global megatrends in industry such as energy-efficiency, tightening of exhaust emission regulations for diesel engines, safety regulations growing stricter, and work processes' automation are guiding also the development of mobile work-machine technology.

Work processes executed with mobile work machines are typically batch processes in which each machine operation is performed separately. To improve productivity, safety, utilisation of special machinery, and handling of operation costs, companies are seeking better control and management of the overall work process. The trend seems to be to guide mobile work-machine operations in the direction of continuous automated work processes. Automatic guided vehicles and similar automatic material-handling machine systems have been used for years. For open-air conditions, some large-scale machinery systems already apply automated or autonomous work machines, such as automatic container-handling systems in harbours and autonomous ore-transportation systems in mines.

In this study dealing with automated mobile work-machine systems, it is important to clarify the distinction from manually driven mobile work machines. From the technical point of view, automated mobile work-machine systems are defined in this study such that the automation system controlling one or more mobile work machines has a hierarchical structure including a production control level, system operation control level, and on-board automation level. From the operation standpoint, the machines at the work site can be operated remotely from a control room or operate autonomously, but they can also be manually driven. One major element in automated mobile work-machine systems is the communication system, which connects all the subsystems and control levels and links the system to other systems. The connection to the machines is wireless in most cases. A schematic overview of an automated mobile work-machine system is provided in Figure 2.

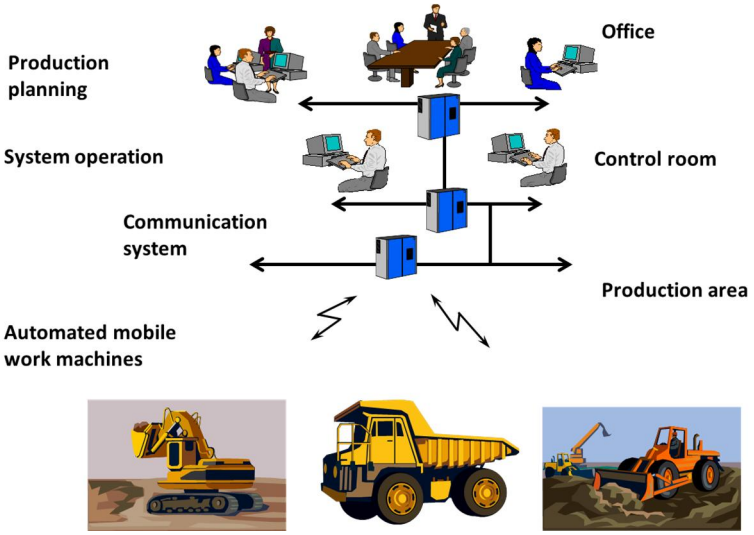


Figure 2. The main elements of an automated mobile work-machine system.

From a life-cycle perspective, manual work machines and an automated mobile work-machine system differ greatly. Manual work machines are products that are placed on the market, but automated mobile work-machine systems are unique projects. The systems are built and commissioned at the work site in the final production environment. From both of these perspectives, such machinery applications can be compared with large process-automation applications. From the machine manufacturer's point of view, the switch from machines to automated machinery systems transforms the design and engineering problems from machine design and manufacturing issues into system design, systems engineering, subsystem integration, system installation, and commissioning ones.

In technical terms, automated mobile work-machine systems as described above are multi-technology complicated systems such as production lines in a factory or paper machines in a paper mill. They have a huge number of subsystems and components connected and functioning together and interacting in line with pre-programmed rules. On the other hand, there is a certain difference from fixed industrial automation systems. Automated mobile work-machine systems can be considered complex socio-technical systems wherein people, machines, the automation system, and the operating environment interact with each other. Complex systems typically have many components that can autonomously interact through emergent rules (Amaral & Uzzi 2007, p. 1033).

1.2 New safety threats and challenges to safety engineering

From a design and development point of view, the move from machines to automation systems introduces new challenges to the manufacturer's and system

supplier's development processes. According to a recently published study on system design (Boucher & Kelly-Rand 2011), there are five main challenges in system design: lack of cross-function knowledge among designers, system complexity evolving into a complex ecosystem of systems of systems, increasing difficulty of identification of system-level problems early in the system-development process, difficulties with prediction of system behaviour before physical prototypes exist, and lack of integrated tools for multi-engineering disciplines (ibid., pp. 5–6).

Machine manufacturers and system suppliers are responsible for their products', machines', and machinery systems' safety. The shift from manually operated mobile work machines toward automated mobile work-machine systems takes machinery-safety considerations also to a new, system safety, level. Traditional issues of machinery safety are becoming system-safety issues. From discussions with mobile machine manufacturers and system suppliers, the biggest concern seems to be the new automation-related threats and possible unexpected hazardous events. New safety threats are seen in complex human–machine interactions, complex system operations and maintenance situations, systematic or random system failures in control systems, and system interfaces within the operation environment at the work sites. Experiences from other sectors of industry wherein automation has been utilised for years confirm these concerns. Among others, Rasmussen (1997), Leveson (1995, 2011b), and Endsley (1995) have pointed out that the system complexity, increased amount of software, automated functions, and automatic operation bring out new safety issues and design problems for system designers and safety engineers.

Leveson (1995) described potential problems related to the construction of software in industrial applications. Complex software always displays design errors, requirement flaws, or implementation bugs. Flexibility for changes can increase complexity in software programs and introduce errors. In large programs, separation into modules decreases the complexity of individual modules but increases the number of interfaces between modules and can thereby increase errors in interface design (ibid., pp. 33–38). On the other hand, more complexity and interaction between subsystems makes it difficult for system designers to consider all operation situations and system states in advance. There will also be a great deal of interaction and communication between the operators and maintenance staff. For system operators, with greater complexity and interaction come new challenges for handling all of the planned situations and, especially, unplanned and unexpected events so that safety can be ensured in all circumstances (Leveson 2004, p. 239). Rasmussen (1997, p. 184) stated that a system is always more than the sum of its elements and pointed out that system complexity leads to problems in risk management. Complex socio-technical systems are difficult to model with structural or functional models because system and operator behaviour in actual work situations is strongly dependent on the specific situation and effects in the work-site environment. There is need for conceptual models beyond traditional structural and behavioural system models (ibid., p. 187). From a safety-engineering perspective, Leveson (2004, p. 238) has claimed that technology is changing more rapidly than engineering techniques are. She points out issues such as increasing

'complexity and coupling', 'more complex relationships between humans and automation', the 'changing nature of accidents', and 'new types of hazards' as characterising the development of new technology in industry and causing uncertainty and new safety threats.

According to Leveson (2011a, p. 55), new digital technology increases the complexity of the systems and introduces new potential causal factors. In complex systems, accidents occur on account of the interaction of perfectly functioning components. In practice, when one is designing an innovative multi-technology solution, there are no failure data or user experiences available, or data are very limited, to certain specific applications. According to Sammarco (2005a, p. 698) and Leveson (2011a, p. 59), current accident models and safety-engineering techniques do not cover all of the new technological and operational aspects. This implies that proactive analysis and control of system hazards is growing increasingly important. Leveson (2011a) also states that hazard analyses, which have long been used in industries that use dangerous processes and for other hazardous systems, can identify the causes of accidents that have never occurred before. In unique, new technology systems, analysis should begin with identification of all potential hazardous events and situations and then involve assessment of whether they are possible or not. If the consequences are very serious (e.g., fatal), the hazards in question should be eliminated even if it is not possible to determine their likelihood.

1.3 The research gap

In the mobile-machine manufacturing industry, there has been increasing need to understand system-level safety elements and to learn to identify, analyse, assess, and control safety risks in complex mobile work-machine systems. Development from single automated machines to autonomous machine fleets has brought questions of how to specify system-level safety requirements for these unique machinery applications and how to manage system-safety issues throughout the life cycle of the machinery applications under development. On the other hand, there is still lack of practical methods of verifying and validating complex safety-related applications, system-level functions, and on-board machine-safety solutions. Traditional machine-safety solutions, safety standards, and risk-management practices are said to be not enough in the design and development of automated mobile work-machine systems. According to mobile-machine manufacturers and system suppliers, machinery system development is based on traditional machine-design practices and is divided sharply into the main engineering domains: mechanical, hydraulic, electrical, electronic control system, and automation design. System-level safety issues are identified and discussed only as automation-related issues affecting machinery applications.

Research on product- and machinery-safety issues and into issues associated with risk assessment have been conducted over the years in the scientific community considering machinery safety – by, among others, Reunanen (1993), Kui-

vanen (1995), Kivistö-Rahnasto (2000), Malm et al. (2001, 2011), Fadier and De la Garza (2007), Rausand and Utne (2009), Lundteigen et al. (2009), and Hietikko et al. (2010, 2011). Research has concentrated mainly on single manual machines, industrial robot applications, or industrial machines in general. Effects of programmable electronics, digital communication, and software-based safety functions on safety design in machinery applications have been studied and discussed by Alanen et al. (2004), Leveson (2004, 1995), Hedberg et al. (2006), Rausand and Utne (2009), Alanen (2010), Malm et al. (2011), Hietikko et al. (2013), and others. A large amount of research has been carried out and published on automation technology and its implementation in mobile machinery applications. Only a few studies of safety or risk-assessment issues related to automated mobile work-machine systems have been published in the last 15 years. These include research by Pukkila (1999), Paques et al. (1999), Sammarco et al. (2001), Sammarco (2002), Alanen et al. (2004), and Tiusanen et al. (2008, 2013a and 2013b). International standards for mobile work machines have been developed for manual machines; among these are ISO 20474-1 (2008) and its machine-specific parts 2–14. The international standardisation work on safety of autonomous mobile work machines is ongoing, and it has been forecast within ISO that the first draft work addressing this issue should be ready for comments in late 2014.

Research on system-level risk-management issues and aspects of system safety has been conducted in the scientific system-safety community in the defence, aviation, space, and process-industry fields. Guidelines for system-safety engineering and results of case studies have been published over the years by, among others, Roland and Moriarty (1990), Toola (1992), Leveson (1995, 2004, 2011b, 2012), Stephans (2004), and Vincoli (2006). Systems-engineering practices and processes that include risk-management and safety-engineering guidelines have been developed over the years in the international system-safety community and published by, for example, the US Department of Defence (DoD DAU, 2001), US Federal Aviation Administration (FAA ATO, 2006), NASA (NASA, 2007), and International Council on Systems Engineering (SE Handbook, 2011).

Safety-engineering practices in industrial applications have been subject to strong standardisation in the last decade. In the machinery-safety sector, basic guidelines are introduced in SFS EN ISO 12100 (2010). Guidelines for occupational health and safety performance and industrial safety engineering are described in BS 18004 (2008), and functional safety engineering guidelines and requirements are described in the widely referenced SFS-EN 61508 (2011) series of standards. At the same time, systems-engineering guidelines have been standardised by the ISO and IEC to support wider implementation of the systems-engineering approach. Some of the main standards in this domain are ISO IEC 15288 (2008), ISO IEC 26702 (2007), and ISO IEC 16085 (2006).

Regardless of the extensive international standardisation efforts, there are not yet safety-engineering or risk-assessment guidelines specific to overall complex automated mobile work-machine systems. There is still increasing need for knowledge and practical methodology for specifying system-safety requirements for new, unique automated mobile work-machine systems.

The research gaps from the safety-engineering perspective are the lack of knowledge and experience of a system-safety approach and practical risk assessment methodology applicable for automated mobile work-machine systems, and the lack of knowledge and experience of the integration of the system safety methods into the general systems-engineering approach in automated mobile work-machine system applications.

1.4 The scope and objectives of the study

This study belongs to the field of risk management for industrial machinery applications, and the study's context is automated mobile work-machine systems. The scope of the study is system-level operations and functions of the machinery systems, especially automation-related safety risks. Safety risks are examined in limited scope in this study, with the focus being on harm caused by automation-related mechanical hazards. Other occupational health and safety risks caused by the machinery or work-site environment, such as noise, dust, vibration, and exhaust emissions, are excluded from study here.

The objectives of this study are a practical approach for system-level safety-risk assessment in automated mobile work-machine systems and qualitative information on the usefulness of the approach and selected methods.

This study covers risk-assessment issues and activities in the early phases of the system life cycle – hazard identification, risk estimation, system safety requirements' specification, and verification in a functional level. The study focuses on evaluation of the usefulness of the risk-assessment approach and current risk-analysis and risk-estimation methods.

1.5 Limitations of the study

The issues related to detailed requirement specification, safety design along with verification and validation of safety-related functions and technical safety solutions are not in the scope of the study. The study examines and discusses automated mobile work-machine systems from the machine manufacturer's and systems supplier's perspective, with a focus on technology-independent system-level elements. The technology implementations and solutions of the machinery, control systems, communication systems, and other automation-related infrastructure on the site are discussed only when specifically relevant to the safety-related elements and risks under study. The analysis results in case studies are limited to number of hazards or deviations, examples of identified hazardous events, risk estimation results, number of proposals for actions, and examples of principles of specified safety solutions. This is because of the confidentiality of the case study material requested by companies involved in this research.

1.6 Contributions of the study

The research focuses on methods and techniques for obtaining the necessary information and reasoning for risk assessment and risk-reduction decision-making. The aim of this study is to provide new information on how the risk-analysis methods in current use should be utilised for reaching the system-safety objectives and to increase the quality and effectiveness of safety-engineering work. In the long run, the research is aimed at improving risk-management processes and practices among mobile work-machine manufacturers and in the sectors of industry that utilise automated mobile work-machine systems.

The study contributes to the scientific machinery-safety, functional-safety, and system-safety communities by developing and examining system-safety practices and risk-assessment methodology in the context of automated mobile work-machine systems. Its contribution to the machinery-safety research community is the system-level approach to widening the traditional machinery risk-assessment procedure introduced in SFS EN ISO 12100 (2010) with the practices and methods introduced in the system-safety and general occupational health and safety domains. To the functional safety research community, it contributes an approach and methods for the hazard- and risk-analysis phases of the safety life cycle described in SFS EN 61508-1 (2011) to support system-safety requirement specification for new, unique machine automation applications. Its contribution to the system-safety research community is in information and experiences surrounding the applicability of the system-safety approach and methods in a different sector of industry – the mobile work-machine industry and applications. In practice, these contributions involve the following:

- Review and study of current machinery-safety engineering practices, industrial safety engineering practices, and functional safety engineering practices, along with discussion of their applicability for the risk assessment of complex machinery-automation applications
- Study of system-safety practices developed for large-scale safety-critical systems, for a reference for the system-safety approach and methods applied, in complex socio-technical systems
- Study of the systems-engineering approach and process and of the link to system-level safety-risk-management activities throughout the life cycle
- Construction of a practical risk-assessment approach and risk-analysis methodology for automated mobile work-machine systems
- Evaluation of the usefulness of the risk-assessment approach and risk-analysis methodology in four automated mobile work-machine systems
- Discussion of the results in relation to the current safety-engineering guidelines and the latest results of system-safety research.

1.7 The structure of the thesis

To help the reader follow the thesis, a brief summary of its structure and content is provided here. This chapter has described the background for the study, the research interest inspiring the study, and the research problem, along with introduction to the scope and objectives and the expected contribution of the work. Chapter 2 introduces some key terms and definitions that serve as cornerstones of the study. It also contributes by reviewing current safety-engineering practices and by briefly introducing the systems-engineering approach. Chapter 3 describes the two research approaches utilised in this study: the constructive research approach, aimed to construct of a new risk-assessment approach for automated mobile work-machine systems, and the case-study research approach, applied to analyse and evaluate the implementations of the new approach and selected risk-assessment methods. Chapter 4 describes the results of the constructive research work by introducing the main characteristics of the new risk-assessment approach in its current form. Chapters 5, 6, 7 and 8 introduce the four selected case projects in which the new risk-assessment approach has been implemented and evaluated. After the case studies' results are thus presented, analysed, and discussed case by case. The findings of the case study research are discussed in Chapter 9, and Chapter 10 presents an evaluation of the overall study. Finally, the conclusions of the study are summarised in Chapter 11.

2. Framework of the study

2.1 Risk and risk assessment

The concept of risk is complex and the term 'risk' has various definitions, depending on the context in which the term is used (Rausand 2011, p. 47). In literature the word "risk" is used in many different senses and many kinds of risk are discussed: business risk, social risk, economic risk, safety risk, investment risk, military risk, political risk, etc. The different points of view related to the concept of risk, risk perception, quantification of risk, risk analysis and risk assessment are discussed widely in literature among others in Kaplan & Garrick (1981), Lewis (1990), Kuivanen (1995), Kaplan (1997), Renn (1998), Hollnagel (2008) and Rausand (2011). Renn (1998, p. 51) expresses that there is no commonly accepted definition for the term risk, however, all risk concepts have one element in common – the distinction between reality and possibility. Kaplan & Garrick (1981, p. 13) simplifies the idea of risk analysis to be an answer to the following three questions: What can happen?, How likely is it that that happen?, and If it does happen, what are the consequences?

The general risk-assessment vocabulary in ISO Guide 73 (2009, p. 1) defines risk in general terms by stating that it is an effect of uncertainty on objectives, where that effect can be a positive or negative deviation from the expected. The objectives might be, for example, financial, health and safety, or environmental goals, and they can be at various levels, from strategic to product level. According to the ISO Guide 73 (2009, p. 2), risk can be expressed in terms of a combination of the consequences of an event and the associated likelihood of occurrence. Uncertainty under this definition may be related to information on the event, consequences, or likelihood.

From a safety-engineering point of view, ISO IEC Guide 51 (1999, p. 2) defines risk as a combination of the probability of occurrence of harm and the severity of that harm. This definition has been adopted also in the basic machinery-safety standard SFS EN ISO 12100 (2010, p. 3). *In this study, dealing as it does with issues of safety risks in automated mobile work-machinery systems, the latter definition of risk (a safety-oriented one at base) is taken as a cornerstone for the research and development work.*

According to ISO Guide 73 (2009, p. 5), risk assessment is an overall process of risk identification, risk analysis, and risk evaluation. The risk-assessment standard ISO 31000 (2009, pp. 17–20) describes the general risk-assessment process and its phases in detail. Figure 3 illustrates the general risk-assessment process and its connections to the overall risk-management process described in ISO 31000 (ibid., p. 14). The latter risk-assessment standard describes a wide variety of general risk-assessment tools and techniques, categorises them, and evaluates their applicability for risks' identification, analysis, and evaluation. This description of the risk-assessment process is similar to the description in the machinery-safety standard SFS EN ISO 12100 (2010, p. 10), which sets forth risk-assessment and risk-reduction guidelines for machinery design. Instead of risk identification and risk handling, that standard uses the terms 'hazard identification' and 'risk reduction', on account of its safety-oriented perspective. *Another cornerstone for the research and development work in this study is that safety-oriented description of the process.*

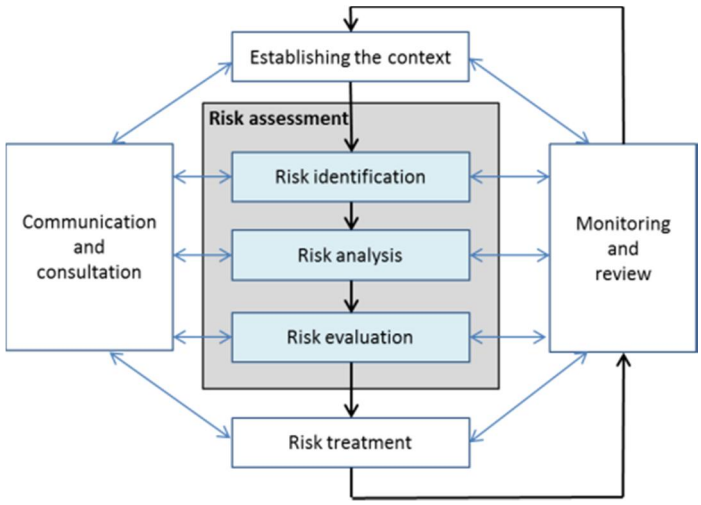


Figure 3. The general risk-assessment process as part of the overall risk-management process, according to ISO 31000 (2009, p. 14).

2.2 Safety and safety engineering practices

The term 'safety' too has various definitions, which depend on the context in which it is used. Leveson (1995, p. 181) has expressed the definition in the form: 'Safety is freedom from accidents and loss', while MIL-STD-882D (2000, p. 2) defines safety as freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or harm to the environment. ISO IEC Guide 51 (1999) describes the concept of safety by stating that there can be no absolute safety: some risk always remains (residual risk). A product, process, or service can only be relatively safe. Safety is achieved by reducing risk to

a tolerable level. Under this concept of safety, tolerable risk is assessed via a search for optimal balance among the ideal of absolute safety; the demands to be met by the relevant product, process, or service; and factors such as benefits, fitness for purpose, and cost-effectiveness (ibid., p. 3).

The basic machinery-safety standard SFS EN ISO 12100 (2010) does not define safety. It describes the aim of the risk assessment and risk reduction as being to eliminate hazards as far as possible and to reduce risks sufficiently through implementation of protective measures (ibid., p. 9). *In this study,* designed to construct a practical risk-assessment approach and examine risk-assessment methods in automated mobile work-machine systems, *safety is understood as an absence of accidents involving unacceptable effects mainly on persons but also on equipment or on property.*

Safety-engineering practices for purposes of this study are the approaches and normative guidelines developed to support the designers, manufacturers, or end users in development and maintaining of safety in industrial applications. The risk-assessment process is one of the key elements in safety-engineering practices. Safety-engineering practices have been developed in light of needs and interest in various sectors of industry (Leveson 2003, p. 1). Between diverse domains such as manufacturing, the process industry, the nuclear power sector, civil aviation, the space industry, and defence-sector engineering, efforts aimed at reaching safety differ considerably. At least four general approaches and practices for safety engineering can be cited: *industrial safety engineering, system-safety engineering, machinery-safety engineering, and functional safety engineering.*

The field of safety engineering and safety evaluation is strongly regulated and standardised for sector-specific needs. To get a general view of the current normative framework in the field of safety engineering guidelines in different domains two figures have been composed. Figure 4 gives an overview of the development of the essential machinery safety directives and standards, and functional safety standards. Figure 5 gives an overview of the development of the essential systems engineering, general risk management, system safety, and RAMS (Reliability, Availability, Maintainability and Safety) management standards.

2.3 Machinery-safety engineering

The latest international machinery-safety standards, published mainly since 2000, have been chosen as the baseline for this review. Current methodology for machinery-safety design, hazard identification, and risk assessment are studied through review of the Machinery Directive (Directive 2006/42/EC, 2006), which has been transposed into Finnish legislation as a government decree (VNa 400/2008, 2008), and the latest internationally ratified ISO machinery-safety and control-system-safety standards: SFS EN ISO 12100 (2010), ISO TR 14121-2 (2007), and SFS EN ISO 13849-1 (2007). Added to that issues related to electrical safety, control circuits and safety functions in machinery are covered in IEC 60204-1 (2000).

2.3.1 The Machine Directive

In Europe, machinery safety is regulated and harmonised by the Machinery Directive to ensure the establishment and functioning of the internal market and to ensure a high level of protection of people's health and safety and of the environment (Directive 2006/42/EC, 2006). The Machinery Directive states that the manufacturer must carry out a risk assessment for the machinery that it plans to place on the market. The Machinery Directive applies not only to individual standalone machines but also for machinery systems, where the latter are defined as 'assemblies of machinery' (ibid., p. 4).

Large installations can usually be divided into sections, which may each be considered assemblies of machinery (Fraser 2009, p. 33). According to the Directive 2006/42/EC (2006, p. 4), a company that places on the market or puts into service an assembly of machinery is considered to be the manufacturer of that assembly of machinery and is responsible for ensuring that said assembly as a whole complies with the essential health and safety requirements of the Directive. This is because the safety of machinery systems depends on the safety of the machine units and also on the suitability of the machine units, their control systems, and the interfaces between them and the assembly as a whole. Fraser (2009, p. 34) states that the risk assessment must address both the suitability of the machine units for the safety of the assembly as a whole and the hazards resulting from the interfaces between units of the assembly.

According to the Machinery Directive, the manufacturer or an authorised representative thereof should first determine the limits of the machinery, which include the intended use and any reasonably foreseeable misuse of the machinery (Directive 2006/42/EC, 2006, p. 13). According to the risk assessment results the manufacturer must select the most appropriate methods and apply the following principles, in this order: eliminate or reduce risks as far as possible, take the necessary protective measures in relation to risks that cannot be eliminated, and inform users of the residual risks due to any shortcomings of the protective measures applied (Directive 2006/42/EC, 2006, p. 13). The Directive sets out the essential health and safety requirements that machines placed on the Community market must fulfil and the procedures for assessing their conformity. These fundamental requirements include special mandates arising from the mobility of the machines but not requirements for automatically operating mobile machinery.

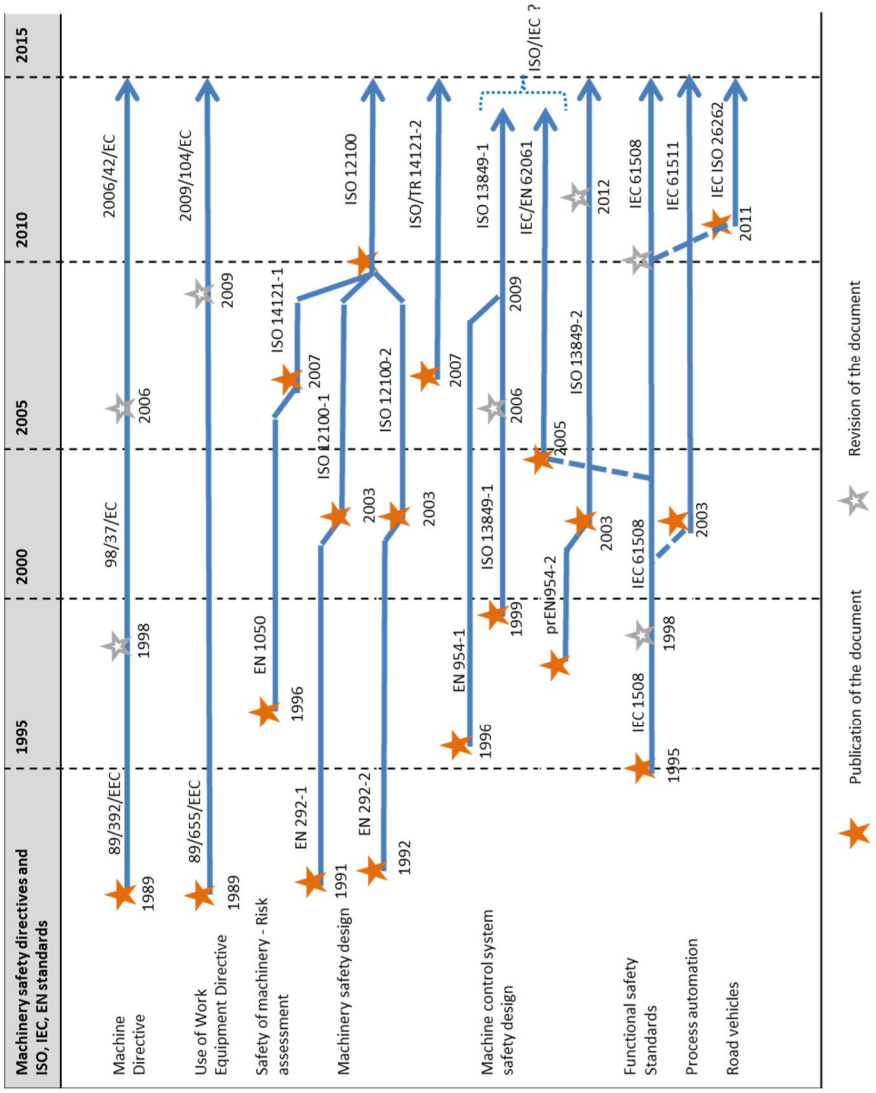


Figure 4. An overview of the development of the machinery safety directives and the essential machinery and functional safety standards.

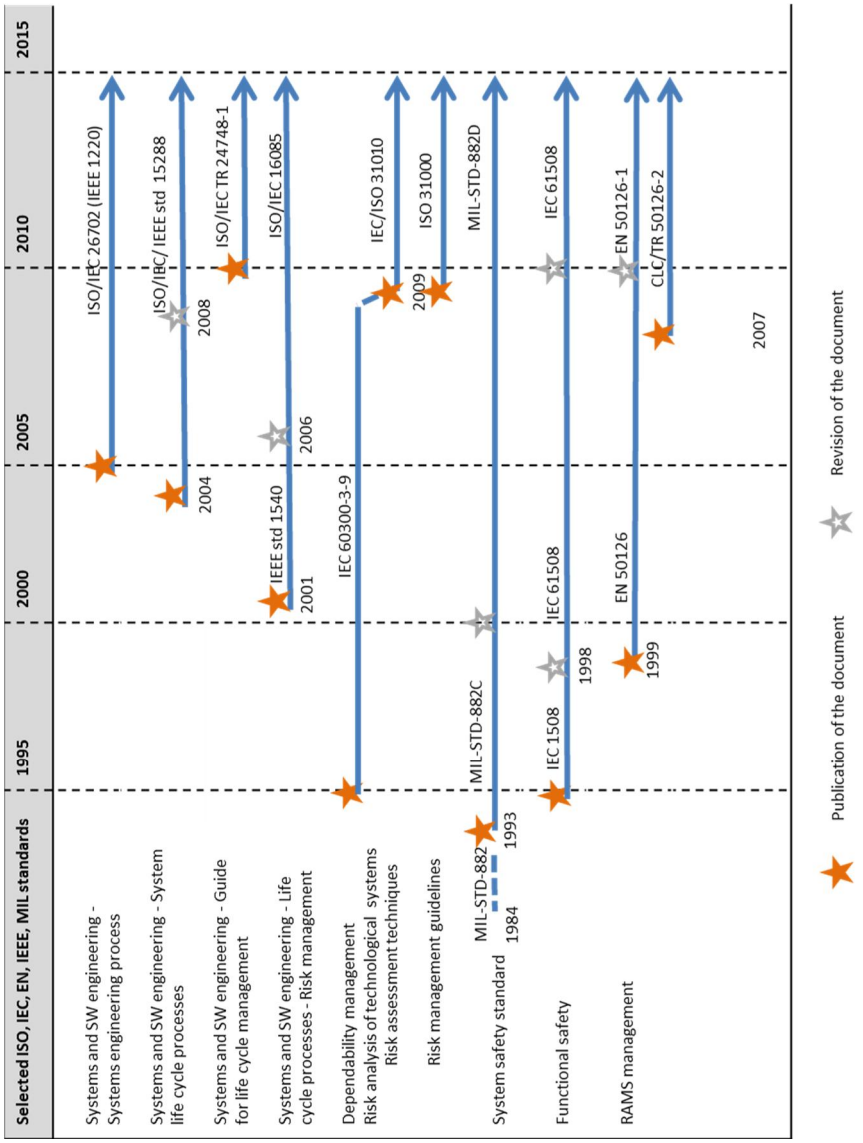


Figure 5. An overview of the development of the systems engineering, risk assessment, system safety, functional safety, and RAMS management standards.

2.3.2 Risk-assessment procedure in machinery-safety standards

Machinery-safety guidelines are developed mainly to help the machine-manufacturing industry build safe manual standalone machines. The standard SFS EN ISO 12100 (2010) introduces risk-assessment and risk-reduction processes for machine manufacturers and system designers. Risk assessment is described as a series of logical steps to enable analysis and evaluation of the risks associated with machinery. It is followed by risk reduction. Iteration of this process may be necessary for minimisation of hazards or at least to reduce risks adequately via the implementation of protective measures (see Figure 6). The objective of risk assessment is the best practicable risk reduction. The risk-assessment process is iterative, and several applications of it might be necessary for reducing the risk and making the best use of the available technology. In carrying out this process, it is necessary to take into account the following four factors, in decreasing order of priority (ibid., p. 9):

- The safety of the machine over all phases in its life cycle
- The ability of the machine to perform its function
- Usability of the machine
- The manufacturing, operation, and dismantling costs of the machine.

Hazard identification in this approach involves systematic identification of reasonably foreseeable hazards (constant hazards and hazards that can appear unexpectedly), hazardous situations, and/or hazardous events in all phases of the machine life cycle. *Risk estimation* is carried out for each hazard via determining of two factors: severity of harm and the probability of occurrence of that harm. The probability factor is presented as a function of three parameters: people's exposure to the hazard, the probability of occurrence of a hazardous event, and the technical and human possibilities for avoiding or limiting the harm (ibid., p. 17).

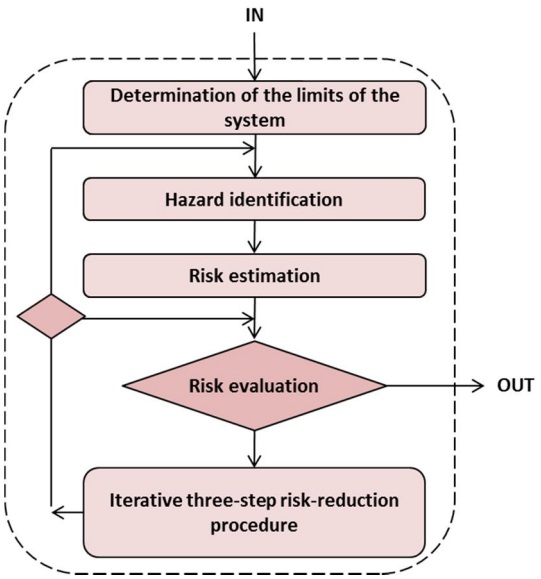


Figure 6. The risk-assessment and risk-reduction model from SFS EN ISO 12100 (2010, p. 10), modified and simplified.

After risk estimation, *risk evaluation* is carried out to determine whether risk-reduction measures are required. The adequacy of the risk reduction shall be determined after each step in the risk reduction until sufficient reduction in risk has been achieved. Risk reduction in this approach is described as a three-step process. The three steps in risk reduction are inherently safe design measures, safeguarding and/or complementary protective measures, and information for use (ibid., pp. 21–22). This approach also includes guidelines for the consideration of protective measures implemented by the end user such as safe work procedures, use of personal protective equipment, and training (ibid., p. 11).

ISO TR 14121-2 (2007, pp. 4–5) introduces two types of hazard-identification approaches for machine design: a checklist-based top-down approach, which starts with potential consequences and examines the possible causes, and a bottom-up approach, which identifies all possible hazards, causes, and consequences. Both SFS EN ISO 12100 (2010) and ISO TR 14121-2 (2007) can be applied for complicated machinery applications, but they do not primarily offer support for system-level hazard identification and risk estimation for complex automated machinery applications. The ISO TR document (ibid., pp. 6–10) presents several methods for risk estimation: a risk matrix, a risk graph, numerical scoring, quantified risk estimation, and so called hybrid methods.

Hybrid methods combine two of the methods mentioned above. In practice hybrid methods are risk graphs that contain within them either matrices or scoring systems for one of the elements of risk. A certain amount of quantification could also be included in qualitative approaches. For example, something that is “likely”

can be expressed as being once a year, and a “high” exposure can be specified as being hourly. An example of a hybrid method that proposes four categories for the severity factor and five classes for the probability is introduced in the report. (Ibid., pp. 23–27, 88–99.)

Risk reduction based on machine-control-system functions has had important implications for the machinery-safety engineering approach. Specific guidelines have been developed to support specification of requirements for safety-related control functions in machinery applications. The standard SFS EN ISO 13849-1 (2007) provides guidance on principles for design and integration of safety-related parts of machine-control systems, including the design of software. The standard specifies characteristics, including performance level (PL), that are required in the design of safety functions. This standard (2007) gives an overview of a control-system-specific approach to risk assessment and reduction that supplements the risk-assessment process described above from SFS EN ISO 12100 (2010) (see Figure 4). The standard can be applied to safety-related parts of control systems for all kinds of machinery, regardless of the type of technology and energy used. It also states specific requirements for programmable electronic systems.

A safety-engineering model and supporting tools based on the main machinery-safety standards especially for machine-control-system safety design have been developed and evaluated by Hietikko et al. (2009, 2010). Risk-estimation methods (matrices and graphs) applied for machine-control-system safety engineering has been studied through comparison of assessment results from several groups who analysed the same case system. Significant divergence between case studies was detected in the risk parameters and risk levels affecting safety-requirement specification for particular functions (Hietikko et al. 2011, p. 773).

International standards for mobile work machines have been developed mainly for manual machines. Standards addressing mobile work-machine safety issues provide guidance for machine designers and manufacturers by introducing hazard lists and requirements for risk-reduction measures. However, these machine-level standards do not describe the risk-assessment process but refer to the general risk-assessment standard, SFS EN ISO 12100 (2010). For example, for earth-moving machinery, the ISO 20474-1–ISO 20474-14 family of safety standards has been developed for the main machine types associated with mechanised earth-moving work. The first standard in the set (ISO 20474-1:2008) covers general hazards and safety requirements, and the others complement these by addressing machine-type-specific issues. Examples of other mobile work-machine safety standards can be named: forest-machinery standard ISO 11850 (2011) and crane standard ISO TR 19961 (2010). Standardisation work for safety of autonomous mobile work machines has begun in ISO technical committee 127. A new work item, ISO 17757 Earthmoving Machinery – Autonomous Machine Safety, aimed at setting requirements for autonomous work machines and giving general safety guidelines for machines running without operators, is under development. It has been forecast that this is going to be ready for comments in September 2014.

2.4 Industrial safety engineering

Traditional occupational safety and health work in industry focuses on improving the safety, health, and welfare of people at work. The work aimed at improving existing work sites and workplaces and at investigating individual past accidents is called industrial safety engineering by, among others, Leveson (2003, pp. 7–8). The legislation pertaining to work-environment safety requirements in Europe is based on Directive 89/391/EEC (1989) (Directive 89/391/EEC, 1989), called the Occupational Safety and Health Framework Directive, which sets the general objectives for occupational safety and health work in the workplace and imposes obligations for both employer and employees. It introduces general principles for the assessment of risks, the reduction of risks, and prevention of risks. The employer is responsible for the safety of work equipment in the workplace. When obtaining machinery systems, the employer has various responsibilities related to the minimum safety and health requirements in workers' use of work equipment at work (Directive 2009/104/EC, 2009). In Finnish legislation, these requirements are found in VNa 403/2008 (2008). According to the directive, the employer should attend to the work conditions and characteristics specific to the workplace and to the hazards that exist there. If it is not possible to eliminate the risks, the employer should take appropriate measures to minimise them (Directive 2009/104/EC 2009, p. 6).

One internationally well-known guide for management of occupational health and safety at work is BS 18004 (2008), which gives companies and other organisations guidance in how to build occupational health and safety management elements for their overall management system to manage their occupational health and safety risks and improve their occupational health and safety performance (ibid., p. 1). The purpose of the risk-assessment process in occupational health and safety management is to understand the hazards that might arise in the course of the organisation's activities and ensure that the risks to people that arise from these hazards are assessed, prioritised, and brought to an acceptable level. As the guidelines emphasise, it is quite obvious that there is no single method of hazard identification and risk assessment that can suit all organisations.

BS 18004 (ibid., p. 75) defines risk as the combination of the likelihood of occurrence of a hazardous event or exposure and the severity of injury or ill heath that can be caused by that event or exposure. Risk assessment is a process of evaluation of the risks arising from the hazards, taking into account the adequacy of any existing controls, and deciding on whether the level of risk is acceptable. The standard (ibid., pp. 77–78) introduces some risk-assessment tools and methods, and it points out that in many cases occupational health and safety risks can be addressed via simple methods and the assessment can be qualitative. Methods such as checklists and questionnaires, risk matrices, ranking and voting tables, failure mode and effect analysis (FMEA), hazard and operability (HAZOP) studies, and computer modelling are cited as examples of applicable methods.

According to the standard, an acceptable risk is a risk that has been reduced to a level that can be tolerated by the organisation with regard to its legal obligations

and policies (ibid., p. 76). The evaluation of risks' acceptability can be based, for example, on a five-band structure reflecting use of the 'as low as reasonably practicable' (ALARP) principle (IEC ISO 31010:2009, pp. 16, 86). The risk categories can be used in relation to various risk-reduction measures or several time scales for actions that must be applied for the relevant risk category (BS 18004:2008, p. 84). In general, the risk-assessment process described in BS 18004 seems to be well in line with the general risk-assessment process described in ISO 31000 (2009).

2.5 Functional safety engineering

Since programmable electronic control systems have become common in industry, new methods and standards have been developed for the management of functional safety issues and risks related to complex system functions in dangerous processes and machinery systems. The functional safety approach has been established to ensure safety of automation in various fields of industry. In general, the term 'functional' in the context of machinery systems can be defined at referring to the system being able to fulfil its intended purpose and functions in a correct and safe manner (Sundquist 2013, pp. 1–2). In general, the functional safety engineering approach is aimed at ensuring safety by eliminating the risks, reducing them to an acceptable level, or rendering them as low as is reasonably practical for reaching a tolerable risk level. These terms are discussed later in Section 2.5.2. The first edition of the international functional safety standard for Functional Safety of Electrical / Electronic / Programmable Electronic Safety-related Systems was published in mid-1990 as IEC 1508. The latest edition, consisting of seven parts, was published in Finland in 2011 (SFS EN 61508, 2011). The latter family of functional safety standards was developed for application in all sectors of industry wherein safety-critical systems are used. The standard SFS EN 61508-4 (2010, p. 21) introduces a general definition for functional safety: it is part of overall safety related to the Equipment Under Control (EUC) scheme and the control system of the equipment that depends on the correct functioning of electrical / electronic / programmable electronic (E/E/PE) safety-related systems and other risk-reduction measures. An overview of the development history of the essential functional safety standards is shown in Figure 4 in page 28.

The SFS EN 61508-1 standard (2011) introduces and specifies a generic approach to safety engineering that covers all activities in the safety life cycle of systems utilising E/E/PE components to perform safety functions (see Figure 7). Although functional safety is a perspective aimed at ensuring overall safety of the system, the SFS EN 61508 standards (2011) focus only on that portion of the overall risk reduction that is allocated to the safety-related E/E/PE parts of the control system. Because of this, the objective of the functional safety engineering approach is to identify safety-related subsystems and to specify their functionality and safety integrity requirements and their design principles. The functional safety approach, then, requires specification of the right functionality of the safety-related functions and of their reliability requirements. The level of reliability needed de-

pends on the magnitude of the risk intended for reduction by means of the safety-related control function.

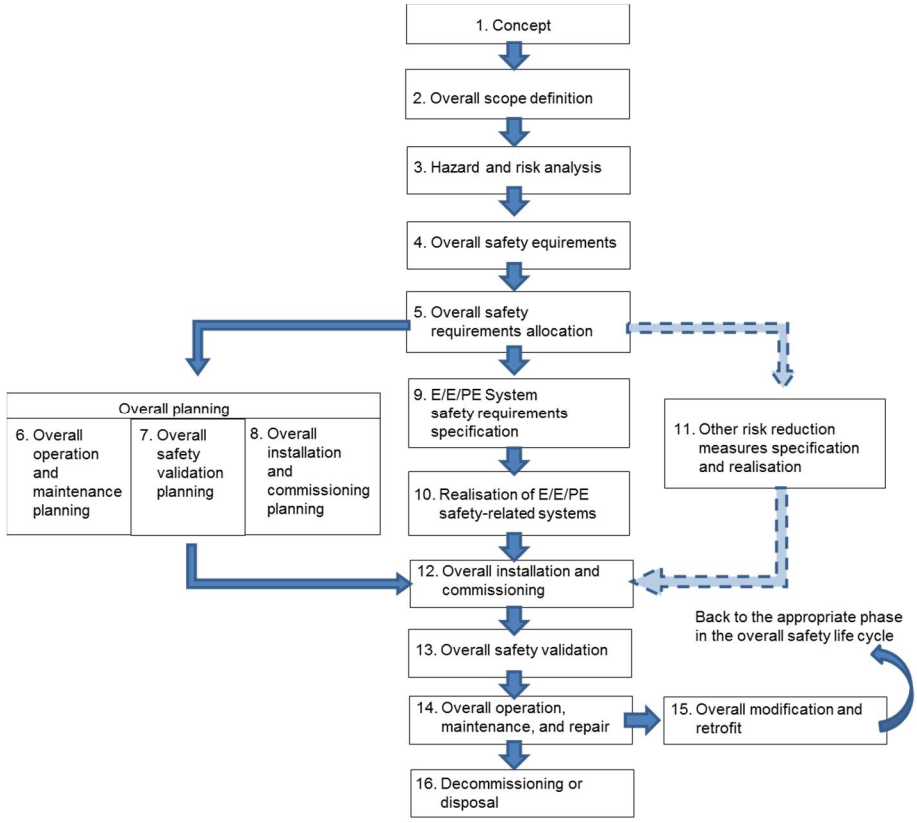


Figure 7. Phases in the safety life cycle, according to SFS EN 61508-1 (2011, p. 35).

2.5.1 Risk assessment and the risk-reduction process

According to the functional safety guidelines, the objectives of the hazard- and risk-analysis task in the overall safety life-cycle approach as stated by SFS EN 61508-1 (2011, p. 41) are to determine the hazards, hazardous events, and hazardous situations related to the equipment under control and its control system in all modes of operation, in all reasonably foreseeable circumstances (including fault conditions and reasonably foreseeable misuse); to determine the sequences of events leading to the hazardous events; and to determine the EUC risks associated with the hazardous events.

The scope of the preliminary hazard and risk analysis is primarily the overall EUC and its environment. Although hazard and risk analysis is introduced as one particular phase in the safety life-cycle model (see Figure 7), it may be necessary

to conduct more than one hazard and risk analysis during the parts of the overall safety life cycle devoted to requirement specifications. If decisions taken in later parts of the safety life cycle change the basis for the earlier decisions, a further hazard and risk analysis should be carried out (ibid., p. 53).

The first part of the SFS EN 61508 (2011) set of standards describes the outline of the hazard- and risk-analysis procedure and refers to the fifth part (SFS EN 61508-5, 2011), which introduces examples of methods for determination of safety integrity levels. The fourth part of the set introduces functional safety terminology and definitions (SFS EN 61508-4, 2010). Hazard and risk analysis can be conducted via application of qualitative or quantitative methods and techniques (SFS EN 61508-1:2011, p. 55). A qualitative risk graph or risk matrix can be used for risks' estimation (SFS EN 61508-5:2011, p. 49). The functional safety engineering approach highlights the need to understand the relationship between identified and estimated risk, the necessary risk-reduction measures, and the safety integrity of the safety-related systems and other risk-reduction measures.

Here too, risk in the system under study is regarded as a combination of the probability of occurrence of harm and the severity of that harm (SFS EN 61508-4:2011, p. 19), the same definition found in ISO IEC Guide 51 (1999, p. 2). However, the terminology defined in the functional safety literature causes confusion. While SFS EN 61508-4 (2011, p. 19) introduces a new term 'harmful event', as an occurrence in which a hazardous situation or hazardous event results in harm. This differs from the definition of the latter term given in ISO IEC Guide 51 (1999, p. 2). However both SFS EN 61508-1 (2011) and SFS EN 61508-5 (2011) express in their hazard- and risk-analysis text that a risk in the equipment under control is a combination of a hazardous event and consequences associated with that hazardous event. In this author's understanding, that is not the same thing as a combination of the probability of occurrence of harm and the severity of that harm.

2.5.2 About tolerable and acceptable risk levels

The necessary risk-reduction measures are the combinations of measures to reduce a given risk to a tolerable level for a specific situation (see Figure 8). If a risk cannot be reduced to an acceptable level, the ALARP principle is introduced as one applicable approach for reducing risk as far as is reasonably practicable for reaching a tolerable risk level (ibid., p. 47). The ALARP principle involves a process in which all risk-reduction options are considered in terms of benefits and costs. As the functional safety engineering guidelines are focused on safety-related E/E/PE systems, they do not give guidance in how to specify requirements for any other risk-reduction measures. At the same time, they do not make reference to literature dealing with overall safety-engineering and risk-assessment issues such as industrial safety engineering, machinery-safety engineering, or system-safety engineering work. In fact, SFS EN 61508-1 (2011, pp. 59, 61, 63) states that other technologies are not within the standard's scope and that it is applicable only if at least some of the risk-reduction measures are implemented with the E/E/PE system.

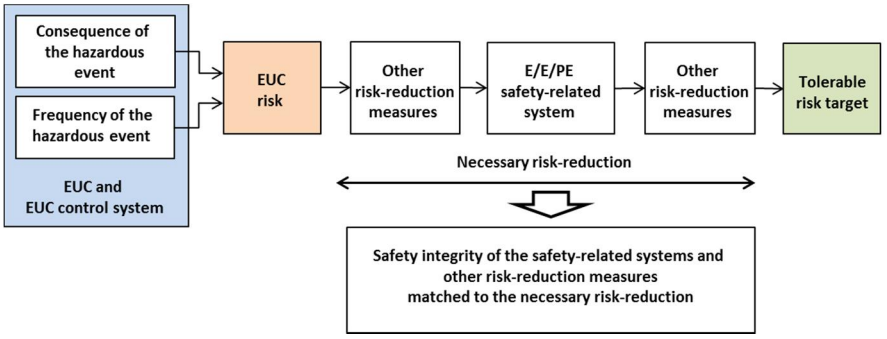


Figure 8. Risk and safety integrity concepts as described in SFS EN 61508-5 (2011, p. 27).

'Tolerable' is different from 'acceptable'. The risk level that is tolerable in a specific situation depends on many factors, such as severity of injury, the number of people exposed, the frequency of exposure, and the duration of the exposure, and it can be specified either qualitatively or quantitatively. Tolerable risk is the risk that is accepted in a given context on the basis of society's current values, according to SFS EN 61508-5 (2011, p. 19), which states: 'Tolerable indicates a willingness to live with a risk so as to secure certain benefits, at the same time expecting it to be kept under review and reduced as and when this can be done' (ibid., p. 47).

In addition to the above mentioned ALARP principle there are several other approaches developped to for determining whether or not the risk related to a system is acceptable. Rausand (2011) discusses the risk acceptance criteria more in depth and introduces three approaches to risk acceptance (ALARA, GAMAB and MEM) (ibid., pp. 106–116).

Safety integrity in the functional safety-engineering approach refers to 'the probability of an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time' (SFS EN 61508-4:2010, p. 35). The standard SFS EN 61508-1 (2011) defines four risk-based safety integrity levels (SILs), with SIL 4 being the highest and SIL 1 the lowest. The safety integrity requirements for a particular SIL are specified in terms of the average probability of dangerous failure of a safety function on demand or in terms of the average frequency of a dangerous failure of a safety function, depending on the role of the safety function in the EUC (low- or high-demand-mode operation) (ibid., p. 65). Safety integrity applies to the E/E/PE safety-related systems and to other technical risk-reduction measures. Once the tolerable risk level has been set and the necessary risk reduction estimated, the safety integrity requirements for the safety-related systems can be assigned. Typically, the allocation process is iterative, for optimisation of the design to meet the various requirements associated with the safety-related functions in the EUC (SFS EN 61508-5:2011, p. 35). Parts 2 and 3 of the SFS EN 61508 family (2011) present a broad range of design principles, safety-engineering techniques and measures, and verification and validation methods for both hardware and software development

that are necessary for reaching the target SIL in the relevant safety-related functions. In addition to the standards theoretical background of the essential methods and tools for quantitative reliability analysis, SIL analysis, reliability assessment of E/E/PE safety-related systems and SIL verification is provided among others by Rausand (2014).

In complex safety-related systems, there is typically need for multiple layers of protection and risk-reduction measures if an acceptable risk level is to be reached or risk reduced to a tolerable level. In such cases, the functional safety engineering approach emphasises use of the 'layers of protection' analysis (LOPA) method (IEC ISO 31010:2009, p. 59). The LOPA method is described as useful in complex systems wherein needs arise for a holistic approach to evaluation of interactions between individual safety layers and between safety layers and causes of demand for risk reduction such as hazards, system functionality, and the operation environment (SFS EN 61508-5:2011, p. 35). LOPA was developed as a tool for SIL allocation. In the functional safety engineering context, the LOPA method provides a basis for the specification of independent protection layers (IPLs) and SILs for safety-related E/E/PE systems. Via analysis of the risk reduction produced by each layer of protection, LOPA can be used to aid in allocation of risk-reduction resources. The layers of protection are characterised in terms of specificity, affectivity, independence, dependability, and auditability (ibid., p. 73).

2.5.3 Application-specific standards for the machinery sector

Several application standards based on the main functional safety standard have been developed for diverse domains employing safety-related software and programmable electronic control systems, such as avionics, medical devices, railways, road vehicles (ISO 26262-2, 2011), and machinery. The machinery-sector application standard SFS EN 62061 (2005) has been created to provide guidelines for the requirement specification, design, and verifications of safety-related control systems in machinery applications. In practice, there have been two approaches for machine control-system-safety design: those of SFS EN ISO 13849-1 (2007), based on the old EN 954-1 (1996), and SFS EN 62061 (2005), which is based on the old IEC 61508 (1998). This divaricate situation has led to confusion as to which standard to apply in specific machinery applications. Some guidance has been published to help designers choose the appropriate guidelines for the application at hand (SFS 5974, 2011). The SFS EN 62061 (2005) standard does not deal with the general risk-assessment process in machinery applications, neither does it give guidance in how the safety-related functions should be identified. It refers to the old ISO 12100-1 (2003), ISO 12100-2 (2003), and ISO 14121 (2007) standards, which have now been superseded by SFS EN ISO 12100 (2010). It states that the safety-related functions will be specified in accordance with the risk-assessment and risk-reduction processes described in those standards.

2.5.4 Application guidelines for the process-industry sector

An application standard for the process industry (IEC 61511-1, 2003) has been established to specify guidelines and practices for functional safety engineering for safety-instrumented systems designed to ensure the safety of an industrial process. There is an important difference between the basic functional safety standard and this application standard. While SFS EN 61508-1 (2011) has been developed for manufacturers and suppliers of safety-related devices, IEC 61511-1:2003 was developed for designers of safety-instrumented systems, integrators of these systems, and the end users (ibid., p. 12).

According to IEC 61511-1 (ibid., p. 41), the objectives of the hazard and risk analysis in process-industry applications include:

- to identify the hazards and hazardous events of the process and associated equipment,
- to estimate the process risks associated with the hazardous event in terms of consequences and likelihood of the event, to determine the sequence of events leading to the hazardous event (in consideration of the various operation modes),
- to determine any requirements for risk reduction, to determine the safety functions required for the necessary risk reduction, and
- to determine whether any of the safety functions are safety-instrumented functions.

IEC 61511-2 (2004) emphasises that in the process industry, a preliminary hazard and risk assessment should be carried out early, in the project's basic process-design phase. At this stage, the objective should be to try to eliminate hazards or reduce the risks as far as is reasonably practicable by applying inherent safety principles and good engineering practice. It is important to start the hazard- and risk-assessment work as early as possible because the assessment results serve as input for system-architecture design and, at the same time, designing and implementing a safety-instrumented system can take a long time. The process-design and system-architecture information is needed before the process and instrumentation diagrams can be finalised (ibid., p. 18). A final hazard and risk assessment should be completed once the process and instrumentation design and diagrams have been completed. The so-called final analysis should use a formal, fully documented procedure such as hazard and operability studies (HAZOP). The objective of the final assessment should be to confirm that the safety layers designed are adequate for guaranteed safety of the process plant (ibid., p 43). To emphasise the importance of distinct safety layers and of both technological risk-reduction measures and the role and actions of human operators, IEC 61511-1 (2003, p. 45) introduces examples of typical risk-reduction methods in the context of a process plant.

2.6 System-safety engineering

The system-safety approach was developed firstly for complex military, aviation, and space-industry systems, and nowadays it is also applied in the process industry. System safety has been defined as a 'sub-discipline of systems engineering that applies scientific, engineering and management principles to ensure adequate safety, the timely identification of hazard risk, and initiation of actions to prevent or control those hazards throughout the life cycle and within the constraints of operational effectiveness, time and cost' (Stephenson 1991; Vincoli 2006, p. 6). System safety is concerned primarily with new systems (Leveson 2003, p. 8) and has the goal of reducing the risk to an acceptable level (Vincoli 2006, p. 6). Vincoli (2006) points out that following safety regulations, standards, and written codes is aimed only at meeting minimum safety requirements. The risk-management work associated with system safety is an attempt to exceed these minimum compliance standards and provide the highest level of safety (the lowest level of acceptable risk) achievable for the target system with acceptable cost implications. It is important to consider direct costs and indirect implications – such as operation restrictions, system performance, operation schedules, and downtime – related to alternative risk-reduction solutions (ibid., p. 8).

The first ideas of system safety evolved as missile systems and space-travel systems were being developed. The old 'trial-and-error' method could not be used anymore. As aircraft and aviation systems grew more complex, the risks of devastating consequences of a failure increased, and the traditional 'fly–fix–fly' approach was no longer acceptable. The possible failures and errors need to be identified in the design phase if one is to be able to design controls to prevent accidents and other unwanted situations. The development of systems engineering in those industries has been the driving force for advances in concepts of system safety (Roland and Moriarty 1983, p. 12; Stephans 2004, p. 4). The US Department of Defence (DoD) formalised system-safety requirements by publishing MIL-STD-882C 'System Safety Program requirements, which became mandatory for system-safety programmes (Roland and Moriarty 1983, p. 12). The MIL-STD-882C has been superseded by MIL-STD-882D (2000). System safety is sometimes considered the same as software safety. Sammarco et al. (2001) attempt to clear up this misunderstanding by stating that system safety involves seeking to design safety into all phases of the entire system. Software is a subsystem, so software safety is part of the system safety.

In complex systems, the human–system interface and, more generally, human–technology interaction issues and design requirements are getting more and more important. It is vital for human factors and aspects of human behaviour to be considered a part of system requirements, with the operation and maintenance strategies and principles designed in view of operators' needs and ability to find out the best possible and safest operation and maintenance solutions. (Vincoli 2006, pp. 39–41)

MIL-STD-882D (2000) does not give any guidance for the selection of risk-analysis methods but does refer to the publications of the System Safety Society

(ibid., p. 24). It is also worth mentioning at this juncture that the system-safety literature does not refer to the widely applied general functional safety standard SFS-EN 61508-1:2011. This is one indication of how differentiated safety-engineering development work has become over the years.

The system life cycle has been described in various textbooks and standards. According to Stephans (2004), the main stages in a system's life cycle are the concept, definition, development, production, and system operation. Roland and Moriarty (1983) state that the three basic system-safety analysis methods are preliminary hazard analysis (PHA), fault hazard analysis (FHA), and fault tree analysis (FTA). These differ fundamentally in their concepts and practical execution (ibid., p. 193). Distinct analyses methods have been developed for certain purposes to support decision-making in certain phases of the system life cycle (see Figure 9). A list of various methods and more detailed descriptions of them can be found in such works as the following: Roland and Moriarty (1983, 1990), Stephenson (1991), Stephans (2004), and Vincoli (2006). The system-safety literature and the standard MIL-STD-882D (2000) introduce a risk-matrix method for the estimation of risks. For example, Vincoli (2006, pp. 13–16) proposes four categories for hazard severity and five categories for the occurrence of harm (mishaps). Risks are classed into four categories, with the following criteria: unacceptable (changes must be made), unacceptable (make changes if possible), acceptable with management review, and acceptable without review.

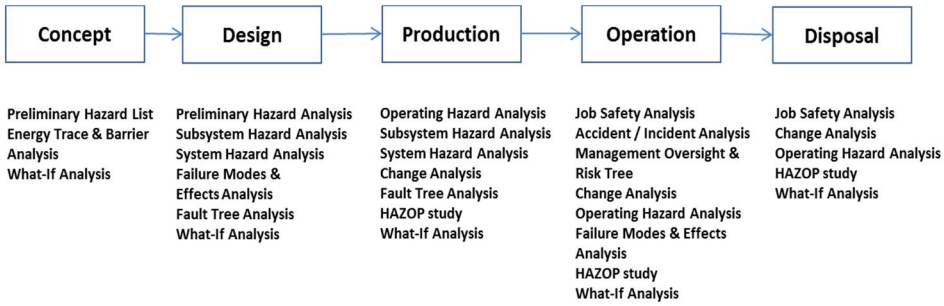


Figure 9. Phases in the life cycle and the primary system-safety tasks for a 'one-of-a-kind' project or product, according to Vincoli (2006, p. 33).

2.7 The systems-engineering approach

This chapter reviews the systems-engineering approach (or 'systems-engineering management') and the systems-engineering process in brief. The aim is to introduce the basic ideas of the systems-engineering approach and identify risk-management activities in the general systems-engineering life-cycle model. The main focus is on how the risk-assessment activities and, more precisely, the safety-engineering activities are described and made part of the general systems-engineering approach.

The systems-engineering discipline is thought to have begun in 1950s amidst the development of the first complex military applications, such as ballistic missile systems. In the 1960s, the Apollo programme brought the systems-engineering approach to non-military applications (Leveson 2011b, p. 69). This gives an idea of the origins of the systems-engineering approach – very large critical systems such as military, space, and aviation applications. This century's literature has produced several, quite similar definitions for systems engineering. System-engineering guidelines from the US Department of Defense (DoD DAU 2001, p. 3) highlight that systems engineering involves two significant disciplines: the technical knowledge domain in which the engineer operates and systems-engineering management. It also states that 'Systems engineering is an interdisciplinary engineering management process that evolves and verifies an integrated, life-cycle balanced set of system solutions that satisfy customer needs'. The FAA as the principal US air-traffic organisation (FAA ATO 2006, p. 5) defines systems engineering as follows: 'Systems engineering is a discipline that concentrates on the design and application of the whole (system) as distinct from the parts. It involves looking at a problem in its entirety, taking into account all the facets and all the variables and relating the social to the technical aspects'.

International systems-engineering standards are quite new. All of them have been published in this century: ISO IEC 15288 (2008) introduces and specifies various system life-cycle processes, such as agreement processes, organisational project-enabling processes, project processes, and technical processes); ISO IEC 26702 (2007) specifies and gives guidelines for the applications and management of the systems-engineering process; and ISO IEC 12207 (2008) introduces a common framework for software life-cycle processes. Because of the varied and partly overlapping process descriptions for the life cycle, the technical report ISO IEC TR 24748-1 2010 has been published to give guidance in the joint usage of the process content of ISO IEC 15288 (2008) and ISO IEC 12207 (2008) pertaining to life-cycle management of systems and software. The ISO IEC 16085 (2006) standard introduces and describes a process for the management of risk during systems or software acquisition, supply, development, operation, and maintenance. Even though the systems-engineering approach is strongly standardised, Granholm (2013, p. 25) states that its practical implementations differ from one organisation to the next. The systems-engineering approach should be understood as a scalable plan of actions including company-specific applications of life-cycle and systems-engineering processes, decisions on system architecture, and requirement specifications and management.

Systems-engineering management guidelines give guidance on such matters as engineering work processes, use of optimisation, and risk-management methods. According to the SE Handbook (2011, p. 7), systems engineering is based on systems thinking. The systems-engineering approach has a horizontal orientation and includes both technical and management processes. The SE Handbook (2011, p. 8) states also that decisions made in early phases of the system life cycle, when consequences are not understood, can have enormous implications later in the life cycle. Systems-engineering management is said to encompass

elements from technical and human-centred disciplines such as control engineering, industrial engineering, organisational studies, and project management (Leveson 2011b, p. 69; FAA ATO 2006, p. 11; DoD DAU 2001, pp. 3–5). Granholm (2013, p. 23) sums up the main characteristics of systems engineering, listing them as systematic and extensive requirement specifications and management, systematic verification of design solutions and validation of implementations, and breaking down of system design problems into manageable sub-problems. According to the DoD (DAU 2001, pp. 4–5), systems-engineering management is characterised by the following three viewpoints:

- Phasing of the development to control the design process, to provide baselines for the design co-ordination, and to provide an interface for the acquisition management
- A systems-engineering process providing a procedure for design problem-solving and tracking of requirements through the development phase
- Integration of the system life cycle's activities into the development process, to ensure that the solutions remain viable throughout their life.

2.7.1 System and life-cycle modelling

Among the basic concepts in the systems-engineering approach are the model of a system and the model of a system life cycle. These two models describe the system's hierarchical architecture, related products and processes, and how various stakeholders are related to various phases in the life cycle. In the systems-engineering standards, 'system' is defined as 'a combination of interacting elements organized to achieve one or more stated purposes' (ISO IEC 15288:2008, p. 6). Alternatively, a system is 'a set or arrangement of elements [people, products (hardware and software) and processes (facilities, equipment, material, and procedures)] that are related, and whose behaviour satisfies operational needs and provides for the life cycle sustainment of the products' (ISO IEC 26702:2007, p. 9). Under these definitions, the system model is introduced and described as representing the hierarchy and interactions among system elements, products, and processes. Such models are presented in, among other places, SE Handbook (2011), ISO IEC 15288 (2008), and ISO IEC 26702 (2007) (see Figure 10).

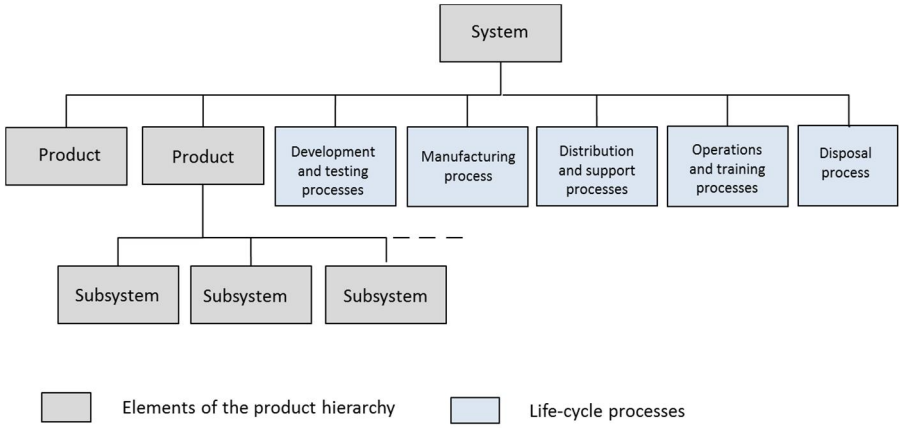


Figure 10. System elements and life-cycle processes, according to ISO IEC 26702 (2007, p. 4).

System life-cycle models and the phases in the life cycle are specified in several systems-engineering references as described in SE Handbook (2011, p. 26). According to ISO IEC TR 24748 (2010, p. 13), the system life cycle's phases are concept, development, production, utilisation, support, and retirement. The ISO IEC 26702 (2007, p. 20) combines these into two main phases – development and operation – and then specifies separately the system-definition phase and the subsystem-definition phase. The latter phase includes the various stages of design and the fabrication, assembly, integration, and testing (see Figure 11).

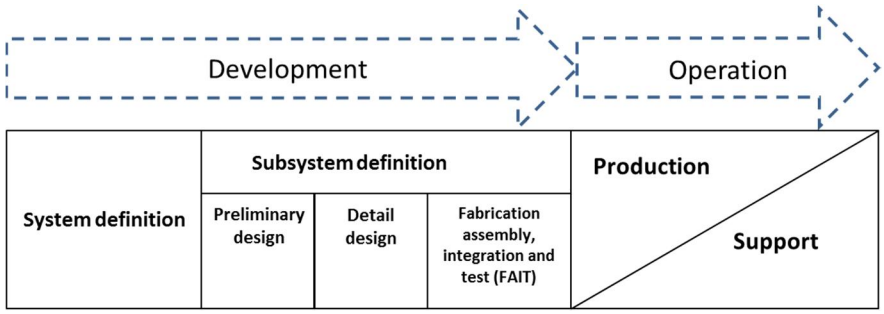


Figure 11. A system life-cycle model adapted from ISO IEC 26702 (2007).

Various system development models are described in the systems-engineering literature, including waterfall, spiral, V, and agile development models. V-models are commonly used to visualise the top-down system development procedure from the overall system level down to the detailed subsystem and component levels. For example, SE handbook (2011) uses a simplified three-level model for system hierarchy in their V-model (see Figure 12) (SE Handbook 2011, p. 27).

The V-model highlights the importance of integration, verification, and validation, along with opportunity- and risk-management activities in the systems-engineering approach. The left side of the 'V' represents the top-down procedure for definition, breaking down, and specification of the system as subsystems and low-level components to be designed and produced. The bottom of the 'V' represents the construction and procurement of the components and subsystems, and the right side illustrates the bottom-up procedure for integration of the subsystems into the overall system and validation against the specified requirements (DoD DAU 2001, p. 65; SE Handbook 2011, pp. 27–32). In the systems-engineering approach, it is important to draw a distinction between verification and validation activities. Verification refers to the activities that compare a system or system element with the required characteristics, while validation activities are intended to ensure that the system can accomplish its intended use, goals, and objectives (i.e., meet stakeholder requirements) in the intended operation environment (ISO IEC 15288:2008, p. 7).

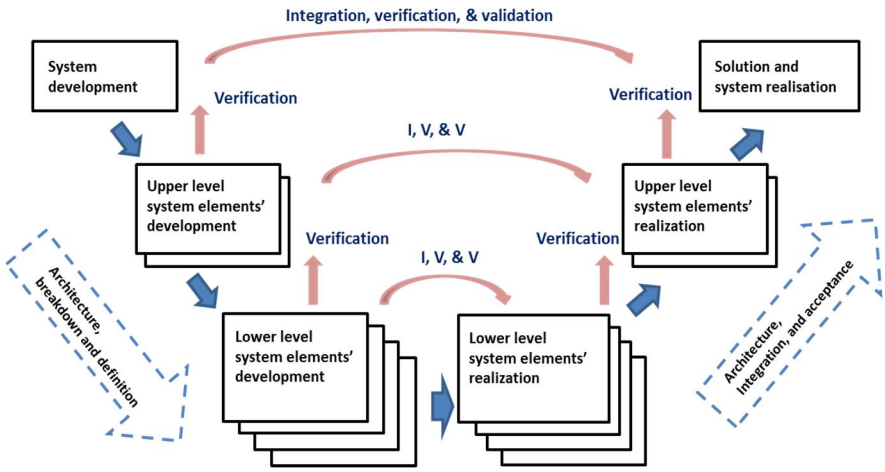


Figure 12. A simplified system development V-model, modified from SE Handbook 2011 (p. 27).

2.7.2 The systems-engineering process

The systems-engineering process is an essential element of systems-engineering management. According to the DoD's DAU (2001, pp. 5–6), this process is an iterative and recursive problem-solving process to be applied sequentially throughout all stages of development. The aim of the systems-engineering process is to transform needs and requirements into a set of system descriptions, to generate information for decision-makers, and to provide input for the next level of development. The main activities in the process are requirements' analysis, functional analysis and allocation, and design synthesis (see Figure 13).

ISO IEC 26702 (2007) specifies the systems-engineering process and describes its application in each stage in the life cycle and to all activities associated with product development, verification/testing, manufacturing, training, operation, support, distribution, disposal, and human–systems engineering. Systems-engineering control loops and control activities are used to track decisions and requirements, to maintain technical baselines, to manage interfaces, to control risks, to trace costs and adherence to schedules, to track technical performance, and to verify that requirements are met (DoD DAU 2001, p. 6).

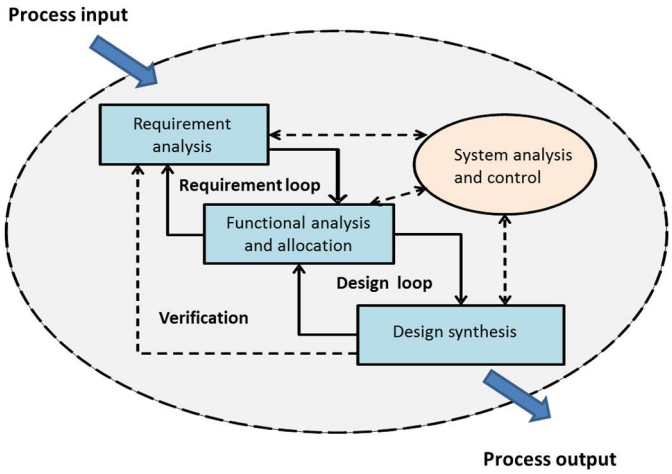


Figure 13. A simplified flowchart of the systems-engineering problem-solving process, according to the DoD's DAU (2001, p. 31).

2.7.3 Risk assessment and safety engineering

From a systems-engineering management perspective, the risk-management process is a continuous process to identify, analyse, treat, and monitor risks related to the acquisition, development, maintenance, or operation of a system (ISO IEC 15288:2008, p. 30). The general risk-assessment process is described in ISO IEC 15288 (2008) and specified in more detail in the specific risk-assessment process standard ISO IEC 16085 (2006). The integration of risk-management activities into the systems-engineering process application in each phase in the system life cycle is described in ISO IEC 26702 (2007). In the systems-engineering approach, risk management covers both project risk-management and product risk-management issues. Figure 14 summarises general risk-management activities and synthesises them with the V-model concept and the system-development and operation phases.

The standard procedure for systems-engineering process application described in ISO IEC 26702 (2007) includes safety-engineering activities, which are systematically integrated into each phase of the process and system-analysis efforts (see Figure 12). In the requirement-analysis phase, the safety-engineering objective is

to identify significant risks of death, injury, or illness of personnel who operate, maintain, or support the system. In the requirement validation, the system-analysis results, including risk-analysis results, are compared with established acceptable risk levels. In the functional analysis phase, operational hazards that could result in personal injury, property or product damage, or environmental impact are identified. In the synthesis phase, the alternative design solutions for the functional elements are analysed and assessed, for identification of potential hazards to the system; to those who operate, service, or support it; or to the environment. Finally, in the design-verification phase, the low-level design solutions are checked against the verified functional architecture and the validated requirement baseline.

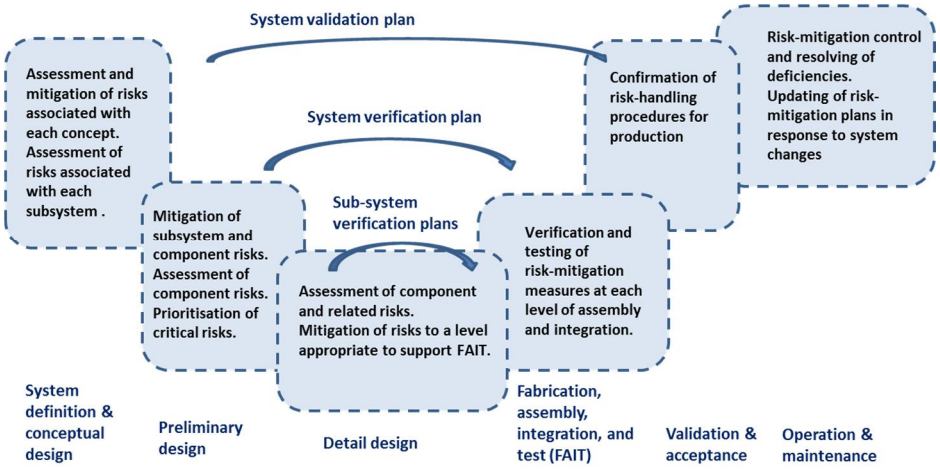


Figure 14. General risk-assessment activities related to the system's development and operation phases, modified from ISO IEC 26702 (2007) and ISO IEC 16085 (2006).

The general purpose of systems-analysis efforts is to resolve conflicts identified in systems-engineering tasks, to manage risks throughout the systems-engineering efforts, and to support the overall process so as to end up with balanced requirements and design solutions (ISO IEC 26702:2007, p. 57). From a safety-engineering standpoint, this means, among other elements, analysis of safety and environmental impacts of alternative system products and the final system implementation, assessment of risk levels as part of the life-cycle cost analyses and environment impact analyses, and assessment of risk-handling and risk-mitigation options to quantify costs and effects on the probability and impact of risks. In the end, the system-analysis efforts should support the risks' evaluation and selection of risk-handling options, for revealing of feasible solutions that bring risks to an acceptable level with the best possible cost–benefit ratio (ibid., p. 61).

3. Research approaches, methods and materials

This chapter describes the two research approaches utilised in this study: the constructive research approach, aimed to construct of a new risk-assessment approach for automated mobile work-machine systems, and the case-study research approach, applied to analyse and evaluate the implementations of the new approach and selected risk-assessment methods.

3.1 The constructive research approach

The research and development of the risk-assessment approach followed a constructive research approach. This approach, which is typical in technical sciences and for design sciences in general, is aimed at the construction of models, diagrams, plans, methods, and organisations. Constructive research resembles problem-solving in a design project (Olkkonen 1993, p. 76). According to Oyegoke (2011, pp. 578–579), constructive research can be characterised as applied studies aimed at uncovering new knowledge in the form of normative solutions. Constructive research is differentiated from scientific problem-solving in that the usability of the research results is demonstrated in the former approach through the implementation of solutions.

The goal in constructive research is to create innovative and a theory-justified solution that is applicable for practical situations and solving the practical problem at hand. The solution is based partly on existing knowledge and partly on an innovative, heuristic research process (Rohweder 2008, p. 11). According to Olkkonen (1993), the innovation phase is often heuristic in nature and is the core element of successful constructive research. Given the innovative, problem-solving nature of constructive research, the solutions must be demonstrated and verified in practical implementations (ibid., p. 76). The research and development process in constructive research is typically long and includes continuously obtaining and assessing the latest information. Demonstration of the solution, for evidence that it works, requires intensive dialogue between theory and practice, along with use of researcher interventions as a research method (Hyötyläinen 2005, pp. 34–35). The interaction between theoretical reasoning and practical demonstration connects features of action research to constructive research. Sometimes the latter is akin to action research aimed at changing

the target organisation rather than creating a new construction or procedure. Both approaches, action research and constructive research, require deep understanding of the problem under study in order to carry the research results forth into practice (Rohweder 2008, p. 11).

Constructive research typically proceeds from an existing problem, after which the research proceeds step by step, developing the method or construction to solve the problem and evaluating the results. According to Kasanen et al. (1991), development of the construction is the key issue of research and development in constructive research. Constructive research is characterised by division of the research process into phases, which may vary with the context (ibid., p. 306; Kasanen et al. 1993):

- Finding and specifying a practically relevant problem whose solution has research potential
- Studying the topic and obtaining a general understanding of it
- Innovating and constructing a solution idea
- Demonstrating that the solution works
- Showing the theoretical connections and the research contribution of the solution concept
- Examining the scope of usefulness of the solution.

The constructive research approach has long been studied and applied in management accounting research (Kasanen et al. 1991, 1993; Olkkonen 1993; Lukka 2000). In recent years, the approach has been applied in, for example, the context of complex information system development and implementation (Hyötyläinen 2005; Lammi 2007), the development of pedagogy for education in sustainable development (Rohweder 2008), and project-management research (Oyegoke 2011).

In the field of safety research, applications of the constructive research approach include the development and evaluation of process automation and machinery-safety engineering practices. Toola (1992) developed risk-analysis methodology for the conceptual design phase of safety-critical process-control systems. Reunanen (1993) constructed and evaluated a systematic safety-design process and methodology for machine design. Also, Kivistö-Rahnasto (2000) studied the integration of European machinery-safety-legislation-based risk-assessment and conformity assessment methodologies into the machine-design process.

3.2 The construction of the risk-assessment approach

The author's work to construct the approach and methodology for system-level hazard identification and risk assessment in automated mobile work-machine systems was based on knowledge of machinery-safety and machine-control-system safety-design methodology, international safety requirements, standards, and regulations. Author's knowledge of these topics has increased and been updated over the years as part of research and development activities within VTT's

research team. The author's research work on the risk-assessment approach was carried out in two stretches, in 2000–2002 and 2003–2008, in several research projects in VTT. The theoretical basis for the approach including system theory, system modelling, the system-safety approach to safety engineering, and safety-related factors in complex human–technology interaction was studied and integrated into the risk-assessment approach. The risk-assessment approach and selected risk analysis methods have been applied in several industrial projects in Finland, in Sweden and in South Africa in 2000–2013. Experiences of risk-analysis work and feedback on the usefulness of the approach and methodology have been received from industrial partners and utilised for the development of the approach. Four of these industrial projects have been selected for case studies in this thesis.

The research and development work in this study has been conducted in line with the phases specified for the constructive research approach (Kasanen et al. 1993; Kasanen et al. 1991, p. 306). This research work proceeded with the following tasks (see Figure 15):

- Problem definition and specification of the research strategy
- Specification of the system-safety approach requirements, method selection, and development of the first version of the approach and analysis methods
- Implementation and testing of the first version of the approach and analysis methods in two industrial projects
- Development of the second version of the approach and analysis methods on the basis of the research results and the available literature
- Implementation and testing of the second version of the approach and analysis methods in industrial projects
- Development and outlining of the current version of the approach
- Examination of the case project results and evaluation of the usefulness of the risk assessment approach and analysis methods.

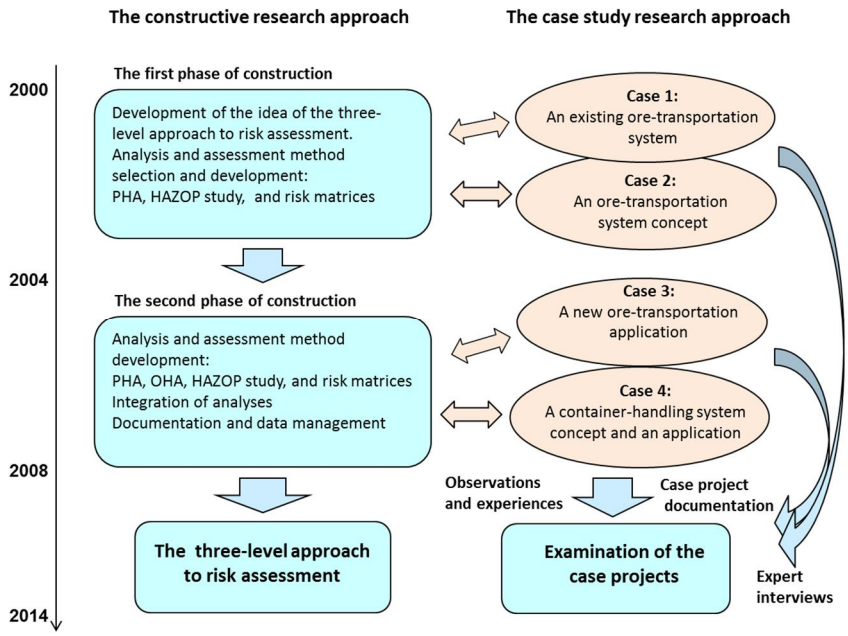


Figure 15. An overview of the research approaches and the research phases in the thesis.

3.2.1 The first phase of construction

The baseline for this research and development work comes from author's experience of machinery-safety design and evaluation work that had been carried out at VTT in the 1990s. One major milestone in European machinery-safety legislation came in 1995, when the Machinery Directive (Directive 89/392/EEC) came into force. The basic machinery-safety standards, including EN 292 in 1995 and EN 1050 in 1997, were published and harmonised throughout Europe. International guidelines for the implementation and development of risk-analysis methodology were obtained from SFS-IEC 60300-3-9, released in 2000. Traditional risk-analysis methods such as checklist-based PHA and FMEA for machine-control-system analysis had been used successfully in risk analysis for individual industrial machines, robot cells, and manufacturing systems at VTT (Reunanen 1993; Kuivanen 1995; Kivistö-Rahnasto 2000). Hazards related to the use of mobile work machines had been examined via job-safety analysis (JSA) by the author (Tiusanen 2000).

The original impulse for the risk-analysis methodology's development to the author of this thesis was the industry's need to analyse and evaluate the safety of automated mining-machine systems. Need for development of systematic methodology to analyse failures and possible deviations in control functions in complex

control systems led to the adoption of a HAZOP method for automated mobile machine applications and to studies of its usefulness (Tiusanen 1999). The HAZOP standard (IEC 61882, 2001) and experiences and guidelines in the literature (e.g., Redmill et al. 1999) provided a good basis for this intention. The first version of the risk-assessment approach was compiled utilising PHA and HAZOP methods (Tiusanen 2000). The PHA was selected on the basis of the system safety literature (Roland and Moriarty 1983; Stephenson 1991), and previous research results and experiences of machinery and automation risk analysis in VTT (Toola 1992; Reunanen 1993; Kuivanen 1995).

Preliminary hazard analysis (PHA) is an inductive analysis method. Its objective is to identify and categorise hazards, hazardous situations and hazardous events that can cause harm to persons, facilities and systems. For machinery applications the check lists provided in SFS EN ISO 12100 (2010) gives a good baseline for the identification hazards, hazardous situations and hazardous events. PHA is commonly conducted early in the system life cycle, when there is little information available and forms the framework for other risk analyses, that may be performed. The output of the PHA is then used for the development of system safety requirements. PHA can also be used when analysing existing systems for initiation of a safety evaluation or for prioritising risks for further analyses. Identification and analysis of hazards is typically followed by qualitative risk estimation. (IEC ISO 31010:2009, pp. 31–32; Roland and Moriarty 1983, pp. 195–200; Leveson 1995, pp. 295–300; Vincoli 2006, pp. 65–83)

Hazard and operability study (HAZOP) is a structured and systematic examination of a planned or existing product, process, procedure or system. The objective of a HAZOP study is to identify risks to people, equipment, environment and organisational objectives. HAZOP technique was originally developed for the analysis of chemical process systems, but its usage has nowadays extended to other industrial branches and various systems. (IEC ISO 31010:2009, pp. 32.) A HAZOP study is a detailed problem identification process, carried out by an expert team. HAZOP study focuses on the identification of potential deviations from the design intent, examination of their possible causes and assessment of their consequences (IEC 61882:2001, p. 13). Redmill et al. (1999) declare that HAZOP technique can be employed at all stages in a system's life cycle and be applied to operational systems just as well as system designs. HAZOP is a structured team-work-based technique that is effective for analysing new systems and novel technologies and particularly powerful for exploring interactions between parts of a system. HAZOP study starts with a specified deviation from the design intent and analysis work directs both backwards to explore its possible causes and forwards to examine its consequence (ibid., pp. 24–25)

The idea of assessing risks at several system levels in such applications was adopted from the system safety literature and international standards in that time such as Roland and Moriarty (1983), Stephenson (1991), EN 50126-1 (1999) and MIL-STD-882D (2000). *The ground and concept for the risk assessment in three levels was based mainly on the following reasoning:*

- The need to identify new system level risks and unexperienced threats in highly automated mobile work machine applications.
- The system architecture and main elements of an automated mobile work machine system, which include subsystems in three hierarchy levels, communication systems, on-board automation systems and machinery in the production area (see Figure 2).
- Understanding of the general systems engineering approach and system life cycle phases.
- Understanding of the different objectives and the purpose of use of risk assessment activities through system life cycle phases.
- Understanding of the needs to identify and assess different risks in different system levels and system development phases utilising different analysis methods.
- Understanding of the top-down approach in risk assessment process and decision to assess risks in three levels: *overall system level risks, operational risks* during system operation and maintenance, and *functional risks* related to system functions or machine control functions.

The three-level approach was concretised in industrial projects. In 2000–2001, VTT carried out two large-scale risk-assessment projects in the mining industry. These were the first automated mobile work-machine system risk-assessment projects so were selected as cases for evaluation of the first development version of the three-level risk-assessment approach (Case-studies 3 and 4). The author of this thesis was the project manager in both case projects and also led most of the risk-analysis sessions and documented most of the analysis results. The author's contribution to the case projects is described in case-study descriptions in Chapters 5 and 6. Also, the author's comments and experiences related to the case projects are included in the observation results in each case study.

3.2.2 The second phase of construction

The author's work to develop the three-level risk-assessment approach and the risk-analysis methods for automated mobile work-machine systems continued with the results, feedback, and experiences from the first two industrial implementations taken into consideration. The development of the essential machinery safety, functional safety and systems engineering standards was followed (see Figures 4 and 5), as well as the relevant system safety literature. In practice, the work continued in two research projects and in several assignments in the mining-industry sector in 2003–2008. A research project was conducted in 2003–2005 in which the analysis method for the examination of operational risks in automated mobile machinery applications was studied and developed by Tiusanen et al. (2005). The method was an application of the operating hazard analysis (OHA). The overall

approach was further developed in a research project in 2005–2007 (Tiusanen et al. 2008). The author of this thesis was the project manager and the key researcher in the research projects.

Operating hazard analysis (OHA), sometimes called operating and support hazard analysis (OSHA) is used to analyse hazards associated with the operation and maintenance of the system. It considers especially hazards resulting from tasks, activities, or operating system functions as the system is operated or maintained in its intended operating environment. The approach in OHA is similar to PHA to identify hazards, but the categorising function in the analysis is an operational event. The analysis focuses on human factors, procedures and human-machine interfaces, not only on technical failures or human errors. In complex systems complicated operational events or simultaneous activities can lead to hazardous events. According to the system safety literature OHA should be initially carried out as early in the life cycle as possible as soon as the necessary information is available and updated periodically throughout the life cycle. (Roland and Moriarty 1983, pp. 209–210; Vincoli 2006, pp. 93–97; Stephenson 1991, p. 78–79.)

To support the management of the large amount of analysis data involved, a database-based technique for data collection and reporting in HAZOP studies was developed by Pátkai (2006) in her Master of Science thesis. These two research projects were followed by a large risk-assessment assignment related to automated mobile work machines in cargo-handling work at container terminals. Two of VTT's industrial projects from 2003–2008 were selected for case studies in this thesis to represent the second phase in development of the three-level approach and risk-analysis methods. The cases (Case-studies 3 and 4) represent different branches of industry, different companies, and different machinery-automation applications. The author of this thesis was the project manager in both case projects and also led most of the risk-analysis sessions and documented most of the analysis results. The author's contribution to the case projects is described in case-study descriptions in Chapters 7 and 8. Also, the author's comments and experiences related to the case projects are included in the observation results in each case study.

The research on the three-level risk-assessment approach and, specifically, on the new supporting methods and techniques has continued since 2011 in a research project that is part of the Finnish Metals and Engineering Competence Cluster's (FIMECC) EFFIMA programme work (FIMA 2011; FIMECC 2012). The focus in the research has been on the use of a simulator-assisted design approach utilising 3D models and work-site-level simulator environments in automated mobile work-machine systems. The simulator-assisted safety-engineering approach and the first results of its implementation have been presented by Tiusanen et al. (2013a).

3.3 The case-study research approach

In this study the case-study research is applied to analyse the implementation and evaluate the usefulness of the three-level risk-assessment approach and selected risk-assessment methods in this context. The examination of the selected cases in this study employs a qualitative case-study research approach.

Case studies typically have an important role in theory-building as part of constructive research. Eisenhardt (1989) has emphasised that the novelty, testability, and empirical validity of case studies derives from the link to empirical evidence. Eisenhardt (1989, p. 548) also argued that, because of its independence from prior literature or past empirical observation, case-study research is particularly well suited to new research areas for which existing theories seem inadequate. The aim in case-study research is to examine, describe, and explain phenomena mainly by asking 'How?' and 'Why?' (Yin 2009, p. 10). According to Yin (2009), case-study research is preferred for examination of contemporary events. The case-study approach relies on the same techniques as history research but adds direct observation of the events being studied and interviews with people involved in the events. Case-study research is used especially in attempts to understand a real-life phenomenon in depth. It is important to understand contextual conditions, because they are a substantial element of the real-world phenomena under study (ibid., p. 18). According to Saaranen-Kauppinen and Puusniekka (2006, p. 42), it is essential that the case study forms a coherent entity. Many projects, studies in constructive research, and investigative studies can be considered case studies.

This case-study research in this study applies so called multiple-case design (Yin 2009, p. 46). Altogether four case-projects are studied, and each of them includs several risk-assessment activities. Even though the systematic examination of four case-projects required a lot of time and effort, the use of multiple-case design instead of single-case design has the following reasoning in this thesis:

- The cases are associated with the construction and development of the three-level risk-assessment approach and they are related to different phases of the construction of the approach.
- Cases 1 and 2 are examined to evaluate the usefulness of the three-level risk-assessment approach and the usefulness of the PHA and HAZOP methods and risk-estimation methods utilised in the first construction phase.
- Cases 3 and 4 are examined to evaluate the usefulness of the approach and the PHA, OHA and HAZOP methods and risk-estimation methods utilised in the second construction phase.
- The use of multiple cases extends the scope of the use of the approach and methods and increases the amount of findings. The cases are related to different life cycle phases of an automated mobile work machine system. The cases have different viewpoints and objectives for risk assessment and risk evaluation.

- The cases represent different machinery applications and automation technologies (underground ore transportation and container handling in a port terminal) and thus extend the scope of the evidence and amount of the findings.
- Each case has different project teams even though the machine manufacturer in Cases 1, 2 and 3 is the same. Experiences and comments are received from a large number of industrial experts and researchers.

3.3.1 The case projects in this study

Case 1 was a risk-analysis and safety-evaluation assignment from mining company LKAB. The target system was an existing semi-automatic mobile work-machine system in an underground mine in Kiruna, Sweden. The mining company's interest lay in evaluating the safety of the automation system with reference to European machinery-safety requirements. The target system was composed of rubber-tyred mining machines that load, haul, and dump ore in the underground mine: multi-function 'load–haul–dump', or LHD, machines. The work for this assignment was conducted in 2000–2001 in Sweden and partly in Finland. The project is examined in this thesis to evaluate the usefulness of the first version of the three-level risk-assessment approach and the PHA and HAZOP methods in a real-world complex automated mining-machine application.

Case 2 was a risk-assessment and conceptual safety design assignment from the mining-machine manufacturer Sandvik. This assignment was related to the conceptual design of an automated ore-transportation system (the AutoMine™ system) at Sandvik Mining and Construction in Finland. The assignment was conducted in 2000–2001 in Finland and partly in Sweden. This project is examined in the thesis to evaluate the usefulness of the first version of the three-level risk-assessment approach and the PHA and HAZOP methods in a complex automated mining-machine application in the early phases of its life cycle.

The target systems in Cases 1 and 2 were applications of LHD machines capable of operating autonomously in horizontal tunnels in an underground mine, but the machinery and automation technology were different. The two case studies were conducted almost in parallel temporally, and there was close interaction between these projects, because the same machine manufacturer and the same research team at VTT were involved. From a system life-cycle perspective, these two cases represent the opposite ends of a system's development phase (Figure 16).

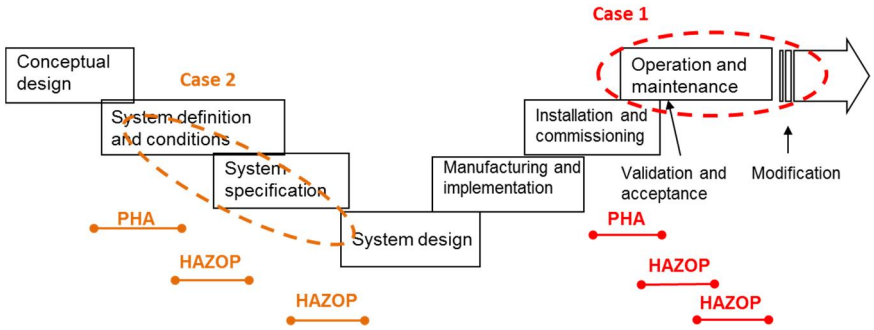


Figure 16. A simplified overview of Case studies 1 and 2 linked to phases in the system life cycle, as modified from Stephans (2004, p. 20).

Case 3 was a risk-assessment and safety-evaluation assignment from Sandvik. The assignment was related to system design for an underground ore-transportation system using automated dump trucks to be implemented in the De Beers Finsch mine in South Africa. The assignment was carried out in Finland and partly in South Africa in 2003–2004. This project is examined in this thesis for evaluation of the usefulness of the second version of the three-level risk-assessment approach and the PHA, OHA, and HAZOP methods in the system-specification and design phases of a complex automated mining-machine application (Figure 17).

Case 4 was a risk-assessment and conceptual safety design assignment from cargo-handling equipment manufacturer Cargotec. The assignment was related to the system-design phase of an automatic crane system to be implemented at a container harbour in Germany. The assignment was conducted in 2006–2008 in Finland. The project is examined in this thesis to evaluate the usefulness of the second version of the three-level risk-assessment approach in relation to the systems-engineering approach. In this case study, the usefulness of PHA, of OHA, and of HAZOP methods are examined in a complex automated cargo-handling application in the early phases of its life cycle (Figure 17).

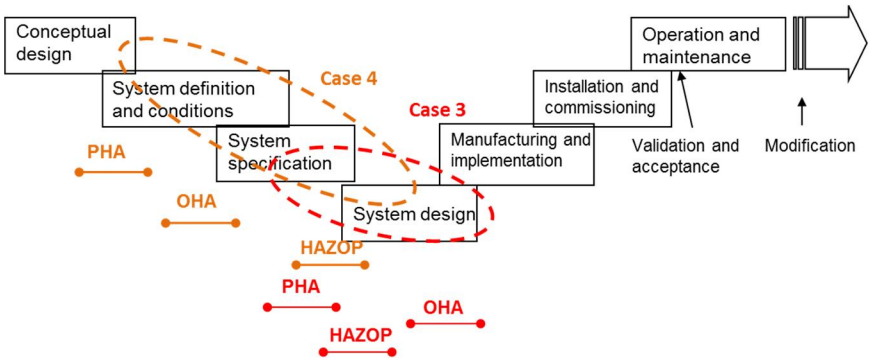


Figure 17. A simplified overview of Case studies 3 and 4 linked to phases in the system life cycle as modified from Stephans (2004, p. 20).

3.3.2 The case-study material

The use of multiple sources of information is important for ensuring high-quality data collection in qualitative research. In this study the case-study material is based mainly on case-project documentation, researchers' observations and industrial expert interviews. The material is supplemented with publicly available information about the case projects and target systems.

Patton (1999, p. 1192) states that no single method can ever adequately address the problem of rival explanations and describes the triangulation principle for data collection. Triangulation (a term that comes from the well-known land-surveying method) is based on the assumption that each method of data collection reveals different aspects of empirical reality. Use of multiple methods of data collection and analysis helps to situate the results and adds value to the research. According to Patton (ibid., p. 1193), combinations of interviews, observation, and document analysis are typically expected in fieldwork. The intention in use of multiple methods of data collection should not be just to demonstrate that different data sources yield the same results. Different data sources may give slightly different results because different types of data-collection methods are sensitive to different influences in the real-world environment.

Emphasising the use of multiple source of evidence, Yin (2009, p. 102) introduces the six sources of evidence most commonly used in case studies: documentation, archival records, interviews, direct observations, participant observation, and physical artefacts. According to Yin (ibid., pp. 101–113), documentation as a source of evidence may include, for example, memoranda, minutes of meetings, analysis reports, and progress reports. Archival records could include, for example, files in public use, statistical data, organisational records, and maps. Interviews are considered to be among the most important sources of case-study information. These can take the form of in-depth interviews, focused interviews, or a formal survey. Direct observations can range from formal to casual data-collection tasks: they can include observation of factory work, observation of meetings, and observations made throughout a field visit and discussions with employees on a work site.

In this study the available project documents cover among others the following information:

- Descriptions of the machinery system under study: its operating environment, operating principles, an overall system hierarchy scheme, the main units of the system and their connections.
- Descriptions of the risk-analysis methods used, persons involved, supporting tools, and work methods utilised in the analysis sessions.
- Risk analysis and risk estimation results, descriptions of the proposed safety measures and other relevant workshop and project meeting results.

Documented project information and the risk assessment results are supplemented with the results from expert interviews and the author's experiences. In addition to all this information, publicly available information on the case projects and the systems under study is searched and examined. Expert interviews were conducted in the case-study companies and at VTT in 2012 for amendment of the project materials and the evaluation of the impacts of the safety-engineering work done in the assignments. The interviewees at the companies were selected so as to represent the experience of the assignments under study, knowledge of safety engineering in the company, and the knowledge of the development of safety- and risk-analysis methods. The interviewees at VTT were researchers who had participated in the development of the three-level risk-assessment approach and the risk-analysis methods and also in the case projects. All interviews were carried out as semi-structured themed interviews.

Three people at the mining-machine manufacturing company were interviewed. One of them participated in Case projects 1 and 2, a man who had been working at the company on the development of the automated mining-machine concept and its technologies since late 1990. One interviewee had over a decade's experience in the development of the mine-automation technologies and system design, especially where ore-transportation applications such as that in Case project 3 were involved. The third interviewee had extensive experience in underground and surface mining-machine research and development and their safety engineering. There were three interviewees at the cargo-handling equipment manufacturing company too. One was among the company's key experts in Case project 4. He had over 30 years' experience in research and development of the machine automation and more than 20 years of experience in mobile cargo-handling equipment technologies. Another interviewee had over a decade's experience in mobile work-machine safety engineering and over five years' experience in mobile cargo-handling equipment technologies at the company. The third interviewee had over five years' experience with cargo-handling equipment technologies and safety standardisation. The following themes were used to guide the interviews in the companies:

- Experiences from the case studies: pros and cons, practical impacts of system-safety thinking at the company, expertise, safety engineering, and impacts on the R&D process
- How the safety objectives were achieved in the case systems
- Problems and challenges in application of safety requirements and conducting of risk assessment for complex machinery applications
- Future needs in safety-engineering research.

Three researchers from VTT were interviewed. Two of the interviewees currently work as senior scientists at VTT's risk- and reliability-management knowledge centre. They both had over 25 years' experience in machinery-safety and machine-control-system-safety research and development work. One interviewee, who currently works as a senior scientist at VTT's systems-engineering knowledge

centre, has over 20 years' experience in machine-control-system design and more than 10 years of experience with development of systems-engineering methodology and system safety-engineering methodology for mobile machinery. The following themes were used to guide the discussions with VTT interviewees:

- Experiences from the case studies: pros and cons, practical impacts on the development of the risk-assessment approach, and analysis methods
- Experiences of the approach development, analysis methods, and management of the analysis information
- Effects of the risk-assessment approach development work at VTT
- Future needs in safety-engineering research.

The author of the thesis has carried out all the document analyses in the individual case studies and conducted all the expert interviews. The interviews were recorded and the material then transcribed by a VTT subcontractor.

3.3.3 The analysis method applied in case studies

The four selected case-projects are analysed to evaluate the *usefulness* of the risk-assessment approach and the usefulness of the risk-analysis and risk-estimation methods. The basis for the analysis and evaluation of the usefulness is applied from the literature. According to Nielsen (1993), the usefulness of a system is connected to the wider scope of system acceptability. Usefulness is part of the practical acceptance of the system. The term 'usefulness' describes whether the 'system' can be used to reach the specified objectives or not. Usefulness of a system can be evaluated through assessment of the system's *usability and utility* (ibid., pp. 24–25). In the context of this thesis, the term 'system' can be replaced with 'method' when one is evaluating the usefulness of the risk-assessment approach and risk-analysis methods. Silius and Tervakari (2003, p. 4) have presented four perspectives for evaluation of the usefulness: ease of use, the quality of information, meeting of the users' needs, and benefits for the users.

Nielsen (1993, p. 25) characterises *utility* such that it answers the question of whether the functionality of the system in principle can do what was expected and needed. Silius and Tervakari (2003, p. 7) and Tervakari (2008, p. 1) have expanded the concept of utility and define it in two dimensions: the added value gained from the system studied and the support the system under study provides for the users' reaching of their goals. Nielsen (1993, p. 25), in turn, characterises *usability* as answering the question of how well users can make use of the functionality of the system. For methods, usability could be covered by definitions such as 'the method is easy to use', 'the method is easy to learn,' and 'the method is efficient to use'.

The objectives for the analysis of the case-study material are defined with the three basic research questions which try to cover the above mentioned aspects and viewpoints of the 'usefulness', 'usability' and 'utility' of the three-level risk-assessment approach and applied methods.

- How well do the selected analysis methods and risk estimation methods suit for the specific risk assessment objectives in the particular case?
- How well does the three-level risk-assessment approach suit for the overall risk assessment objectives in the particular case?
- What are the benefits and impact of the risk-assessment work in the particular cases and more generally in the companies?

In this study the case projects are related to the various phases in development of the three-level risk-assessment approach, and the combinations of methods utilised in these differed. Because of this, research questions are specified separately for each case study, in line with the main research objectives in this study.

The following risk assessment results and documented information, observations and experiences are examined in each case study:

- Hazard-identification and risk-estimation results such as the number of automation related hazards or hazardous events.
- Risk estimation results along with the number and type of proposed safety measures proposed by the analysis team. In Cases 3 and 4 the risk estimation results were documented before and after the proposed safety measures. These results are analysed to evaluate the impact of the risk-assessment efforts to the system design in these cases.
- Analysis-team compositions, time, and manpower used for the analyses. The number of people involved in the analysis, estimation, and evaluation meetings and the quantity of meetings held are analysed to provide understanding of the work effort needed for the specific risk-assessment tasks at hand.
- Documented comments, experiences, improvement proposals and researchers' observations of the methods and work practices in the analysis sessions.
- Documented comments, experiences, improvement proposals and researchers' observations of the documentation and reporting practices.
- Factors affecting the quality of the risk-analysis methods, such as definition and limitation of the objectives, specification of the analysis method, organisation of the analyses, execution of the analyses, and reporting on the analyses (Rouhiainen 1990, p. 43; Heikkilä et al. 2007, pp. 8–9) are also examined.

The risk-analysis and risk-estimation methods are analysed through examination of the *pros and cons of the selected methods and work practices in the projects.* These analysis results are supplemented with the results from expert interviews and the author's experiences and publicly available information on the case projects. These findings are considered to represent the 'usability' aspects.

The usefulness of the three-level risk-assessment approach in automated mobile work-machine systems is examined through *evaluation of possible benefits of the results and impacts of the risk-assessment work* in light of the risk-assessment results achieved in the projects, project documentation, and industrial experts'

comments and experiences. These findings are considered to represent the 'utility' aspects.

The case studies are analysed and reported following the same systematic structure: description of the case and specification of the research questions; description of the risk analysis, risk estimation and risk evaluation methods; risk assessment results; comments and experiences from the companies, researchers' and author's observations; and discussions.

In this study the focus in the case-study analysis was not in the costs of safety engineering efforts or economic impact of the results. Direct or indirect costs of risk-assessment work and costs related to the final safety solutions are not estimated in the case projects. Benefits are considered only from safety point of view and as possible improvements on safety engineering and systems engineering practices. In earlier studies cost–benefit evaluation of risk-assessment efforts in manual work-machine systems and in automatic industrial robot applications have been examined and discussed by, among others, Reunanen (1993) and Kuivanen (1995).

4. The three-level approach to risk assessment

The objectives of this study were a practical approach for system-level safety-risk assessment in automated mobile work-machine systems and qualitative information on the usefulness of the approach and selected methods. Motivating the research and development work on the three-level approach to risk assessment was the shift from manually operated mobile work machines toward automated mobile work-machine systems. This move toward automated mobile work-machine systems extends the perspectives from traditional concrete machine-level safety risks to new potential system-safety risks associated with individual phases in the life cycle of a complex machinery-automation application. There was a need in industry for a practical safety-engineering practice to identify, assess, and evaluate new automation-related safety risks.

4.1 System thinking for safety engineering practices

The result of the risk-assessment application constructed is a simplified system-safety approach utilising selected risk-analysis methods focused on system-level safety issues arising from the shift from individual manual mobile machines to automated machinery systems. The result widens the traditional machinery risk-assessment procedure introduced in SFS EN ISO 12100 (2010) to system-level issues. The new three-level approach to risk assessment integrates and utilises elements from current machinery safety engineering, industrial safety engineering, and system-safety-engineering practices. The three-level approach is based on the system thinking and system-modelling principles adopted from the general systems-engineering approach, such as its phases in the system life cycle; system-development breakdown; and system modelling with a three-level system hierarchy: the overall system level, the upper system level, and the lower system level. The overall system level in this approach covers the work-site-related issues, including the machinery system under study, its operation environment and interfaces to other systems, and activities in the operation environment in the various phases of the system life cycle. Upper system level corresponds to system operations, operation modes, system functions, and human–technology interactions that extend through the entire ma-

chinery application horizontally or vertically. Lower system level corresponds to subsystem-level functions, specific safety systems, and on-board functions, and human–technology interfaces.

The three-level approach to risk assessment applies general practices from the fields of system safety, functional safety, and industrial safety engineering for complex mobile work-machine systems. In light of these practices, results of the constructive research, and case-project experiences, the following principles were chosen for the main characteristics of the new approach to risk assessment:

- The objective of the risk-assessment work is to support the work of the system-development project to reduce the risk to an acceptable level.
- The risk-assessment work starts as the conceptual design begins.
- Risk assessment is a continuous process.
- Risk-assessment objectives and a related execution plan are specified for each system-development phase and each level of the system.
- Different types of risks need to be identified, with different analysis methods, in different stages of system development.
- The risk analysis is based on well-known and widely accepted risk-analysis methods and risk-evaluation principles.
- The main methods of risk analysis for the system-level risk analysis in the approach applied are PHA, OHA, and HAZOP study.
- The three main perspectives – human, technology, and environment – are considered in all risk-assessment activities.

4.2 Risk-assessment activities on three levels

The three-level approach to risk assessment links system-safety tasks to specific phases in system development and levels of system analysis, with certain risk-analysis methods employed. In this approach, system-safety issues and system-level safety risks are grouped into three categories, which are named in accordance with the method of risk analysis applied (see Figure 18).

PHA is for the overall-system-level assessment. The objective at PHA level is the identification and assessment of the major automation-related system risks affecting the overall machinery application. This includes the most significant risks associated with the automated machinery, risks linked to the system's operation environment, and other work-site-level safety constraints. The overall-system-level risk assessment utilises the PHA method for hazard identification and analysis, a risk-matrix method for risk estimation, and specified criteria for risk evaluation. The PHA method applied in this approach is based on the methodology described in SFS EN ISO 12100 (2010), IEC ISO 31010 (2009), Roland and Moriarty (1983), Leveson (1995) and Vincoli (2006). A PHA-type method is applied for the overall

production-area analysis and in analysis of system operation and maintenance concepts in the conceptual design and system-definition phases. The PHA covers conceptual work-site-level issues, the automated machinery system under study and its operation environment, and interfaces to other systems and activities in that environment. The PHA covers all phases of the system life cycle, including construction, testing, and commissioning of the system – all new elements, not present with manual machine applications.

OHA is for the upper-system-level assessment. The objective at OHA level is the identification and assessment of the operations risks related to the planned and designed system operations and to maintenance procedures, system functions, and human–technology interaction. The upper-system-level risk-assessment application utilises the OHA method, a risk-matrix-based method for risks' estimation, and specified criteria for risk evaluation. The OHA focuses on system operation and maintenance procedures, aspects of human–technology interaction, and system functions that extend throughout the machinery application. The OHA method applied in this approach is based on the methodology described in Roland and Moriarty (1983), Stephenson (1991) and Stephans (2004). The objectives in the OHA is to identify potential hazards and hazardous events in the operation procedures for the system in the selected phases in the life cycle, in view of both human error and technical failures; to estimate the risks; to evaluate the safety measures designed or planned; and to specify possible additional safety measures for this application. Among others the following types of operator errors are used to guide the analysis (Stephenson 1991, p. 142):

- Neglect to perform required actions
- Perform actions that are not required
- Fail to recognise needed action
- Respond improperly (early, late, or inappropriately)
- Engage in poor communication
- Make a maintenance error.

The OHA should be conducted in early phases of the system concept's development or at the beginning of the customer-specific application project, depending on the stage in the system's development. In this approach, the OHA is meant to be updated in the system's implementation and commissioning phase for purposes of validating the safety measures designed and implemented to control the operations' risks and to identify any new site-specific risks (or potential risks) that were not identified in the system-development phase. Upper-system-level risk assessment should be carried out when the machinery-automation system or part of it is being modified and when operation and maintenance procedures are undergoing changes.

HAZOP study is for the lower-system-level assessment. The objective in HAZOP studies is the identification and assessment of functional safety risks related to possible technical failures, software errors and human error in subsystem functions, on-board functions, and human–technology interfaces. In HAZOP studies, the focus is on analysis of lower-system-level functions and, especially,

on identification of safety-related deviations in the interfaces between subsystems and in the user interfaces. Possible human errors and technical problems (both referred to below as 'deviations') and their causes and consequences are systematically analysed by means of the 'guide words' and the procedure described in the HAZOP standard (IEC 61882:2001). The guide words 'no', 'less', 'more', 'as well as', 'other than', 'part of', 'reverse', 'before', 'after', 'early', and 'late' are modified case specific to identify deviations. The HAZOP studies are supported by system architecture modelling, function-level drawings, and the use-case descriptions. These supporting documents can be utilised for sharing of information within the control system design teams. The HAZOP study for the on-board control systems is conducted at function level and can be continued at more detailed, signal level if necessary. Lower-system-level risk assessment should be carried out also when subsystems or parts of them are being modified or the automated functions are being changed.

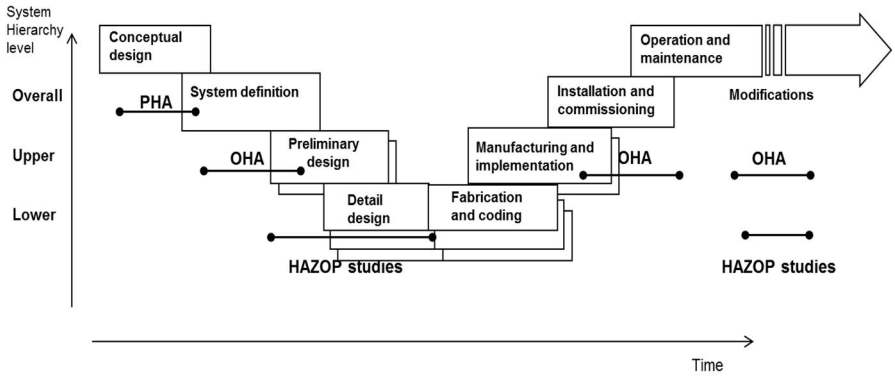


Figure 18. An outline of the system-level risk-analysis tasks' allocation to the various phases in the system life cycle and levels of the system hierarchy.

4.3 Integration with the systems engineering and functional safety engineering approaches

The risk assessment is a continuous process. In the three-level approach, the main idea is that the risk-assessment work proceeds systematically throughout the full process of system development, in all its phases, and the higher-level analysis results are used as input to lower-level analysis. According to systems-engineering literature and the standard ISO IEC 26702 (2007), the systems-engineering process is performed iteratively at each level of the system hierarchy and the risk-assessment activities are closely connected to the phases of the systems-engineering process: requirements' analysis, functional analysis and synthesis, and system-analysis tasks.

The aim in the three-level approach to risk assessment is to support the specification of a requirement baseline and the design and verification of the functional and physical architecture in each phase of system development and at each level of the hierarchy of the automated mobile work-machine system. The objectives and execution plan for safety-engineering tasks are specified level-specifically: the safety-engineering tasks have different scopes, objectives, and methods in PHA-, OHA-, and HAZOP-level risk-assessment processes, so they are able to identify and assess different types of safety risks in different phases of system development and at the individual levels of the system hierarchy.

An outline of the safety-engineering tasks at 'heading level' linked to the various phases of the system-engineering process is presented in Figure 19. The systems-engineering process model in the figure is adapted from ISO IEC 26702 (ibid., p. 12).

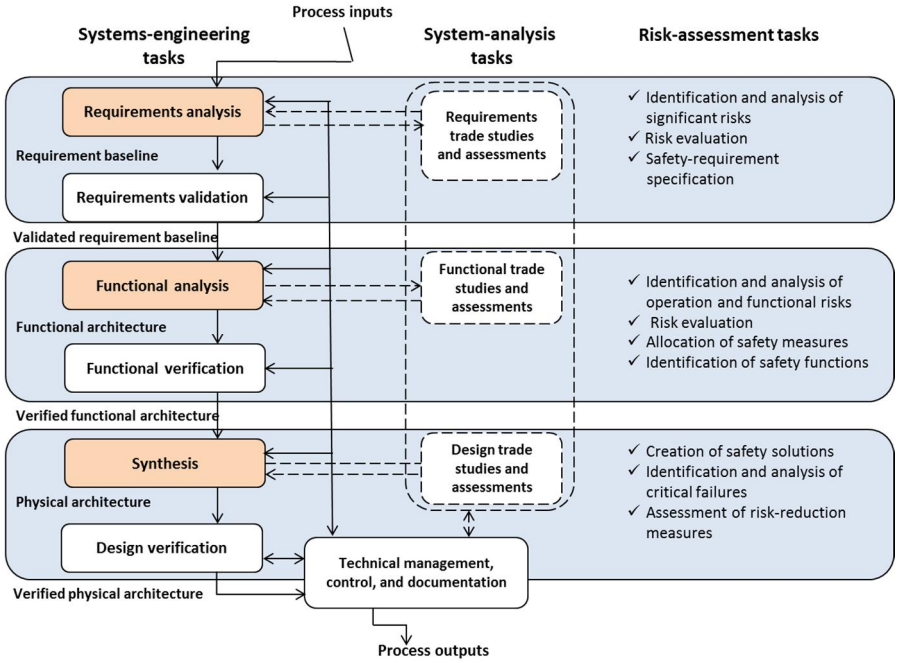


Figure 19. An outline of the risk-assessment tasks allocated to the various phases in the systems-engineering process and associated system-analysis activities.

The development and design of safety-related automation systems in industry is required to follow set functional safety guidelines. The functional safety standard SFS EN 61508-1 (2011) has become the *de facto* standard in many fields of industry, including those utilising automated mobile machinery. Said standard focuses on the design and verification of safety-related E/E/PE parts of the control system and only outlines the risk-assessment procedure that forms the basis for specification and assignment of requirements for safety-related control functions

and other risk-reduction measures. The present study's output – the three-level approach to risk assessment – offers a practical solution to supplement the functional safety standard guidelines for hazard and risk analysis by introducing three qualitative levels of risk assessment (again, PHA, OHA, and HAZOP studies) for the overall risk-assessment process in the context of complex automated mobile work machinery. In many cases, it is important to separate the safety-related functions clearly from other control functions and from other risk-reduction measures. Figure 20 gives a simplified overview of the three-level approach to risk assessment and its risk-assessment activities integrated with the systems-engineering and functional safety engineering approaches.

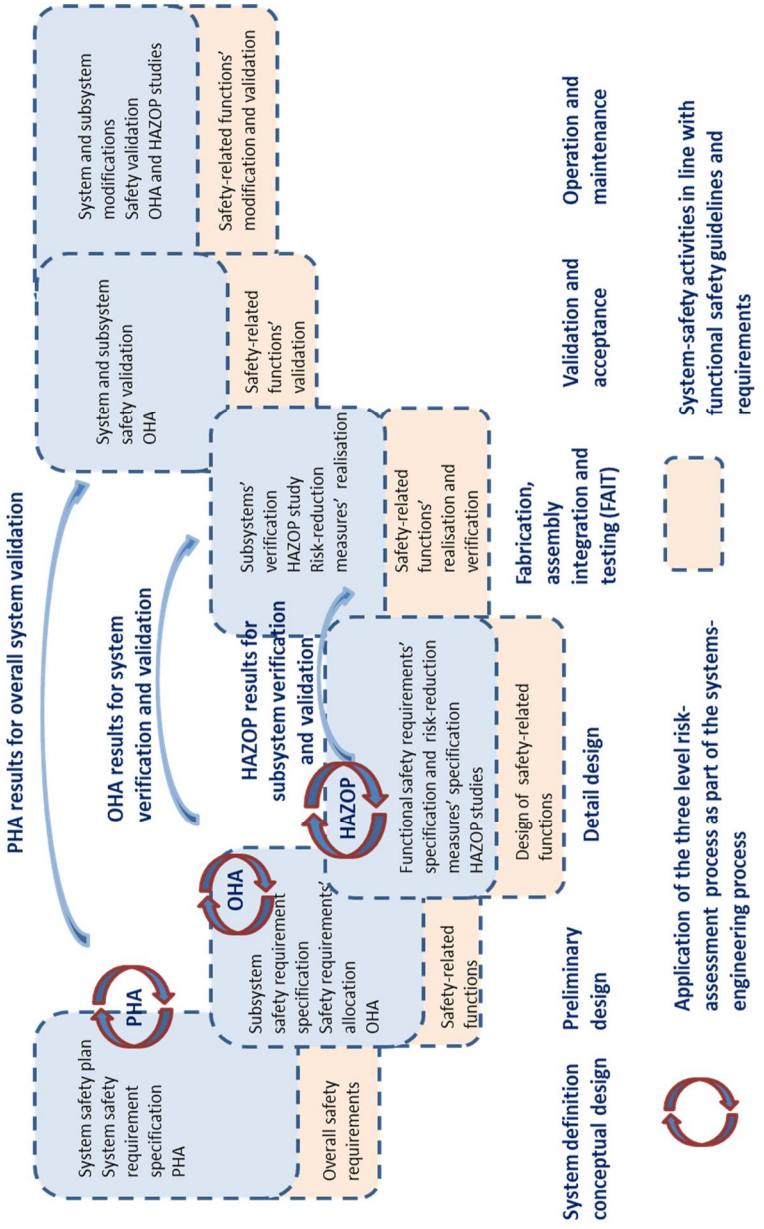


Figure 20. An outline of the three-level approach to risk assessment adapted to the system's life cycle and the various levels of system development and set in the context of the system hierarchy.

5. Case study 1: The existing ore-transportation system

5.1 Introduction

The objective of the first case study is to evaluate the usefulness of the first implementation of the three-level approach to risk assessment and the usefulness of PHA and HAZOP methods, as they were used at the time of the field work, in a phase in the operation of a complex automated mining-machine application.

The target system in this case study is a semi-automatic ore-transportation system in an underground iron-ore mine in Kiruna, Sweden (see Figure 21). On the assignment of the mining company, VTT undertook evaluation of the safety of the semi-automatic ore-transportation system and assessment of its conformity to the main safety and health requirements set in the Machinery Directive as in force at the time (see Figure 4). Special focus in the assignment was placed on automation-related safety issues.

Figure 21. An electrically powered LHD in the Kiruna mine (Sandvik). Reprinted with permission from Sandvik Mining and Construction.

The work was conducted in 2000–2001 in co-operation with the mining company, the mining-machine manufacturer, and the mining company's subcontractor who had delivered subsystems for the automation system. The ore-transportation system using electrically powered LHDs had been operating in various extents since 1998 (Gustafson 2011, p. 22). A simplified block diagram showing the main ele-

ments of the target system, Figure 22 outlines the LHDs and their on-board control systems, communication system, automation-control unit, and operator stations.

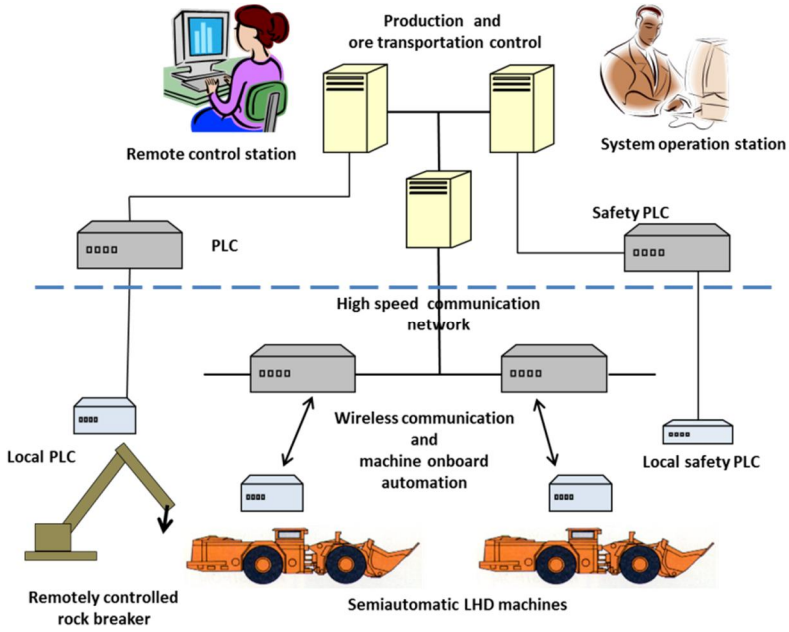


Figure 22. A block diagram of the target system.

The project in question included several risk-analysis tasks, of which the three described below have been selected for this case study, representing all three levels of risk analysis in the three-level risk-assessment approach. The overall system risk analysis with respect to potential hazards and safety risks in the automated production area applied PHA methods. The upper-system-level risk analysis of system operations and system functions and the lower-system-level risk analysis of the LHD on-board control system employed the HAZOP method. This case study addresses the following research questions:

- How suitable is PHA for work-site-level hazard identification and risk analysis in automated mobile work-machine systems?
- How well does the simplified risk-estimation methodology suit risk estimation at the various levels of risk assessment?
- How appropriate is the HAZOP method for risk analysis of system operations and system functions?
- How suitable is the HAZOP method for risk analysis of on-board control functions?

- How well does the three-level risk-assessment approach applied at the time of the assignment suit risk assessment for a highly automated mining-machine system in its operation phase?
- What are the benefits and impacts of the risk-assessment effort in this case and more generally in the companies?

5.2 Implementation of the three-level risk-assessment approach

5.2.1 Hazard identification in the PHA

The objective of the first overall system risk analysis in this case was to identify automation-related hazards and hazardous events and to evaluate their safety risks in the operation area of automated LHDs.

The analysis was carried out as an application of PHA methodology by a team composed of nine experts from the mining company, representing the mine management, occupational safety management, production, LHD operators, control-room operators, and underground maintenance, alongside two researchers from VTT. The PHA team had four one-day analysis meetings in Kiruna. Because of practical factors such as the participants' work-shift arrangements, the meetings were grouped into two sessions, of two days each. Visits to the automated underground production areas and underground control rooms were organised for the researchers during the analysis sessions. Not all experts from the mining company were present the whole time. The author of this thesis and another researcher from VTT took part in all the meetings. The representative of the site's occupational safety management presided over the analysis sessions, and the author of this thesis documented the results.

All present from the mining company had some experience of risk-analysis team work. Underground work-site safety audits, mining job-safety analyses, and safety analyses of work equipment and machines in use were routine for the mine. Overall risk analysis for the semi-automatic ore-transportation system had not been carried out before. To prepare the team for this analysis work, PHA methods and analysis work practices were introduced to the team. The system operations and work tasks associated with the various phases in operation of the automated ore-transportation process were specified and limited before analysis. The following phases were examined:

- Work in the production area before automated production starts
- Machine operators' work in the production area and in the control room in daily work shifts
- Support work in the production area during automated-production periods

- Troubleshooting and maintenance work in the production area, necessitated by production breaks, during automated-production periods.

Potential manual-mining-machine-related hazards were discussed and listed at the beginning of the analysis, to clarify the focus and limit it to automation-related hazards and potential hazardous events. Examples of mobile-work-machine-related hazards are overrun hazards in a tunnel, hazards of crushing against a tunnel wall, hazards associated with collision with a service car or some other vehicle in a tunnel, and electrical hazards related to high-voltage circuits in electrically powered machines. Among others, the following 'hints' were formulated by the researchers for the identification of new automation-related hazards or hazardous events:

- Unexpected behaviour of an automatic machine while it is moving
- Operator error causing unexpected start-up
- Operator error in tele-operation
- Indirect effects of human error that affects operation procedures
- Indirect effects of human error in change management
- System failure causing failures in data communication
- Misunderstanding of work procedures in the production area.

The identification of hazards and hazardous events involved applying a mixture of a brainstorming technique, scenario-analysis techniques (IEC ISO 31010:2009, p. 40), and a systematic job-safety analysis checklist developed for the analysis of production automation (Kuivanen 1995, p. 81) with the aid of work-shift routine descriptions and underground-production-area layout pictures. The brainstorming and scenario analyses were conducted informally through team discussion. The hazards identified and descriptions of potential hazardous events were noted on a whiteboard for further analysis. In a formal brainstorming session, participants explore ideas first as individuals, without discussion, for freely flowing thinking (Reunanen 1993; IEC/ISO 31010:2009). After the identification of potential hazards and hazardous events, the analysis continued with systematic consideration of the operators' work tasks in the control room and the mine service workers' tasks in the automated production area. This part of the analysis too entailed team discussion technique. The analysis results were collected and documented in a PHA worksheet (included as Appendix 1).

In the PHA, 58 distinct hazards or hazardous events were identified with respect to operations in the automated production area, and 46 of them were deemed to have potential to cause a risk to personal safety. Among others, the following hazardous scenarios were identified as new automation-related system-level risks specific to this context and operation environment:

- The mine support group are still working in the production area although automatic operation has started.
- An operator loads the wrong data, and the automatic LHD navigates out of the production area.

- An operator makes an error in defining the area and the automatic LHD dumps the load into a shaft in which feeder-system maintenance is in progress.
- The electricity supply is disconnected from the machine unexpectedly during its automatic test procedure.
- An automated LHD makes an unexpected movement while being serviced.
- An LHD operator starts tele-operating the wrong machine, because of a technical failure or human error.

5.2.2 Risk estimation and risk evaluation in the PHA

Risk estimation was performed on the basis of three-level estimation of the severity of the consequence and of the probability of the hazardous event. This rough estimation model had been used at VTT for risk estimation for industrial machines and production systems such as industrial robot applications (Kuivanen 1995). The risk-estimation method was a simplified version of the method presented in the risk-assessment standard EN 1050 in force at the time (see Figure 4). The baseline in the risk estimation was a situation without any protective measures. The risk level, which indicates the magnitude of the risk, was calculated with the formula $R = S \times P$, where R is the risk level, S corresponds to the severity of the harm, and P represents the probability of occurrence of that harm. Severity levels were indicated with the following values:

- 3 for severe (fatality or permanent injury)
- 2 for significant (reportable injury)
- 1 for insignificant (slight or no injury).

Probability levels too were indicated with values:

- 3 is probable (the risk can be realised in normal operation)
- 2 is improbable (the risk can be actualised only in certain conditions)
- 1 is rare (in all conditions).

From these values, each risk was categorised as being at one of three levels, for prioritising of the actions required to reduce the risks to an acceptable level (see Table 1).

Table 1. Risk levels and indication of the urgency of action.

Risk level	Urgency of actions
9	Measures must be taken immediately to make changes in the system. The risk must be reduced.
6 or 4	Measures must be taken to develop the system with regard to the issue at hand. The risk must be reduced.
1, 2, or 3	There should be a plan for developing the system.

Risk evaluation was then done. This involved considering the adequacy of the existing safety measures, technical and instruction-related, and estimating the residual safety risk. In total, 51 proposals for actions were specified, with the following among them:

- The local safety system that isolates the automated production area must be fail-safe.
- Human and vehicular traffic must be controlled at the gates.
- Safety instructions and safe work procedures both for the automated production area and for the control-room operations must be documented, and training must be given in their use.
- Work in the automated production area must be planned and scheduled in detail in advance.
- System operators must always be aware of what activities are going on in the automated production area and in the ore passes.
- Working alone in the automated production area must be avoided.
- Communication practices and technologies must be improved, to ensure that misunderstanding is avoided.

Of the 51 proposals, 36 were improvements of existing measures and 15 were new, additional proposals. Proposals were considered through application of the principle of three-step risk reduction presented in the Machinery Directive, as in force at the time, and in the basic machinery-safety design standard EN 292-2 of the day (See Figure 4). Firstly, the machine manufacturer or system designer should consider the possibilities for elimination or minimisation of risk via machinery design and construction means. Secondly, the machine manufacturer or system designer should take into consideration all protection measures necessary to reduce risks that cannot be eliminated. Finally, if the risks are still not acceptable after these two iterations, users must be informed of the residual risks, the necessary training should be arranged, and any need for provision of personal protection equipment must be specified. This requirement, with the same content, is termed ‘principles of safety integration’ in the current Machinery Directive, Directive 2006/42/EC (2006), and in the present risk-assessment and risk-reduction guideline standard for machinery (SFS EN ISO 12100:2010). Guidelines and references for the safeguarding techniques were taken from the relevant machinery-safety standard of the day, EN 292-2, which has since been replaced by SFS EN ISO 12100 (2010).

Analysis results – hazards, causes and consequences, risk level, existing safety measures, proposals for possible additional safety measures, and the department responsible for actions – were recorded in a table on a risk-analysis worksheet (Appendix 1). All analysis results were linked to the relevant points of the essential health and safety requirements stated by the Machinery Directive for the system conformity assessment. A table was created to link the findings with the relevant

requirements. This table was amended later in light of the results of the more detailed analyses. The evaluation results were then submitted to the project-management and mine-management teams for further evaluation.

5.2.3 HAZOP study of system operations and system functions

The objective of the system-level HAZOP study was to analyse system operations, considering both the errors a system operator might make and the technical problems that are possible. The scope for this HAZOP study was specified as covering the system operations performed by the system operator working in the control room. Related system functions were studied at the level of information exchange between subsystems.

The HAZOP study was carried out by a team composed of seven experts, representing various interested parties from the industry (the mining company, the machine manufacturer, and subsystem suppliers), and two researchers from VTT. This HAZOP team had six one-day analysis meetings in Sweden. For practical reasons, the first four meetings were arranged as two two-day sessions. Four to seven company representatives were present at each meeting. The author of this thesis and another researcher from VTT took part in all the meetings. The HAZOP method was new for all industrial members of the team; however, most members of the team had experience of risk-analysis team work. The HAZOP methods and analysis work practice were introduced to the team before work began.

The first task in the HAZOP study was to identify the system-operation tasks and related information exchange at the operator interface and at the interfaces between subsystems. Tasks were listed, and related information was described by the system experts. In total, 22 distinct system-operation tasks were identified:

- Configuration of the automated system (6 tasks)
- System testing (2 tasks)
- Tasks in the beginning (4 tasks)
- System operation during a work shift (6 tasks)
- System operation at the end of a work shift (4 tasks).

A rough system-architecture drawing was compiled from various documents to support this identification phase and to aid in the later analysis work. The system's information exchange was described in terms of information type, such as status information, control signals, audio/video information, and alarm information.

Possible human errors and technical problems (both referred to below as 'deviations') and their causes and consequences were systematically analysed by means of the 'guide words' and the procedure described in the HAZOP standard (IEC 61882:2001). In this analysis, consequences were estimated roughly by severity, with four categories: personal-safety risk, machinery damage, production stoppage, and delay in production. The team could not find suitable criteria for estimation of the probability of harm or other consequences. Even the three-category estimation described above was considered too difficult, because almost

all deviations seemed to be possible in normal operation conditions and statistical failure data for the system were not available. For each deviation identified, its type, the causes and consequences, existing safety measures, and proposals for possible additional safety measures were recorded in tabular format on an HAZOP worksheet (Appendix 2).

In total, 83 distinct deviations were identified in relation to the selected operator tasks and related information exchange at subsystem interface level. These included the following:

- The technician specifies the automatic area or some elements of it wrongly for the automation system.
- Testing of the autonomous routes is done carelessly.
- The operator does not follow the procedure when changing the system's operation mode.
- Failure in information exchange leads to status information differing between individual subsystems.

Thirteen of the deviations were considered safety-critical and able to cause a personal-safety risk. Evaluation of the risks against the safety measures implemented was performed in view of references obtained from the relevant European machine-control-system safety standards valid at the time, such as ISO 13849-1, EN 60204-1, and IEC 61508. In total, 24 proposals for new corrective actions were specified. The following examples give an overview of the proposals:

- Safety instructions, safe work procedures, and safety training must be improved with respect to the task-specific issues specified by the team.
- Control ensuring that everyone whose work is connected with the automated production system follows the safety instructions must be improved.
- The local safety system must be fail-safe.
- Safety-critical communication between subsystems must be monitored and kept secure, to an appropriate safety integrity level.
- Safety-critical status information must be kept secure, to an appropriate safety integrity level.

After this, the table linking the risk-assessment results to the relevant points in the essential health and safety requirements stated in the Machinery Directive was amended to cover the HAZOP results. The results were then forwarded to the company's R&D management personnel for further evaluation.

5.2.4 HAZOP study of the on-board control system

A more detailed system-level risk analysis was conducted, focusing on the control functions of the machine-control system. The objective of this HAZOP study was

to identify and assess safety-related deviations in the automated LHD on-board control functions.

The first phase in the HAZOP study was to identify the main functions in the on-board control system. Nineteen functions, including automatic tramming (driving), motor start/stop, operation mode selection, and video control, were identified. These determined the scope of this analysis. The functions were prioritised by assumed criticality for personal safety, with the analysis work starting with the most critical functions. The functions were divided into elements (signals) in accordance with the procedure in HAZOP standard IEC 61882 (2001). Because of the large number of related design documents, it was difficult to pull together and connect to each other all control-system modules, I/O connections, signals, and messages that were related to a certain function. Therefore, a new function-level presentation format was devised and developed by VTT, to support the analysis work and for use as system documentation for maintenance and troubleshooting purposes. Figure 23 gives an overview of a function-level drawing integrating information from several separate control-system design documents.

The second phase in the HAZOP study was to identify deviations in the quantities of the signals from specifications and determine their causes and consequences systematically, in line with the standard procedure. The above-mentioned guide words were used to identify deviations.

The third phase in the HAZOP study was to estimate the risks on the basis of the same three-level estimation method applied in the PHA analysis, as described. The severity of the consequence and the probability of the occurrence of harm were estimated first for the scenario involving no protective measures. The risk level was calculated with the formula $R = S \times P$, where R is the risk level, S refers to the severity of consequences, and P corresponds to the probability of harm or other relevant consequences occurring. Severity categories were specified for this purpose, as follows:

- 3 represents injury (fatality or permanent injury)
- 2 indicates machine damage (collision with a wall)
- 1 stands for machine downtime (machinery stopping / system out of use).

Probability categories were clarified, with some guiding examples to support the estimation work:

- 3 represents probable occurrence (e.g., cable failure)
- 2 indicates improbable occurrence (e.g., several independent failures)
- 1 refers to rare occurrence (e.g., CAN bus ‘residual failure’ or SW failure when the SW has been tested well).

For each deviation identified, deviation type, causes and consequences, risk level, existing safety measures, and proposals for possible further safety measures were recorded with the same worksheet template that was used in earlier HAZOP studies.

A HAZOP team composed of seven experts, representing all interested parties – the mining company, the machine manufacturer, on-board subsystem suppliers, and VTT – was established to carry out the analysis. The HAZOP team had four one-day analysis meetings in Sweden. For practical reasons, these meetings were

grouped into two two-day sessions. The number of team members varied, so 5–7 company representatives and two or three researchers from VTT took part in each of the meetings. The author of this thesis participated in all these sessions. After these meetings, a small analysis group composed of 1–3 participants from the industry and one researcher from VTT worked in four half-day tele-meetings.

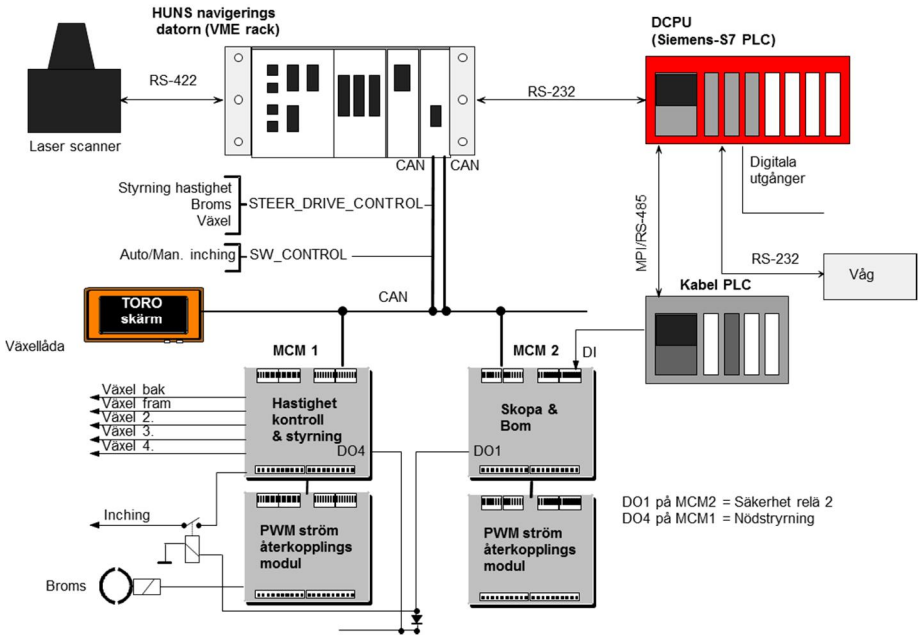


Figure 23. Example of the function-specific drawing format used in the HAZOP study (in Swedish).

As a result of the HAZOP study, in all, 326 distinct deviations were identified, in relation to the 19 functions under study. Ten of the deviations were considered safety-critical. The standards of the time ISO 13849-1, IEC 61508, and EN 60204-1 were used as guidelines and references for the evaluation of the existing implementation of functional safety principles and for the specification of proposals for corrective actions. There were 52 proposals specified. They are not described in detail here, but the following examples provide an overview of them:

- Certified safety components should be used in safety-related functions.
- The system and configuration documentation should be improved.
- Software version and parameter management should be improved, as should history recording.
- Password protection for change management should be implemented.

- A clear principle for identification of operation modes (automatic vs. manual) aboard machines and by the gates should be developed.

The summary table linking the risk-assessment results to the relevant points in the essential health and safety requirements as stated in the Machinery Directive (Directive 98/37/EC, 1998) was adjusted to account for the HAZOP results. The results were then forwarded to the R&D management of the company for further evaluation.

5.3 Experiences, comments, and observations

5.3.1 The mining company's experiences and comments

The practical implementation of the analysis and three-level assessment work was discussed and agreed upon at the beginning of the project, and the work was conducted in keeping with the plan. During the project, no specific comments were received on the methodology used. The mining company's experiences and comments associated with the risk-assessment project and its results were detailed in the final review meeting, in April 2001. Present at the meeting were the manager of the semi-automatic ore-transportation system-development project, the underground mine's industrial-safety delegate and the safety engineer, the system expert of the automation system's supplier, and two researchers from VTT.

According to the mining company, the co-operation in the project went well and the operation and maintenance staff had experienced it as positive to be able to participate in the risk-analysis work. The mining company stated that the results of the project clarified the main areas in which the system improvements need to be concentrated for ensuring the safety of the system and conformity with the Machine Directive's main health and safety requirements: for an access-control system that keeps the operation area of the automatic LHDs safe, safety instructions and set daily procedures for use in system operation and maintenance, system software version management and parameterisation, and reliability of the communication throughout the automation system.

The PHA covered the operation situations of the semi-automatic ore-transportation system in the production area, and the upper-system-level HAZOP study was focused on operator actions and system functions. The HAZOP study for on-board machine operations entailed detailed signal-level analysis. System troubleshooting and daily maintenance issues were covered in the PHA, and operators' actions in system fault situations were touched upon in the upper-system-level HAZOP study of system operations. According to the mining company, the analysis of maintenance tasks in the automated production area should have covered the work done on the machine also, such as troubleshooting of the on-board control system and maintenance of the on-board automation components, because they are automation-related work tasks and could perhaps bring new safety risks.

Even though the analysis was focused on safety issues, the mining company stated that it had been valuable to go through the system systematically with the experts from all interested parties and to have a common understanding of the system architecture, system operation, and system functions. The risk analysis brought together experts from all stakeholders in the automation-development project and got them to discuss potential problems and come up with possible solutions and improvements. The mining company also pointed out that the proposed corrective actions and proposals for improvement specified in the project were valuable and that many of them would be realised in the system-development project in co-operation with the machine manufacturer and subsystem suppliers.

The importance of the analysis documentation format and how the results – identified hazards, hazardous events, causes and consequences, risk levels, existing safety measures, and proposals for additional safety measures – are described in the worksheets was brought up by the industrial partners. As one of the mining company's representatives stated at the final review meeting, the analysis results were, in places, too briefly expressed and difficult to understand, especially for those who were not themselves participating in the analysis sessions.

5.3.2 Observations

The semi-automatic ore-transportation system had been developed, implemented, and extended in the course of several years at the mine. One of the strongest motivations for this project was the mining company becoming aware of its responsibility for the safety of the whole automated ore-transportation system. The mining company had developed the system in co-operation with the subsystem suppliers, integrated the control room and on-board subsystems into the automated production system, and then started to use the system. Under the Machinery Directive, the mining company became the 'manufacturer' of the semi-automatic ore-transportation system. The mining company wanted to have a fuller picture of the safety risks linked to operation and maintenance of the system, not just the basis and reasoning for the safety requirements and safeguarding solutions.

The project in question was the first risk-analysis assignment for such a complex automated mobile work-machine system and, as such, gave researchers valuable information and experience of how to carry out hazard identification and risk evaluation of a complex machinery system in co-operation with multiple industrial partners.

The PHA was carried out with traditional brainstorming and team discussion methods. The identification of the work-related hazards was grounded in the company representatives' many years of experience of mining work and personal experiences of work with the automated LHD system. The analysis proceeded smoothly, and discussion was lively. The role of the VTT researchers was mainly to keep the discussion focused on the question at hand and record the results. In the four full-day analysis sessions, 58 findings of automation-related hazards or hazardous events were identified and 51 distinct proposals were generated and specified.

The upper-system-level HAZOP study of system operations and related system functions completed the higher-level risk analyses by analysing the effects of possible functionality deviations (both human error and system failure) on the selected system operations. In total, 83 deviations were identified, and 24 proposals for corrective actions were defined. Some of the hazardous events caused by these functionality deviations had been identified already in the PHA. New hazardous events were identified as the analysis advanced to a more detailed level in the operation procedures and technical failures. No precise value associated with the new hazards as compared with the earlier results can be presented here, because of the insufficient and inexact expression of the findings.

The efficiency of analysis methods can be evaluated via examination of the effort applied in the analysis versus the number and quality of results yielded. In the PHA meetings, a large amount of time was devoted to general discussion of the work management in the automated production area, prioritisation of production and maintenance activities, daily work scheduling, and communication between the production team and the maintenance teams. Systematic analysis of the system functions in the upper-system-level HAZOP study sessions and discussion of the possible technical problems and failures at higher level, without delving into details of message or signal characteristics, turned out to be important for enabling all interested parties to understand the existing capabilities of detecting failures and the existing inherent redundant information channels. These discussions were not always related to the analysis in question, but, in fact, they were of great value for the mining company, as was indicated at the final review meeting for the assignment.

The on-board system HAZOP study at detailed signal level was the most laborious analysis task in this case. In addition to the actual work to analyse the 19 selected functions, great effort was undergone at VTT to collect the necessary information from various design documents and to create the function-level drawings that made it possible to analyse the on-board system functions in such detail. The HAZOP method, with the aid of guide words, revealed 326 deviations from designed signal characteristics. Most of them involved control-system reliability issues. Accordingly, in addition to the corrective actions related to the 10 safety-critical deviations, much important information was produced for improvement of the on-board system reliability and availability. The traditional worksheet text document turned out to be laborious to create and maintain. For greater efficiency of the analysis work, tele-meeting techniques used with shared documents were applied in a smaller group in the risk-estimation phase. Experiences of that tele-meeting technique were positive.

A risk-estimation method using three categories for the probability of occurrence of harm and for the severity of the harm, with clarifying hints, was considered simple and general enough for qualitative expert estimation in PHA. The simplicity of the method caused difficulties for the evaluation and prioritising of the risks. For example, severity level 3, meaning fatality, and probability level 2 together give the same risk level as severity level 2, meaning reportable injury, in combination with probability 3. The same three-category estimation method, with

differently specified criteria, was used in the on-board system HAZOP study. When the results were compared with the PHA results, the different expression of the same severity or probability categories caused lack of clarity and created some extra work for interpretation of the results.

Use of the semi-automatic ore-transportation system continued in Kiruna in varying extent for several years after the assignment. Some years ago, the mining company stopped using the system, for various reasons (Gustafson 2011, p. 23). According to the machine manufacturer's experts interviewed in March 2012, no automation-related accidents caused by the automated machinery had been reported to the machine manufacturer.

5.4 Discussion

In this case, the target system had been in use for several years. The main purpose of the risk analyses conducted in the assignment was to validate the safety of the automated ore-transportation system. The PHA and HAZOP methods are well known in risk analysis in industry, and most of the work methods used in those analyses in this case were in widespread use. Mobile work machines such as the mining machines in question have been used in mines for many years, the risks related to manually operated machines are known, and machines are manufactured in line with the safety regulations and standards in force. The target system in this case was challenging in the safety sense. It was a technologically complex system, and there was a lot of new technology implemented for the automatic operation, semi-automatic functions, fleet management, and production management. In complexity, it can be compared with other large-scale automated applications for industrial production. The difference is that in this system the material-handling units were rubber-tyred, electrically powered, highly automated mobile work machines. The system was the first of its kind in the entire mining industry.

The systems-engineering guidelines used at the time (such as system-architecture models and descriptions of hierarchical structures of the system), interconnections, and protocols for communications between subsystems and human–technology interactions were utilised in this case, and they had an essential role in the preparation and carrying out of the risk-analysis work aimed at uncovering the automation-related safety risks that had not been experienced yet. Those guidelines are, at base, those described in the latest systems-engineering literature, such as ISO IEC 15288 (2008, pp. 7–10), SE Handbook (2011, pp. 9–14), and Leveson's work (2011b, pp. 61–67). The analysis results and comments from members of the analysis team confirm that, with the aid of system thinking, the traditional risk-analysis methods PHA and HAZOP study were successfully directed to identification of new unforeseen hazards and hazardous events and to possible indirect effects causing hazardous relations and consequences, not only to identification of existing problems and the experienced failures that come to mind first. System thinking was also employed successfully to support risk evaluation and specification of improvement proposals, for development of the safety

functions at an appropriate level of the system hierarchy, and for preparation of safety instructions for the right level of operation and maintenance instructions.

PHA methodology using brainstorming sessions and systematic job-safety analysis was suited well to the overall-level (i.e., work-site-level) risk analysis. The author's experiences of this methodology, the analysis results obtained, and the comments from the industrial partners in this case study support the results that Leveson (2003, pp. 7–8) and Vincoli (2006, pp. 37–38) have described in their discussion of the relationship and differences between industrial safety engineering, on one hand, and system-safety analyses and engineering practices. Vincoli claims that system-safety analysis (including methods such as PHA, SHA, and OHA) provides an excellent way for industrial-safety experts to achieve an accident-free work environment (ibid., p. 38). Leveson (2003, p. 5) describes system safety as based on systems theory and a systems-engineering approach to preventing foreseeable accidents and to minimising the negative consequences of unforeseen accidents. From many years of experience in the process industry, aviation, and the space industry, Leveson also claims that, with introduction of robots in the workplace environment and with long-lasting engineering programmes that involve complex engineering design and manufacturing activities, the traditional concerns of industrial safety and system safety have become more integrated with each other (ibid., p. 8).

Redmill et al. (1999) indicate that HAZOP study is effective for identifying hazards not only in technical systems but also in human-centred systems, because of its way of looking at deviations from the design intent of the processes and tasks and the information flowing between them. The HAZOP method can be used to explore deviations from the design intent by the humans and on the part of the technical system. The interpretations of the guide words must be modified to be appropriate for the human perspective, however (ibid., pp. 166–169). Practical experiences and study results in this case support the above-mentioned opinions expressed by Redmill and colleagues. The team-work-based HAZOP technique with the aid of guide words seems well suited to risk analysis of system operations and system functions, along with on-board control functions of an operational automated mining-machine system.

Risk estimation employing three categories for the probability of occurrence and for severity turned out to be simple and general enough for qualitative expert estimation in this case. However, the simplicity of the method and variation of the category definitions caused confusion and differences in interpretations and, so, decreased the reliability and quality of the analysis results. Risk-estimation methodology and the guidelines applicable for machinery have developed since the time of the case in question. In the latest machinery-safety guidelines for risk assessment, found in SFS EN ISO 12100 (2010) and ISO TR 14121-2 (2007), the probability factor is presented as a function of the following parameters (SFS EN ISO 12100:2010, p. 17):

- The exposure of one or more persons to the hazard
- The probability of the occurrence of a hazardous event

- The technical and human possibilities for avoiding or limiting the harm.

Cox (2008) has examined risk matrices supporting decision-making in the risk-management process and discusses the limitations and problems of using risk matrices in risk management. Four types of problems related to risk matrices have been identified: poor resolution, errors, sub-optimal resource allocation, and ambiguous inputs and outputs. Cox opines that risk-management decisions cannot be based only on rating of risk frequency and severity factors. Although risk matrices are recommended in international risk-management standards, these matrices should be used with caution. The judgement bound up with risks' ranking or rating should be explained with care (ibid., p. 510).

In this case, all risk analyses were performed in several teams of experts, composed of the available people most expert in the subject at hand and the safety factors in question. This led to a situation in which the results of the higher system-level risk analysis were not utilised systematically in the lower-system-level risk analysis as input data. On the other hand, the aim of the assignment was to identify and assess the automation-related safety risks of the existing system as well as possible. Overlap between the analyses and between the various points of view on any given hazard or hazardous event increased the analysis results' reliability and the quality of the improvements and corrective actions proposed.

5.5 Conclusions

From the comments received from the mining company, the risk-assessment work can be considered to have been valid at the time and to have added value for the company by clarifying the most important actions needed for reduction of automation-related safety risks to an acceptable level and by introducing new ideas for system development in co-operation with the machine manufacturer and subsystem suppliers. The mining company indicated that the risk-analysis work had given them valuable information about the automation-related risks and the current status of the system safety of the semi-automatic ore transportation. The machine manufacturer's experts confirmed in the interviews in March 2012 that no automation-related accidents caused by the automated machinery had been reported to the machine manufacturer between the end of the risk-assessment assignment and the system's decommissioning a few years ago. From all of this, one can conclude that the system-safety approach and the methods used were appropriate and supported the mining company in its solving of the system-safety problem.

PHA methodology using brainstorming technique, systematic job-safety analysis, and team discussion technique was practical and efficient for the analysis of the operation situations and identification of potential hazards with the existing automated mobile-machine system. It can also be concluded that the HAZOP method using team discussions and supported by system-architecture drawings worked out well in the analysis of higher-level deviations in subsystem interfaces.

The HAZOP study also fit in well with the analysis of functionality deviations in the on-board machine-control system. The new, innovative function-level drawing

concept turned out to be essential for efficient performance of the analysis. The clear and adequate description of the analysis findings, hazards, causes and consequences, and assessment results turned out to be essential, especially in such a complex automation system, wherein the information is shared with several partners and specialists in various fields of technology.

Considering the practical experiences, one can conclude that the 3 × 3 risk matrix method, as it was used in this case, had deficiencies, which weakened the reliability of the analysis results and created extra work in the risk evaluation. There was some confusion within the PHA analysis team as to which probability they were estimating: that of occurrence of harm or the probability of a hazardous event. In the HAZOP teams, the same confusion occurred with respect to the probability of dangerous deviations (dangerous failure) or of a particular deviation in the general case. The definitions for severity and probability categories should have been specified clearly and should have been the same in all analyses, to render the risk levels comparable. At the same time, the simple multiplication of severity by probability value obscured the significance of the severity factor and made it difficult to evaluate which means of risk reduction are appropriate or what resources should be allocated for them.

The main working language of the analysis sessions was Swedish, and all documents were written in Swedish. This caused problems during the team discussions and with the documents' choice of expressions and wording, thereby affecting the quality and reliability of the analysis results.

6. Case study 2: The ore-transportation-system concept

6.1 Introduction

The objective of the second case study is to evaluate the usefulness of the first implementation of the three-level risk-assessment approach and that of PHA and HAZOP methods, as used at the time of the assignment, in a complex automated mining-machine application in the early phases of its life cycle.

The mining-machine manufacturer (sometimes referred to below simply as 'the manufacturer' or 'the system supplier') was developing an automated ore loading and transportation system concept for underground mines. In 2000–2001, VTT conducted an assignment with the machine manufacturer aimed at analysis of potential automation-related safety risks and to specify safety requirements for the automated work-machine system concept. In the system concept, LHDs and dump trucks tram and navigate autonomously in the tunnels of an underground mine. Hauling and dumping are automatic. The buckets of LHDs are filled by tele-operation from a control room. The autonomous fleet is designed to operate in a restricted area on the production level in an underground mine, and access to the automated area is prevented while the system is in its automatic operation mode. The system concept was composed of the following subsystems (for a diagram, see Figure 24):

- A production-control system, for planning, optimisation of production execution, and understanding of production inputs and outputs
- The mission-control system, a supervisory system controlling and monitoring the autonomous operations, including traffic management and provision of the remote operator's user interface
- A broadband, high-speed data/video communication system for connectivity to automated underground LHDs and trucks
- On-board machine control, monitoring, and navigation systems
- A safety system, for isolating the operation area during autonomous operation and controlling access to the area.

Figure 24. A block diagram of the system concept in the case under study, with the time dimension shown (Sandvik). Reprinted with permission from Sandvik Mining and Construction.

The assignment included several risk-analysis tasks, covering the whole automation system concept and all of its subsystems. Three analyses have been selected for this case study, representing all three levels of risk analysis in the three-level approach to risk assessment. The first, the overall system risk analysis looking at potential hazards and safety risks in the automated LHD production area, was conducted as an application of PHA methodology. The second is upper-system-level risk analysis of system operations and related system functions, which was conducted with HAZOP methods. Finally, the lower-system-level risk analysis for the on-board control system was also conducted via HAZOP methods.

This case study addresses the following research questions:

- How suitable is PHA for work-site-level hazard identification and risk analysis in the conceptual design phase?
- How well suited is the simplified risk-estimation methodology to the risk estimation at different levels of risk assessment?
- How appropriate is the HAZOP method for risk analysis of system-operation and system-function concepts?
- How well does the HAZOP method suit risk analysis of machine on-board control function designs?
- How well does the three-level risk-assessment approach applied at the time fit the risk assessment of an automated ore-transportation system in its conceptual design phase?
- What are the benefits and impacts of the risk-assessment work in this case and more generally in the companies?

6.2 Implementation of the three-level risk-assessment approach

6.2.1 PHA of the automated ore-transportation concept

The objective of the PHA in this case was systematic identification of potential automation-related hazards in the various phases in the life cycle of an automated production area using LHDs or dump trucks; estimation of safety risks; and description of the safety measures necessary at a conceptual level for elimination, reduction, or control of the risks.

The scope of this overall system risk analysis was defined to cover the whole life cycle of an automated LHD production area and all of the main operations related to these phases in the life cycle. The intended use (both manual and automatic) of the machines, work procedures, communication between the control room and the production area, and regular daily maintenance of the machine were taken into consideration during the analysis. The phases in the life cycle of a production area were defined for purposes of this analysis as follows:

- System start-up
- Connection of LHDs to the system
- Production
- Maintenance work in the production area
- Partial production breaks or complete shutdowns of the automation system
- Disconnection of the automation system from the production area.

Thirty distinct system operations were identified from the system-overview description and system-requirement specification. Identification of automation-related hazards and hazardous events followed the same PHA method used with the previous mining-company case (Case 1). The brainstorming and scenario analyses were conducted informally in team discussion. The hazards identified and descriptions of potential hazardous events were projected onto a wall for discussion. The analysis results for each system operation – hazards, causes, consequences, estimated risk levels, descriptions of existing safety measures, and proposals for additional safety measures – were recorded in a table on a PHA worksheet.

The risk estimation followed the same three-level estimation method used in the PHA analysis in the mining-company case described in the previous chapter of the thesis. Severity levels were indicated with the values 3, for ‘severe’ (fatality or permanent injury), 2 for ‘significant’ (reportable injury), and 1 for ‘insignificant’ (slight or no injury). Probability levels were indicated with the value 3, for ‘probable’ (situations that can occur in normal operation); 2, for ‘improbable’ (risks that can be realised only in certain conditions); and 1, for ‘rare’ (eventualities that are unlikely in any conditions). The risk estimation took into account the hazards or hazardous events that could arise in the absence of any safety measures. Risk was assigned one of three levels, as was described for Case 1 (Table 1).

The PHA team established for this assignment had four one-day analysis meetings in Tampere. The analysis team was composed of four experts from the manufacturer, representing both underground-mining and mining-automation knowledge, and two researchers from VTT. At least two of the manufacturer's experts and one researcher from VTT took part in every one of the meetings. The author of this thesis led the sessions and documented the results. The PHA approach was new to the manufacturer's experts in the team. Some of them had taken part in manual machines' risk analyses, using checklists, and some had worked in machine-control system risk analysis using FMEA. The PHA methods and risk-analysis work practice were introduced to the team before work began.

As output of the PHA, 74 hazards or hazardous events were identified. Among them were the following items:

- Someone being in the production area when automatic operation starts
- Unexpected machine movements during connection of subsystems
- An unexpected change in production-area conditions that affects automatic operation
- The safety system in the production area not being ready when the route testing begins.

The risk level was estimated at 3 or higher for 49 of them, meaning that they had to be eliminated or the risks reduced to an acceptable level. The PHA team then performed risk evaluation considering the conceptual safety measures already planned, such as the primary safeguarding system for isolation of the autonomous operation area and to control access to the area, conceptual system-level safety features, and common safety principles and instructions for underground mining work introduced by the manufacturer's experts. The analysis team created 41 proposals for new safety measures, with the following among them:

- If route teaching and testing must be done before the production-area safety system is ready, additional safety instruction and safeguarding arrangements are needed, to prevent access to the tunnels where the LHD is moving.
- Radio communication between the test driver of the LHD and other personnel in the area must be ensured.
- Specific instructions should be prepared for system start-up after servicing, to eliminate hazards caused by faulty connections etc.
- The production-area safety system must be designed in account of all system-operation situations.
- New operators should be trained to predict changes in the mine environment, especially at draw points.

Proposals were considered in line with the three-step risk-reduction approach presented for Case 1, referred to as the 'principles of safety integration'. These

were based on the Machinery Directive as valid at the time, Directive 98/37/EC (1998), and on the basic machinery-safety design standard, then EN 292-1 (1995). Experiences and results of a simultaneously conducted mining-company assignment and the above-mentioned machinery-safety standard were used as references for the specification of the safety requirements. The Machinery Directive's main health and safety requirements were considered references for the minimum safety requirements. Corresponding references today are Directive 2006/42/EC (2006) and SFS EN ISO 12100 (2010). Also in this assignment, the analysis results were linked to the relevant points stated for the essential health and safety requirements in the Machinery Directive for the overall conformity assessment. The results were then forwarded to the R&D management of the company for further evaluation.

6.2.2 HAZOP study of system operations and system functions

The objective in the HAZOP study of system operations and related system functions was to ensure that possible deviations (human errors or technical problems) in the designed system operations conducted in the control room do not cause safety risks in the automated production area. The scope of this HAZOP study was the 'control-room systems', including the 'operator stations' and the 'mission-control system' (see Figure 21). The analysis was conducted in two phases. In the first, operator stations were analysed by a team composed of three automation experts from the machine manufacturer and two researchers from VTT. The team had two full-day meetings. The author of this thesis participated in both meetings, led the analysis, and documented the results. As a starting point, the analysis team specified the system operations in accordance with the system specifications. Among the system operations under study were the following:

- Starting and stopping of the automation system
- Route management
- Operation of LHDs in various operation modes
- Changing of the operation mode
- Tele-operation.

In the first phase of the upper-system-level HAZOP study, the team identified deviations from the designed operator work tasks and functions at operator stations, analysed the possible causes and consequences, and evaluated their criticality to safe system operation. The above-mentioned guide words from IEC 61882 (2001) ('no', 'less', 'more', 'as well as', 'other than', 'part of', 'reverse', 'before', 'after', 'early', and 'late') were applied to support identification. In this study, technical hardware failure, software failure, and operator error and mistakes were considered possible causes of deviations. The risk estimation involved a three-category matrix for risk elements, showing severity and probability (Table 2). The analysis team estimated the consequences without any safeguards. If several consequences of a deviation were identified, the probability of the hazardous

event was estimated with the deviation occurring and the most serious consequence arising (the worst case), regardless of the safeguards in place. After that, the safeguards designed to prevent said deviation or reduce the consequences were listed. If the safeguard was seen as sufficient, no corrective action was proposed; otherwise, further corrective actions were recommended.

Table 2. Categories of risk elements, with related examples.

Element	Value	Examples
Severity	3: Serious	Serious injury and collision by driving into, for example, the wall
	2: Significant	Collision and minor injury caused by sudden stopping of the machine and machine damage necessitating repairs
	1: Insignificant	Excessive wear to machine components and production losses (e.g., non-optimal production)
Probability	3: Probable	Cable or connector faults
	2: Unlikely	Software failures
	1: Rare	CAN 'residual error'

Results were documented into a HAZOP worksheet. In the analysis, 26 deviations were identified. Two of them were considered safety-critical (i.e., of risk level 3 or higher). The analysis team evaluated the risks and defined 13 proposals for corrective actions.

In the second phase of the upper-system-level HAZOP study, another team focused on possible deviations in system functions. This team was composed of two automation experts with the machine manufacturer, one automation expert from that manufacturer's subcontractor, and the author of this thesis (from VTT). The analysis team had five full-day meetings, with the author participating in all of them, leading the analysis, and documenting the results. The team specified the system functions in view of system specifications. The functions studied include the following:

- Mission assignment
- Mission execution
- Traffic control
- Condition monitoring.

The team identified deviations from the designed system functions, analysed their possible causes and consequences, and evaluated their criticality to safe system operation. The list of guide words from the standard IEC 61882 (ibid.) was applied as in previous HAZOP studies, to support the identification of deviations. Also in this study, both technical and human-factor-based causes were considered. The team identified 78 deviations in the analysis, with the following among them:

- The operator making a control error while in tele-operation mode

- Misinterpretation of system information leading to inappropriate actions
- Faulty system information leading to inappropriate operator actions
- Incorrect automatic function occurring because of a hardware failure.

The risk estimation used the same three-category risk matrix for risk elements, severity and probability, employed in the first phase (see Table 2). Twenty safety-critical deviations (risk level 3 or higher) were found. The result of the risk evaluation was 38 proposals for new safety requirements and corrective actions for the design. These included the following:

- There should be instructions to check the production-area map before it may be used for production.
- The operator should regularly test all the functions at the operator stations.
- There should be a machine ID visible in the video picture.
- Automatically activated machine stopping should be reported to the operator.

The machinery-safety standards of the time, such as EN 292-2, ISO 13849-1, IEC 61508, and EN 60204-1, were used as guidelines and references in the evaluation of the designed functional safety principles and specification of safety requirements and corrective actions. In the end, the requirement-specification table drawn up in view of the essential health and safety requirements was amended to consider the HAZOP results. These were then forwarded to the company's R&D management for further evaluation.

6.2.3 HAZOP study of the on-board control system

The objective of the lower-system-level HAZOP study was to identify possible functionality deviations in the on-board control systems, analyse the effects on machine operation, and specify the safety measures necessary for ensuring safe operation in both automatic and manual operation. The system under study was an integrated, distributed machine-control system consisting of several control and I/O modules, connected via CAN bus.

At the outset, all of the machine-control-system functions were identified on the basis of the system specifications, and 22 of them were selected for analysis. The functions under study were the following, among others:

- Motor start and stop
- Steering
- Braking
- Emergency stop
- Normal stop
- Selection of the machine operation mode.

Experiences from use of function-level drawings of the on-board control system in the HAZOP study performed with the mining company led VTT to compile function-specific drawings also in this case, to support the analysis (see Figure 25).

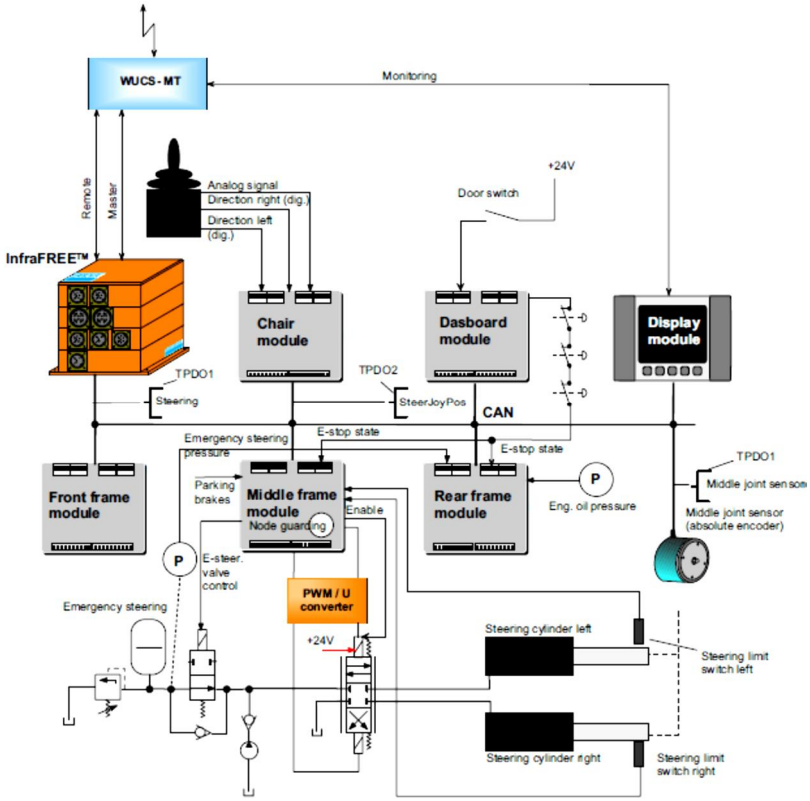


Figure 25. An example of the function-specific drawing format used. Figure used with permission from Sandvik Mining and Construction.

The identification and analysis of deviations were started at the signal level; i.e., for each I/O signal pertaining to a function, all relevant deviations were assessed (for example, 'Steering joystick analogue signal too high'). However, it soon became apparent that, in this case, signal-level analysis was too laborious to be accomplished within the required timeframe. Hence, the analysis team decided to continue the analysis at a higher function level (for example, 'Gear is set higher than requested' or 'Gear is set lower than requested'). The results from the analysis sessions were recorded on HAZOP worksheets, and reports were presented as Word documents. The tables generated included the functions and their design intent, subsidiary functions, a list of deviations, the causes and consequences of the deviations, and descriptions of ways to detect and safeguard against each deviation or its consequences in the implementation designed.

The risks were estimated with the same three-category risk matrix as previously in this case. The analysis team estimated the consequences without any safeguards. After that, the safeguards implemented to prevent such deviation or reduce the consequences were listed. The probability of the hazardous event was

then estimated on the assumption of the deviation occurring and the most serious consequence arising in spite of the safeguards implemented. Risk evaluation in this case meant that if the safeguard was regarded to be sufficient, no corrective action was proposed; otherwise, additional corrective actions were recommended.

The HAZOP team was composed of three experts from the machine manufacturer, three experts with the machine manufacturer's subcontractor, and three researchers from VTT. The analysis team held 13 full-day or half-day meetings. The core team taking part in all of the meetings consisted of two experts from the machine manufacturer and one researcher from VTT. Others took part in one or two meetings. The author of this thesis participated in two of the meetings.

The analysis team identified 441 deviations in functions or in signals. These included the following items:

- The motor starting unexpectedly
- A switch in machine mode to remote mode instead of manual mode
- The gear being set higher than what the operator selected
- The speed (in rpm) being too high
- Steering being too great on the left
- The brakes not working effectively
- The motor stopping unexpectedly.

The team estimated the risk level as 3 or higher for 133 deviations. The standards of the time ISO 13849-1, IEC 61508, and EN 60204-1 were used as guidance and references for the evaluation of the designed functional safety principles and specification of safety requirements and of corrective actions for the on-board control system. The HAZOP team determined 140 proposals for design requirements or instructions. These included the following items:

- Fixed limits for safety-related parameters
- Control feedback signals and feedback diagnostics
- Feasibility tests to detect abnormal combinations of enabling signals
- Validity times for safety-critical messages
- User instructions for calibration
- User instructions for regular checking of safety functions
- A log file to record parameter changes.

The conformity assessment table prepared in line with the key health and safety requirements was amended to feature these results. The results were then forwarded to the R&D management of the company for further evaluation.

6.2.4 Requirement specifications for safety-related functions

One of the main objectives in this assignment was to specify requirements for the safety-related functions of the automated mobile work-machine system. From the technical point of view, the focus in safety-requirement specification was on specifying requirements for the primary and independent safeguarding system, which isolates the

automated area, and on functional safety requirements for the safety-critical functions, which were identified in the automated mobile work-machine concept (see Figure 26).

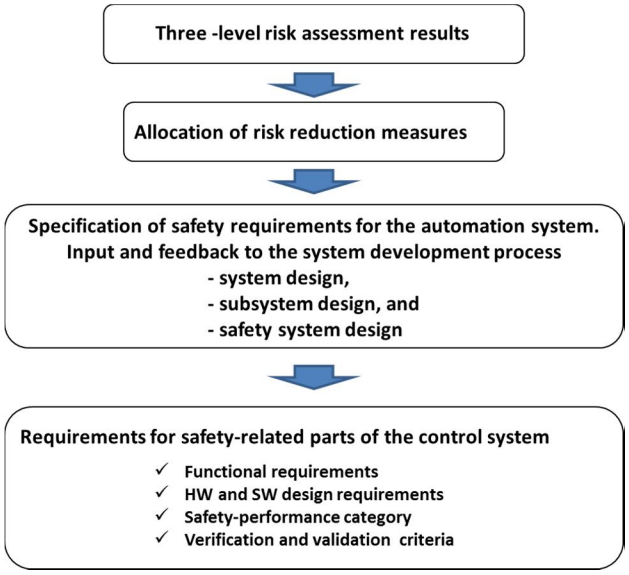


Figure 26. Simplified procedure used for the specification of functionality-related safety requirements.

The reference standard used at the time, ISO 13849-1 (which has since been replaced by SFS EN ISO 13849-1:2007), defined five 'safety performance categories' for safety-related control functions, as follows:

- B: The occurrence of a fault can lead to loss of the safety function.
- 1: The occurrence of a fault can lead to loss of the safety function, but the probability of occurrence is lower than for category B.
- 2: The occurrence of a fault can lead to loss of the safety function between checks. Loss of the safety function is detected by a check.
- 3: When a single fault occurs, the safety function is always performed. Some but not all faults will be detected. Accumulation of undetected faults can lead to loss of the safety function.
- 4: When a fault occurs, the safety function is always performed. Faults will be detected in time to prevent loss of the safety function.

For categories B and 1, the principles for achieving safety were characterised mainly by selection of components and good design and implementation practices. For categories 2, 3, and 4, the safety principles were characterised chiefly by system-architecture and active failure-detection methods.

The functional safety requirement specification – in other words, categorisation of the safety-related functions identified in the PHA and HAZOP studies in terms of these safety-performance levels – was performed with the highest risk level estimated for a dangerous deviation of the function considered first, then all other identified and available safety measures that are related to risk reduction for the safety-critical deviations in that function. Finally, the amount of risk reduction assigned for the safety-related function determined the performance category for the function.

6.3 Experiences, comments, and observations

6.3.1 Experiences and feedback from the company

Direct feedback and comments on the risk-analysis methods and their usefulness were received from the manufacturer's experts during the project. In addition, a questionnaire was sent by e-mail to the manufacturer's experts soon after the assignment's completion in 2001. The experts involved in the risk analyses and risk-evaluation sessions were asked about the benefits of the risk-assessment approach, the risk-analysis methods, their experiences of the work, pros and cons of the assignment in general, and the co-operation. The five (out of seven) experts responding to the questionnaire represented automation design, control-system design, underground mining expertise, and safety-engineering expertise.

According to the comments and the responses to the questionnaire, the most important results of the assignment had been the knowledge of the present level of safety of the conceptual design for the automated ore-transportation system and an estimate of the amount of work required for bringing the risks related to the operational and functional concepts to the required, acceptable level. The manufacturer's experts indicated that the co-operation among system designers, subcontractors' experts, and VTT's experts had been frank and open. The work proceeded effectively, and all participants were motivated regardless of their heavy workload. The project was considered to be a good learning process. One of the manufacturer's automation experts expressed his experiences thus: 'It was valuable to join the project. I learned a new way of thinking, which means that you think about safety issues in a more systematic way when you are defining new concepts and developing new ideas.'

The manufacturer's experts emphasised that the systematic analyses of the entire automation system concept helped them to understand subsystem functions and interrelations among individual subsystems. Reports and subsystem-analysis documents formed a good baseline for the technical construction file for the automated ore-transportation concept, for presentation and specification of safety principles and measures used to eliminate and control safety risks. They also expressed that the HAZOP studies highlighted many important system characteristics, system features, and improvement possibilities beyond the safety-related realm that could be used to improve the functionality, usability, and reliability of the system. They also pointed out that most of the results were directly transferable to the

mine-automation development team, to be considered in the system-development work. The documented approach and analysis methods were directly applicable in new research and development projects and in automation-system analysis.

When questions were asked about proposals for improvements to the risk-analysis approach and its methods, the answers raised the following issues:

- There should have been more time and resources for development of the methodology and analysis tools before the first analysis sessions. In particular, the HAZOP method was not so familiar to all participants, including VTT's experts, and this caused inefficiency in the first analysis sessions.
- The analysis methods turned out to be applicable and efficient after they had been adapted for this particular risk-analysis purpose at hand and practised in the first analysis sessions.
- The precision or level of the analyses and the analysis reports was not clear at first. In the HAZOP studies, it was not so easy to determine the level of deviations, failures, or hazards that should be identified and analysed. Also, the levels of consequences should have been defined more accurately. The reports from the subsystem analysis were not consistent with each other, and this created extra work in later interpretation of the results.
- The risk analyses should have been linked better to each other: the upper-level analysis results could have been better utilised in the more detailed analysis.
- The analysis sessions should be planned such that the right resources and the expertise needed in the session in question are present. Optimal use of the limited expert resources is important and improves motivation for the work.

Three of the manufacturer's experts were interviewed for this thesis in March 2012 (see Subsection 3.3.2). According to the manufacturer's experts, this risk-analysis project in the conceptual design phase for the new autonomous ore-transportation concept and the simultaneous joint risk-analysis project at the LKAB Kiruna mine was the beginning of system-safety thinking in the manufacturer's mine-automation system-development team. The experts confirmed that the main automation-related risks were identified and analysed in the time of the assignment, and the results and knowledge have been utilised in system development and in customer applications and passed down via system-update reviews to this day. They also expressed that the system-safety decisions made at the time seem to have been right. No accidents or near-miss situations related to overrun or crushing hazards in automated ore-transportation systems have been reported to the manufacturer. Applications have been operating since 2004.

The manufacturer's experts emphasised that, even though risk-analysis documentation always features shortcomings and some lack of clarity and the reference standards in effect at the time of the assignment have been updated since, the conceptual baseline for system-safety decisions has been valuable and useful. Documented risk analysis and traceability of the risk-evaluation decisions from the

early conceptual design phase have been valuable for the latter system development, customer-application system design, and selection of safety measures but also in the system's conformity evaluation.

6.3.2 Observations

The PHA analysis at the overall system level proceeded systematically in line with the general underground ore-transportation process description and system-operation descriptions for the automation and with the aid of numerous conceptual production-area-layout sketches. Experience from the earlier mining-company case served as a good reference for the analysis and was essential when the author led the PHA sessions, because there was so little knowledge of underground mining in general at the time. In all, 74 hazards were identified and 41 proposals for safety measures were generated.

The use of the simple three-category method (with 3 × 3 matrices) and the documentation practice brought out three problems in risk estimation. The first issue, related to the simple multiplication of the numbers representing severity and probability levels, has already been discussed (in the material on Case study 1). The second issue that led to confusion in the risk estimation was that the personal-safety and other consequences, such as material damage, production loss, and impact on the operation environment, were not clearly separated in the documentation. The third issue was that the acceptability of the remaining risk was discussed in the team in account of the planned safety measures and proposed additional measures while the residual risk level was not documented.

Difficulties in defining hazards and hazardous events for a relevant and appropriate functional and system-hierarchy level such as system operation, system function, operation mode, and control function were observed during the analysis work. These system characteristics should have been defined and specified more clearly and used consistently throughout the analysis. This shortcoming led the analysis team to analyse some of the same hazards and hazardous events in the PHA and in the upper-system-level HAZOP study, which was not the purpose with this approach to risk analysis. On the other hand, 104 hazards were identified, in total, in the upper-system-level HAZOP studies, and 51 proposals for safety measures were generated. From the standpoint of safety engineering, there being little overlap between the results of various analysis methods is not a problem; in another sense, it confirms the analysis findings. The author's observations verify the presence of an issue identified by the manufacturer's experts, that the PHA results should have been better utilised and tied into the later upper- and lower-system-level HAZOP studies.

The lower-system-level HAZOP study of the on-board control system faced methodology problems. The level of resolution in the HAZOP study was changed quite soon after the first analysis sessions. The analysis at signal level turned out to be too laborious for this purpose and for the resources available for the analysis. However, it was concluded in this case that a function-level study would reveal

the relevant safety-related consequences just as well as a signal-based study. Also, at the same time, if the signal-based analysis is not done very carefully, the analysis team could miss some of the consequences for the functions. The signal-based analysis could, however, reveal unexpected behaviour of the machine, such as jerky or bouncing driving, that is not described in the function specification. Better coverage of possible deviations could have been gained through application of both signal- and function-based studies, but only one of the two could be selected in practice. In this case, most of the analysis was done at the function level, but some selected functions were analysed in more detail with signal-based analysis. In the end, the lower-system-level HAZOP team was effective and noted, in all, 441 deviations, generating 41 proposals for safety measures.

The main objectives of the risk analyses in this case were to specify the safety requirements for the automated ore-transportation system concept and to evaluate the baseline solutions designed. One important part of the overall safety-requirement specification was the functional safety requirements for the safety-related parts of the automation system and on-board control system. Requirement specification for the safety system designed for isolating the operation area during autonomous operation and controlling access to the area turned out to be quite a straightforward process. It proceeded from risk-analysis results to the functionality requirements and safety performance (PL) or safety integrity (SIL) requirements. The same was observed with regard to the on-board control system's requirement specification. Challenges and difficulties were faced in the specification of the functional and safety-performance requirements for the upper-system-level functions of the automation system. Evaluation of the monitoring and diagnostic possibilities, the related capabilities of the automation system, and the operators' ability to detect possible deviations and problems were discussed and examined a great deal during the analysis sessions.

It was also noticed that implementation of the three-step risk-reduction approach, the 'principles of safety integration', applied here in line with the machinery-safety design guidelines in EN 292-2 (1995), required a great deal of effort. Allocation of risk-reduction measures for inherent system functions, for external safety-related functions, for safety instructions, for warnings, and for system-operation development were new issues for the system designers. This clearly reflects the new challenges in concept definition and system-requirement specification for such complex machinery and simultaneously highlights the importance of a systematic approach applying operational and functional analysis perspectives to bring these aspects out even in the conceptual design and requirement analysis.

The risk analyses produced a large amount of information, which was not judged to be safety-critical and was more likely to be related to system availability, usability, subsystem and component reliability, or development possibilities for system functions and operation procedures. The analysis work in the assignment was focused on safety issues, so further actions and utilisation of this possibly valuable information for the system development were not included. According to the manufacturer's experts, the information was considered and forwarded to other processes in the company. In the author's experience, it is quite typical in the manu-

facturing industry for safety engineering and availability or reliability issues to be handled in several processes and by several people at the relevant company. This can lead to situations wherein important system-availability issues identified in the early concept phase may not be raised for review or decision-making. A reliability-engineering method may not bring these issues up either, since the methods and analysis perspectives are different. To be able to utilise this valuable information systematically, the company could establish and maintain an overall RAMS management process. The abbreviation 'RAMS' refers to reliability, availability, maintainability, and safety – that integrates system availability and system-safety information. There have been RAMS management programmes developed and standardised, for example, for safety-critical systems in railway networks (EN 50126-1, 1999; IEC 62278, 2002). RAMS management in early system development phases in machinery applications has been studied among others by Lundteigen et al. (2009), Jännes (2011) and Ahonen et al. (2012).

6.4 Discussion

The manufacturer developing a concept for an automated system for loading and transporting ore for underground mines became aware that traditional machinery-safety design practices and machine-level risk-analysis methods are not sufficient or practical for the analysis of an automated work-machine system that has several subsystems, communication networks, and automatic functions. The safety-engineering problem was how to analyse potential automation-related safety risks and to specify a safety-requirement baseline for the automated work-machine system concept.

The three-level risk-assessment approach including PHA and HAZOP methods was chosen to solve this problem. The results and experiences indicate that this approach was, at least at the time, well suited to risk assessment for an automated ore-transportation system in its conceptual design phase. These findings are in line with the recommendations for functional safety engineering of processor-controlled mining equipment introduced by Sammarco et al. (2001). The recommendations include, in all, nine reports, which were published in 2001–2006 by the United States National Institute for Occupational Safety and Health (NIOSH). Sammarco et al. (ibid., p. 1) recommend the use of PHA and HAZOP methods for risk analysis and the use of qualitative risk-estimation methodology for surface or underground mining systems employing embedded, networked, and/or non-networked programmable electronics. The system-safety solution described in the recommendations is a simplified safety-life-cycle version of the one introduced in IEC 61508 (1998), and it is emphasised that the safety life cycle needs to be tailored to each application. Sammarco and colleagues also point out that hazard identification and analysis must be applied over the full life cycle of the system and must start at the conceptual stage of the project and continue in an iterative manner (Sammarco et al. 2001, p. 4).

In PHA, the analysis of hazards related to the various phases in the system's life cycle in the 30 distinct system operations was carried out with brainstorming and team discussion methods similar to those used in the earlier mining-company case. The biggest difference was that in this case the team was composed mainly of automation experts who did not have extensive practical work experience in mining. While they did have a good general understanding of the underground mining conditions and were experts in the technology of the new automated ore-transportation concept, they did not possess the weight of extensive experience with work practices with traditional manual machines when creating totally new scenarios for automation-related hazardous events. Roland and Moriarty (1983, p. 197) have stated that the results of PHA are products of the analysis team's imagination, experience, and knowledge of the system and its operation environment. They also claim that there is no specific modelling method or logical process to ensure that all hazards are examined; therefore, experience and knowledge may play the most important role in PHA-type analysis (ibid., p. 198). Kuivanen (1995) studied methodology for simultaneous robot-system safety design, using several test subjects in his experimental study of hazard identification and risk assessment. System designers and researchers analysed the same system, using, separately, first a simulation model and then an existing robot application. Individual analysis and assessment results were then compared and analysed. Kuivanen concluded that risk assessment for the overall robot application gives only hints of the risks, not accurate values suitable for use as a basis for the design work. Qualitative risk assessment is too subjective, so group work too is needed in the risk-assessment phase (ibid., p. 131).

In the previous case (Case study 1), wherein the automation system was in use, the system-operation procedures were analysed on the basis of prevailing usage and the system functions were analysed in view of the implementation at that moment, which provided facts that could be checked or verified. In this case, the analysis of system operations was done in the requirement-specification phase in line with the available documentation and system designers' experiences and knowledge. The precision of the analysis depends strongly on the specificity of the available information and on the experts' knowledge of the system. That leads to the question of the level and amount of information needed for carrying out a valid and reliable analysis of operational or functional risks in an early phase in the system life cycle. According to Vincoli (2006), the documentation available should include, in addition to the existing descriptions of operation and maintenance procedure, at least operation-sequence diagrams, functional diagrams, equipment panels' layout, and the results of the preliminary hazard analysis (ibid., p. 96).

The HAZOP study focusing on system operations and related system functions was timely, supporting two separate purposes. The first part of the analysis was performed in the prototype phase for a new version of the operator station, and the analysis supported the prototype's testing. It can be considered an analytical verification of the prototype implementation. The second part of this HAZOP study was carried out in the phase of specification of system operations and of the subsystem controlling machine-fleet automation. The results were directly available in

the specification process, and the changes were made to the specifications 'on the fly'. Results and experiences in this case indicate that it is valuable to conduct the risk analysis of system operations and system functions as early as possible even though the operational and functional descriptions and specifications are still incomplete. This result supports the thinking seen in the system-safety literature, that it is best to conduct the analysis of operating hazards as early in the system life cycle as possible (ibid., p. 95; Stephenson 1991, p. 78; Roland and Moriarty 1983, p. 210). The systematic risk analysis supports the system specification, and the necessary changes can be made to the specifications easily.

Redmill, Chudleigh, and Catmur (1999) have studied HAZOP extensively from the system-safety perspective, also as a method to identify hazards in human-centred systems, where the human operator is critical or even central to system functionality or safety. They declare that HAZOP study is an effective way to identify hazards not only in technical systems but also in human-centred systems in looking at deviations from the design intent of the processes and tasks and in the information flowing between them. The HAZOP method can be used to explore humans' deviations from the design intent just as well as deviations on the part of the technical system. The interpretations of the guide words used must be modified to be appropriate for the human perspective (ibid., pp. 166–169). On the other hand, it was noticed during this project that system-safety guidelines propose a dedicated methodology, distinct from HAZOP study, called operating hazard analysis (OHA) (Roland and Moriarty 1983, pp. 209–210; Stephenson 1991, pp. 78–79), that would be more suitable for the identification and analysis of hazards connected with operation and maintenance procedures in the early system definition and development phases. According to Roland and Moriarty (1983, p. 209), OHA is an attempt to identify hazards resulting from tasks, activities, or operation of system functions. The analysis approach is similar to PHA but focuses the analysis on the level of operation events and activities.

The aim in the lower-system-level HAZOP study was to identify deviations that could have safety-critical consequences such as death or injury. For most individual deviations, several types of non-safety-critical consequences, among them machine damage, machine stoppage, and the system halting, were identified and recorded. The simplifications in the risk-estimation method caused difficulties in risks' evaluation and in specification of the safety measures, because the risk-estimation method did not separate the personal-safety risks from the risks related to material damage or production stoppages. Another notification of the analysis of the identified deviations was made with respect to the appropriate number of consequences versus one individual deviation. The HAZOP standard IEC 61882 (2001, p. 39) and also Redmill et al. (1999, p. 21) highlight that, when using risk estimation, one should determine the probability of occurrence for each of the possible consequences specified. This is a clear principle that supports the consistency and reliability of the analysis method. In practice, it readily increases the amount of work, depending on how many individual consequences are noted by the analysis team. The study leader has an important role in HAZOP studies, to

keep the analysis focused on the functions and conditions in question and to elicit the reasoning for any proposals and ideas offered.

6.5 Conclusions

The machine manufacturer's experiences and comments indicate that the risk-assessment approach can be considered valid and to have added value to the automated ore-transportation system's concept-development and verification work. The system designers stated that the project was a good learning process. Systematic analyses covering the entire automation-system concept aided in development of an understanding of subsystem functions and relations between individual subsystems. Also, reports and subsystem-analysis documents formed a good baseline for the technical construction file and for assessment of the system concept's conformity.

It can be assumed that the approach and methods applied supported the machine manufacturer in making the right system-safety decisions both at the time and later: no accidents or near-miss situations related to crushing hazards or to people or things being run over in automated ore-transportation systems have been reported to the manufacturer since the first application entered use, about a decade ago.

In view of the industrial partners' comments and the author's observations, PHA was found to be suitable analysis method for the automated mobile work-machine system's overall risk-assessment in its conceptual design phase. HAZOP study was found to be suitable analysis method for possible human errors or technical deviations in the designed system operations and upper system level functions. It can also be concluded that in this case the function-level HAZOP study revealed the most significant safety-related deviations in the on-board control system. It is appropriate to use signal based HAZOP study only to selected functions in which the more detailed information is essential.

Many methodological weaknesses and inaccuracies were recognised during the analysis sessions and the documentation process. The results of the case study point to a need for improvements in the risk-assessment approach and analysis methods with respect to the following issues, among others:

- Utilisation of higher-level analysis results and their linking to the more detailed analysis that follows
- Definitions of the analysis levels, hazards, deviations, and causes and consequences
- Isolation of personal-safety consequences and other consequences, such as physical damage or lost production
- Probability estimation in the risk-estimation process
- Evaluation of the residual risk.

Systematic analysis of system operations and system functions in PHA and HAZOP studies in the conceptual design phase brought out a large quantity of information that was related not to safety but to system availability, system usability, subsystem and component reliability, or other areas of development of system functionality and operation procedures. It can be concluded from these findings that also the results of system-safety-engineering tasks that are not safety-related should be considered in systems-engineering reviews, to avoid the loss of possibly important system-development information from early in the system life cycle. Integrated management of RAMS issues, also involving the reliability-engineering team, would be a good way of sharing and utilising this information.

7. Case study 3: The ore-transportation application

7.1 Introduction

The objective of Case study 3 is to evaluate the utility of the second implementation of the three-level risk-assessment approach and the usefulness of PHA, OHA and HAZOP methods. The target system in this case study is a complex automated mining-machine application in its system-specification and system-design phases.

The mining-machine manufacturer was delivering an automated ore-transportation system to an underground mine in South Africa. The mining company was building a new production level for the underground mine and had selected the automatic dump-truck solution for horizontal ore transportation to the crusher. In 2003–2004, VTT conducted a risk-assessment assignment with the system supplier. The automated ore-transportation system in question was unique – the first of its kind in the underground mining industry. The objectives of the assignment were to identify and analyse automation-related safety risks and case-specific safety factors, to specify safety requirements for the application, and to evaluate the necessary risk-reduction measures and assign them. The risk assessment covered the following phases in the customer application's life cycle: installation, testing, integration, commissioning, and operation and maintenance.

The target system uses autonomously operating dump trucks that transport ore from the transfer points (loading points) to the crusher pin (dump point). The main subsystems in this application are a production planning system, a mission-control system and operator stations at the surface control-room level, and automated dump trucks and the local safety system in the underground production area. A wireless communication system connects the machines to a mine-wide high-speed communication system. The autonomous dump trucks are loaded with manually operated LHDs at the transfer points. Isolation of the automated production area and an access-control system had been specified in the primary safeguarding principles for use in automatic operation (Burger 2006, p. 555) (see Figures 27 and 28).

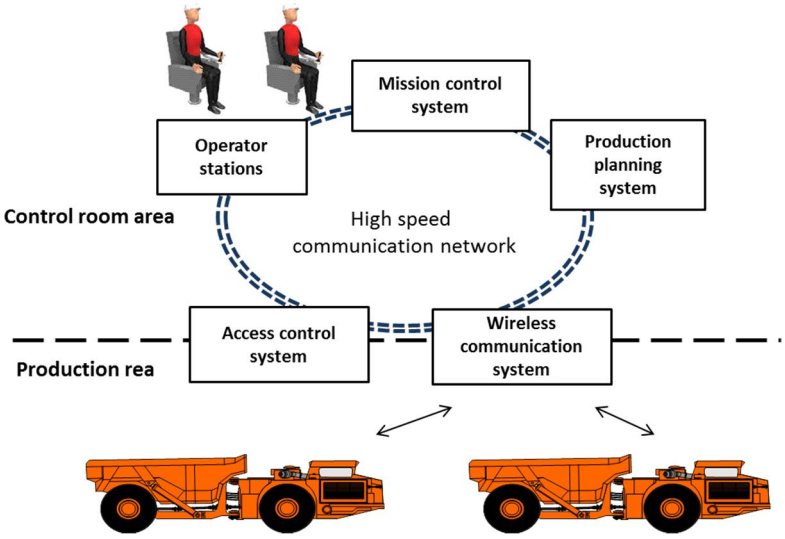


Figure 27. A simplified block diagram for the ore-transportation system under study, modified from the work of Burger (2006, p. 558).

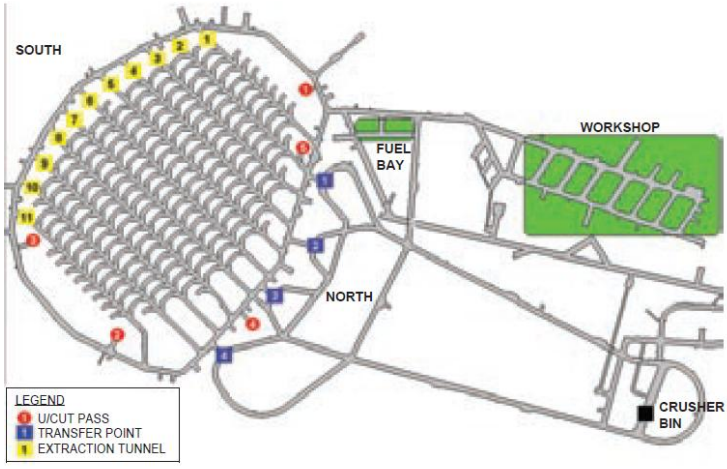


Figure 28. An overall view of production level 630, where the ore-transportation system under study was implemented. Grey lines are underground tunnels. (Burger 2006, p. 554.)

The three-level risk-assessment approach including PHA, HAZOP, and OHA methods and a 5 × 5 risk matrix for risk estimation were applied in this assignment. The case study addresses the following research questions:

- How well suited is PHA to work-site-level hazard identification and risk analysis in the system-specification and system-design phases?
- How suitable is the HAZOP method for risk analysis for the safety-system use cases?
- How appropriate is the OHA method for the upper-system-level risk analysis of system operations?
- How well suited is the risk-estimation methodology to risk estimation at the various levels of the system?
- How well does the three-level risk-assessment approach applied at the time fit the risk assessment of an automated ore-transportation system in its system-specification and system-design phases?
- What are the benefits and impacts of the risk-assessment work in this case and more generally in the companies?

7.2 Implementation of the three-level risk-assessment approach

7.2.1 Implementation and results of the PHA

The objectives of the PHA in this case were to identify potential hazards and hazardous events involving the autonomous ore-transportation system in the underground mine systematically, to estimate the risks, and to assess the safety measures necessary in this particular application. The PHA started with a kick-off meeting in South Africa. Present were the mine-safety officer, the local mine-safety consultant, the safety expert of the system supplier responsible for the system safety on the site, and the author of this thesis for VTT. The available materials were reviewed – among other resources, the mine-specific safety instructions for underground work, local safety regulations, special safety instructions for the use of mobile work machines in the mine, and descriptions of the production and maintenance instructions for the production level. Also, the previous, higher-level risk analysis, conducted for the development of the new underground production level, was reviewed and used as background information for the PHA. The scope for the PHA was specified and limited to the following:

- The *system life-cycle stages* under study were system integration and testing, the system's commissioning phase, production use of the system, and system decommissioning.
- The *system's operating environment* covered the LHD production area, the truck haulage area, the workshop area, the draw points, the transfer points, the crusher bin, the fuel bay, and related tunnels at the 630 level.

- *Activities in the production process* such as loading, hauling, drilling, blasting, development, maintenance, repairs, and secondary breaking were considered.
- *Personnel working in the production area* or visiting it in this case included system operators, machine drivers, drillers, subcontractors, cleaners, service personnel, repair workers, construction workers, managers, and geologists.
- The *machinery* in this case included dump trucks, LHDs, service cars, drilling equipment, and other mine vehicles.

The experiences and results from the earlier automated mining-machinery cases (Case studies 1 and 2) were available in this case and were taken as a baseline for hazard identification. The documentation available consists of the system's specifications, descriptions of its operation and maintenance concepts, and production-area layout drawings. Factors such as underground operating conditions, machinery, equipment, materials, human factors, ergonomics, failures, external systems, unexpected problems with utility systems, and unusual events in the area were used as a checklist to support the identification of hazards and hazardous events in the underground production area. A new feature for this analysis was separate analysis of the effects on personal safety and other possible effects on machinery or production-area infrastructure.

In this case, the risk estimation was done in a new way – in two phases: firstly, without any safety measures and, secondly, in light of the existing, planned, and proposed safety measures. Firstly, the severity of the consequences and the likelihood of the harm were estimated in the scenario of the automated system and its environment without any specific risk-reduction measures. The analysis looked at general safety rules and safety instructions for the mine – such as rules for personal protective equipment, requirements for machine visibility, rules on manual machines' traffic, and underground mining job-safety instructions. Secondly, the risk-reduction measures designed and built into the system concept by the system supplier were recorded. Needs for additional site- and application-specific risk-reduction measures were examined and proposed with respect to both the system supplier's actions and the mining company's actions.

The risk-estimation methods for PHA had been developed in consideration of the available risk-assessment and risk-analysis standards SFS IEC 60300-3-9 (2000) and ISO 14121 (1999), the latter now replaced with SFS EN ISO 12100 (2010). The probability of the harm and the severity of the consequences were estimated, with a scheme involving five categories, and the final rating of risk level employed three categories: low, medium, and high risk (see Tables 3, 4, and 5). To assist in the probability estimation, the categories were concretised with the following hints:

- 1 = Definite — harm occurs continuously when the system is operated in the manner specified
- 2 = Very possible — harm can easily occur in normal operation conditions
- 3 = Possible — harm can occur in normal operating conditions

- 4 = Remotely possible — harm can occur only in certain operation conditions
- 5 = Very unlikely — harm can occur only if several errors or failures occur at the same time.

The severity of the personal-safety consequences and physical damage or loss of production was estimated with the aid of the following hints, which were adapted from the internal risk-assessment guidelines used by the mining company:

- 1 = Multiple-fatality — death of more than one person
- 2 = Fatality — one person dying or being paralysed
- 3 = Reportable injury — one person being seriously injured
- 4 = Lost-time injury — one person being injured (> 3 days' absence)
- 5 = Minor or no injury — a maximum of 3 days' absence
- 1 = Permanent damage — catastrophic damage to the production area
- 2 = Multiple damage items — reparable damage to machinery and infrastructure
- 3 = Major cost implications — reparable damage to a machine or loss of production over several shifts
- 4 = Loss of time/availability — the system being out of use during one shift
- 5 = Minor or no implications — unexpected stopping of the system.

Table 3. Risk rating matrix for estimation of risks to personal safety.

	Probability				
Severity	Definitely A	Very possible B	Possible C	Remotely possible D	Very unlikely E
Multiple-fatality 1	1	2	4	7	11
Fatality/paralysis 2	3	5	8	12	16
Reportable injury 3	6	9	13	17	20
Lost-time injury 4	10	14	18	21	23
Minor/no-loss injury 5	15	19	22	24	25

Table 4. Risk rating matrix for estimation of material damage and production losses.

	Probability				
Severity	Definitely A	Very possible B	Possible C	Remotely possible D	Very unlikely E
Permanent damage 1	1	2	4	7	11
Multiple elements of damage 2	3	5	8	12	16
Major cost implications 3	6	9	13	17	20
Lost time or production 4	10	14	18	21	23
Minor or no cost implications 5	15	19	22	24	25

Table 5. Risk levels and indication of the necessary corrective actions

Risk level	Risk rating	Actions
High	1–6	Measures must be taken immediately to make changes in the system. The risk must be reduced.
Medium	7–15	Measures must be taken to develop the system with regard to the issue at hand. The risk must be reduced.
Low	16–25	There should be a plan for developing the system.

The PHA team was composed of four system experts from the system supplier, the safety officer from the mine, a local mine-safety consultant, and two researchers from VTT. Introductions to the risk-analysis practices and methods used by the mining company and the methods to be used in this case were given to the team at the kick-off meeting in South Africa. In this case, it was not possible to organise the PHA sessions such that all interested parties from the system supplier and with the mining company could have participated. The analysis work had to be adapted to the main project schedule and the availability of the system experts and mine representatives. The solution was for the hazard-identification and risk-estimation work to be done gradually.

In the first phase, two research scientists from VTT prepared a draft version of certain parts of the analysis. The PHA worksheet was developed into the form shown in Appendix 3. In the second phase, the results were reviewed and fleshed out in collaboration with the system supplier's experts at review meetings in Finland. Then, this process was repeated in three iterations. In all, VTT used five full-day analysis sessions to prepare the analysis. One review meeting was held in South Africa. Present at that meeting were the mine-safety officer, the safety ex-

pert of the system supplier, and two researchers from VTT. To obtain practical information and a general overview of the underground conditions on the site, a visit to the underground mine was organised within one project meeting in South Africa. The author of this thesis took part in the visit to the underground production level, which was under construction at the time.

As output of the preliminary hazard analysis, 69 automation-related hazards or hazardous events were identified, among them the following items:

- People enter a tunnel where a test driver is driving the dump truck manually.
- People enter a tunnel where a machine is moving autonomously during system commissioning.
- The wrong machine is selected for tele-operation during system integration and testing.
- Service workers are performing repair work in the restricted area when automatic operation starts.

In all, 134 consequences were defined, 81 of them affecting personal safety. The risk-estimation results included 22 of them being assigned 'high' level, 57 'medium' level, and two 'low' level. In 53 cases, the consequences were deemed to affect the availability of the machinery or influence production volume.

The risk evaluation in the PHA team took into account the safety measures already in place and the safety functions specified for the automated ore-transportation system concept and then considered needs for mine- and machinery-system-specific safety measures. The three-step risk-reduction principle adopted in view of the machinery-safety standard of the time (EN 292-1, 1995), and the Machinery Directive of the time (Directive 98/37/EC, 1998), was amended to include the ideas in the *system-safety precedence sequence* described by Stephenson (1991, p. 11) and by Roland and Moriarty (1983, p. 39). The purpose was to extend the risk evaluation by taking into consideration both the system supplier's and the mining company's risk-reduction opportunities and responsibilities. According to Stephenson (1991, p. 11), the system-safety precedence sequence includes the following steps:

- Design for minimal hazard
- Provide safety devices
- Provide warning devices
- Exert control through procedures and training
- Assess the remaining hazards.

The PHA team created 72 proposals for safety measures, of which 27 were technical requirements for the primary safety functions or for other safety-related functions. In total, 45 proposals were made, both for specific safety instructions for the operators' working in the control room and miners in the automated production area and for general safety instructions for the miners working at the production level near the automated production area. The proposals' foci included these:

- Risks related to the commissioning stage

- Operation and support procedures, system-level training, and instructions
- Operation modes and operation-area status changes
- Safety-critical information that need to be shared by subsystems and operation groups
- Traffic control in the production area
- Troubleshooting and support within the automated area
- System-level modification management.

The risk evaluation for the situation after the proposed risk-reduction measures uncovered 56 'medium' risks and 25 'low' risks. All 'high' risks could be reduced to medium or low level. The number of medium-level risks remaining derives mainly from the philosophy behind the risk-matrix method. The matrix is created such that the highest severity category 1, 'multiple-fatality', leads to a designation of medium risk level even if the probability category is estimated to be E, 'very unlikely', after all risk-reduction measures. This is the case, for instance, with machine fire situations or collisions with a service vehicle. The PHA report was delivered to the customer in accordance with the terms of the assignment.

7.2.2 Implementation and results of the HAZOP study

The primary safeguarding principle for ensuring the safety of personnel in the production area in the automated ore-transportation concept is the area's isolation with fences, gates, and safety devices. The safety system prevents personnel accessing the automated area while automatic operation is in progress, prevents uncontrolled machine exit from the automated production area, and allows machine transfer into and out of the automated production area (see Figure 29) (Burger 2006, p. 559).

The aim of the HAZOP study was to identify safety-critical deviations (both human errors and technical failures) in the specified operation situations of the safety system, estimate the risks, and evaluate the safety measures designed. The analysis was done in the system-design phase of the safety system. Hazards' identification and risk-estimation work were performed first by two researchers at VTT, one of them the author of this thesis. The analysis results were reviewed, and risk evaluation was done in three meetings by a HAZOP group that comprised a system designer from the safety-system supplier, an automation expert from the system supplier, and two researchers from VTT.

The HAZOP method had been developed since the first two system-safety projects (covered in Case studies 1 and 2) to follow the IEC 61882 (2001) standard's guidelines more precisely. One specific change was to describe the operation procedure under study in terms of what is termed *design intent.* The design intent (ibid., p. 41) of the operation procedure was stated in the form of a simplified *use-case description* wherein operator actions and the safety system's responses, opera-

tions, and state transitions are listed in chronological order. Use-case descriptions are used commonly in software and systems engineering for defining the interaction (dialogue) between a user and a technical system as a sequence of steps (Cockburn 2001, p. 53; Lauesen & Kuhail 2012, p. 3). In this case, the users were system operators and mine service workers, and the primary safety system and its user interface represented the technical system in the use-case descriptions.

Figure 29. A view from a gate in the automated production area (Burger 2006, p. 556).

The HAZOP team analysed 19 use cases, among which were safety-system start-up, gate-opening and gate-closing procedures, procedures for production-area changes in operation mode, and situations of unauthorised usage of the safety system. In total, 104 deviations were identified, 86 of them caused by human error or problems in task performance. When one compares the results with the PHA results, it can be seen that 11 new hazardous events were identified in this detailed risk analysis of safety-system use cases. The probability of the hazardous event and the severity of the consequences were estimated with the same five-category risk matrices applied in PHA, and the final rating of risk level was performed with three risk categories: low, medium, and high. Recording of the results used an updated version of the HAZOP worksheet template (Appendix 4).

A system simulator was used in the review meetings by the safety-system supplier to simulate the analysis findings and to evaluate needs for improved safety-system functions. According to the safety-system supplier's expert, the main result of the HAZOP study was knowledge of the system's ability to detect possible human error and technical failure in selected operation situations (i.e., use cases) and detect possible foreseeable attempts to misuse the safety system. The HAZOP team evaluated the risks, and proposals for system improvements were directly transferred for safety-system specification and design. Additional safety measures were proposed in relation to safety instructions, safe work practices, and safety training. The HAZOP report was delivered to the customer in line with the terms of the assignment.

7.2.3 Implementation and results of the OHA

The preliminary hazard analysis provided an overall picture of the potential hazards, possible consequences, and safety risks related to the various phases in the life cycle of the new autonomous ore-transportation system. When the system design proceeded to the phase wherein system-operation procedures were specified, a risk analysis of system operations was conducted. The OHA method applied in this approach is based on the methodology described in Roland and Moriarty (1983), Stephenson (1991) and Stephans (2004). The analysis method applied here was OHA (Roland and Moriarty 1983; Stephenson 1991; Stephans 2004). The objectives in the OHA were to identify potential hazards and hazardous events in the operation procedures for the system in the selected phases in the life cycle, in view of both human error and technical failures; to estimate the risks; to evaluate the safety measures designed or planned; and to specify possible additional safety measures for this application.

The scope of OHA covered, in total, 15 system-operation tasks, in three stages of the system life cycle: system integration and testing, system commissioning, and production use of the system. The following tasks were among those analysed step by step with reference to the procedures described in the system-operation specifications:

- Subsystem initialisation
- Operator station start-up
- Autonomous truck loop operation
- System stoppage
- Operator change
- System shutdown.

Special focus in OHA was put on the human interaction between system operators, maintenance staff, and the mine management; operators' interaction with the automation system, safeguarding systems, and other external information systems in the control room; and performance of tasks described in the operator's manual or control tasks involving tele-operation. In practice, the OHA was conducted in line with the following procedure:

- Review of the system-operation tasks
- Identification of possible hazards caused by human error, failures in task performance, or other problems in completion of a specified task
- Identification and analysis of possible consequences
- Estimation of the risks in the absence of any safety measures
- Description of the existing safety measures
- Description of possible additional safety measures
- Estimation of residual risks.

The documentation available in the OHA included descriptions of system-operation procedures and work tasks, system specifications, and drawings showing the layout of the production area. The relevant PHA results and the safety-system-focused HAZOP study results were taken as input for the OHA analysis. The results were updated and supplemented on the basis of the more detailed information on system-operation tasks. Practical information and a general picture of the operating environment were given during the visits to the underground production area in the mine and to the control room in the office building. Both facilities were under construction at the time. Figure 30 presents an overview of the control room and dump-truck operation in a tunnel.

The severity of the consequences and probability of the occurrence of harm or other physical damage were estimated by means of the same five-category risk matrix as in PHA and in the HAZOP study, and the final rating of risk level used the same three categories of risk: low, medium, and high. Recording of the results employed the same template as in the PHA (see Appendix 3).

Figure 30. The operator's station and a dump truck (Fiscor 2008).

The risk-analysis work was done first at VTT, by two researchers following the same gradual two-phase procedure as in the PHA. The OHA worksheet was similar in nature to the PHA worksheet. The author of this thesis was one of these researchers. Two joint workshops were organised within the project group to review and complete the analysis and for the risk evaluation. At the first meeting were four system experts from the system supplier and a researcher from VTT, and present at the second analysis meeting were three system experts and two researchers from VTT. The author of this thesis participated in the latter meeting. The OHA method was introduced to the analysis team at the first meeting.

The OHA team identified 49 hazards or hazardous events caused by human error. The following were among them:

- A system operator makes the wrong selection.
- A system operator forgets to check information before the next action.
- A system operator specifies safety-critical information incorrectly.
- A system operator performs an unintentional action.

- A system controller does not perform an expected action.
- The system operator and mine service worker do not keep each other informed.

For 13 of them, also a technical failure could have been a possible cause. Before any safety measures were considered, the 'as-is' risk level was estimated: high in two cases and medium in 21. In addition to the personal-safety consequences, there were 52 effects on machinery or production identified and analysed. When the OHA results are compared with the PHA and HAZOP results from earlier, it can be noticed that 36 new hazards or hazardous events were identified.

The risk evaluation took into account the results of the PHA and HAZOP study and then considered needs for additional site-specific and application-specific safety measures. The risk-reduction proposals were created in accordance with the procedure applied in the PHA, taking into consideration both system supplier and mining company risk-reduction possibilities and responsibilities. In addition to the 32 technical safety requirements mainly to do with primary safety-system functions, 49 proposals for safety instructions or safe work procedure were created.

It was judged that the proposed safety measures should reduce personal-safety risks such that 15 medium-risk-level issues and eight low-level issues remain. The explanation for the number of remaining 'medium' risks is roughly the same as in the PHA. The matrix is built such that the highest severity category (1, 'multiple-fatality') yields medium risk level even if the probability is estimated to be of category E, 'very unlikely', after all risk-reduction measures. This can be seen, as is mentioned above, in machine fire situations or collisions with a service vehicle. The OHA report was delivered to the customer in line with the assignment terms.

7.3 Experiences, comments, and observations

7.3.1 Experiences from the mining company

The mining company has published information about the mine-automation project in question. Experiences of the mine extension project (Finsch mine, Block 4) and of the planning, commissioning, and operation of the automated ore-transportation system have been published by Fiscor (2008) and Burger (2006). The mining company emphasises the importance of the integration of separate systems to optimise the mining process and create added value. They also highlight the benefits of the access-control system, which isolates the autonomous production area and protects it against unauthorised access and uncontrolled machine exit (ibid., p. 555).

The system was the first of its kind, and, according to the mining company, the move from manual mining-machine operations to the autonomous ore-transportation system was a technological challenge with no reference points (Fiscor 2008, p. 41). The mining company has also expressed that, with the aid of the inspectorate, they had concluded that they had to put various safety controls in place to prevent people from entering an automated environment. The access-control system pre-

vents people from entering the automated area while the dump trucks are operating. In addition to the safety system and its safeguarding functions, many more safety measures had to be built into the system (ibid., p. 40).

The systems-engineering perspective in design and the importance of the integration of the automation system with the overall operating environment are emphasised also in the comments made by the mining company after a few years' operation of the automated ore-transportation system. According to the mining company (Burger 2006, p. 559), the key to success in this project had been intelligent integration and suitable interfacing of the underground information management and mine-automation systems. It claims also that the successful deployment of underground mine automation and mobile-machine production-management solutions improved not only safety and productivity but also cost performance (ibid.).

7.3.2 The system supplier's experiences and comments

According to the system supplier's experts interviewed for the thesis project in March 2012 (see Subsection 5.5.2), this autonomous dump-truck application in South Africa was the first case of overall automation for the company, and the system-safety engineering culminated largely in the access-control system. 'This project was a learning process in system-safety engineering for us all. The safety-engineering practice that had been used in the system-development phase gave concrete systematic form to how to proceed with a customer application,' stated one of the interviewees. Production in Block 4 in the mine is now nearing an end. The mine will soon begin closing that production level, and planning is in progress for the next production level below it, Block 5. In Block 4, eight autonomous mine dump tracks have been transporting ore from loading points to the crusher bin. The system supplier's experts emphasised that the system has been profitable, and no automation-related accidents have occurred in the time since. The system has been working safely for almost 10 years now. 'In that sense, it can be said that the solutions and decisions for risk-reduction measures and the access-control system have been working well and effectively,' said one of the interviewees in summary.

The system supplier's expert stated that reaching an acceptable risk reduction and residual risk level in an automated work-machine system is still a big safety-engineering challenge, one that cannot be resolved by the system supplier's actions, in-built technical safety measures, or safeguarding technologies alone. The end users' safety culture and compliance with the safety procedures and instructions play an essential role in achieving and maintaining overall system safety from the system installation phase to the operation and maintenance phase. Technical solutions cannot eliminate all risks. In a sense, an automated mobile work-machine system in a mine constitutes an 'automation island' in the generally manually handled excavation process. 'It requires different work-management principles and rules. It is not possible to enter the automated area at the time one wants. Access needs to be agreed on with the automation-system operator and planned well in advance,' explained one of the interviewees.

The importance of the specification of the machine operating mode in the analysis of system failures or deviations in control-system risk analysis was brought up in the interviews. Also raised was the question of how to separate safety issues from issues related to system reliability or to system availability in control-system risk analysis. Failure or deviation in control-system functionality may cause unexpected behaviour from the machine and collision with the tunnel wall during automatic operation, but, because this occurs in an isolated area, it does not cause any direct risks to personal safety. If the same uncontrolled movement occurs, for example, during testing or maintenance of the machine, the consequences can be safety-critical. According to the interviewees, operation mode and use-case information is essential for risk evaluation and allocation of risk-reduction measures to the safety-related parts of the control system and for other appropriate measures to prevent hazardous consequences in certain operation conditions.

The interviewees stated that the system supplier have adopted the risk-assessment process in their day-to-day systems-engineering work practice. All new applications of machinery automation are analysed. The risk-assessment process is conducted from the overall hazard identification, through the system design and verification, up to the safety validation phase. 'Co-operation and experiences, especially from this case, have enhanced the system-safety-related knowledge within the company. On that basis, it has been possible to create our own proactive way of operating in system-safety engineering in customer-application projects,' described one of the interviewees.

In this case, the proposed safety requirements and concrete measures covered all of the main areas for risk reduction: technical means, instructions, warnings, and training. Existing risk-reduction measures and proposed new measures identified were assigned to two categories. System supplier measures and actions (such as technical system design and development measures, along with operation and maintenance instructions) and measures and actions for the mining company (e.g., general safety instructions for operations on the production level) were documented. The experts with both parties considered this a good way of clarifying the necessary risk-reduction actions. According to the system supplier's experts interviewed, this presentation aided in understanding that adequate safety of the automated ore-transportation system can be reached only via synthesis and integration of the systems supplier's and end user's risk-reduction measures.

According to the system supplier's experts, machinery-safety and product-safety legislation are tightening constantly in the mining industry. In Australia, the product-liability legislation has developed to such a level that product-safety responsibility has been defined down to the individual person. Also, all risk-analysis and safety-engineering material related to the product must be available if the authorities ask for it. The IEC functional safety standard has become the normative standard for safety-related systems in mining-automation applications. The standard was first published in 1998 as IEC 61508, and the latest version was issued in 2011 (SFS-EN 61508-1:2011). Interviewees mentioned that also the 'layers of protection' analysis (LOPA) method has been utilised to support the specification of independent protection layers, in assignment of the risk-reduction responsibilities,

and to support the specification of safety integrity levels for safety-related parts of the automation systems and machine-control systems.

Current safety regulations and standards require that an automatically operating machinery system be isolated from its environment with fences and gates. It can be claimed that such a fixed safety solution is not optimal for the overall production process in a mine or on other work sites using automated mobile work machines. In the system supplier's experts' visions, a safety solution without fixed isolating fences and barriers would enable revolutionary development in automated mobile work-machine business. The risk-estimation methodology in which the probability of each hazardous event is estimated on the basis of the worst-case scenario was criticised by one of the system supplier's experts: it was claimed that thinking in terms of worst-case scenarios can lead to untenable situations – in, for example, calculation of stopping distances for mobile machinery. Risk estimation should be grounded in the facts of the real operation environment and application-specific conditions.

7.3.3 Observations

The risk-assessment approach and the analysis methods were accepted by the mining company, and results from the autonomous ore-transportation system risk assessment were synthesised with the production-level risk-assessment results and saved in the underground mine's information-management system. The approach and methods were modified and implemented to fulfil the requirements of the mining company, the system supplier, and local and international safety standards in force at the time.

The work was done with quite limited resources and within the limitations of the customer project's main timetable. The distribution of resources and of analysis work efforts were tackled at the first joint project meeting. The mining company's experts joined in the PHA work, and the system supplier with its subcontractors participated in the HAZOP analysis and OHA. The results were reviewed and evaluated in joint project meetings.

Risk-analysis results from the conceptual design phase of the automated ore-transportation system and safety measures designed for the system concept (see the discussion of Case 2) formed a baseline for the application-specific safety-engineering work. In this case, PHA was an essential method of risk analysis. Its results were supplemented with OHA and a HAZOP study, and the analysis results were linked to each other. The PHA was done differently than in the previous cases. For practical reasons, it was not possible to organise brainstorming sessions or team discussions to identify hazards, causes, and consequences with the analysis teams. The same researchers from VTT worked on all of the risk analyses, and the results were distributed in the project team and discussed at the project meetings. The analysis results prepared by the researchers were reviewed, evaluated, and supplemented by the experts from the mining company and the system supplier at review meetings. The OHA was conducted with the

same procedure, in co-operation with the system supplier's experts, and the HAZOP study was carried out in co-operation with the system supplier's and the safety-system supplier's experts. The limited resources, including common time available at joint meetings, were used as efficiently as possible. This applied approach might limit the creation and identification of new site-specific hazards and hazardous events; after all, the discussion in team sessions readily began concentrating on topics and findings on which materials already existed. On the other hand, the opportunity for direct communication within the international project team, researchers' experience of previous cases of mining automation, and the opportunity to visit the mine in South Africa assisted with understanding the site-specific issues, system operations, operation environment, and system functions.

The HAZOP study followed the same standard procedure that had been used in the previous cases. The analysis was focused on finding safety-critical deviations, both technical and of human origin, in the intended use and designed operating situations of the access-control system. This was the first time the author applied use-case descriptions in HAZOP work. Detailed descriptions of the preconditions for the operation situations and the intended dialogue involving the system operators, mine service workers, and the related subsystems helped to make the analysis more systematic. They also aided in more precise specification of the deviations, causes, and consequences, which was essential because of the complexity of the entire automation system and the large number of individual modes of operation and operation situations. The utilisation of the safety-system simulator turned out to be profitable both for verifying the analysis findings and for enabling testing and evaluation of proposed modifications and improvements to the safety-system software.

From the project's outset, the system supplier was aware of the importance of safety issues and risks related to human factors in this kind of autonomous system's implementation, operation, and maintenance. Even though the primary safeguarding system was designed to isolate the autonomous system and control access to the automated area, it had been recognised that there were safety-critical interfaces to manual machine operations and other operations that should be considered in the system design, system implementation, and integration with the operation environment in the mine. These concerns were confirmed in PHA. It appeared that situations would arise in normal operation of the autonomous ore-transportation system wherein system safety assurance relies almost entirely on human actions. One example is the production-area inspection before the system starts up for automatic operation. A miner goes through the automated production area and checks that there is nobody in the area before closing the gates and giving the operator permission to commence automatic operation. Technically, it is almost impossible to survey the whole of this large area completely. The HAZOP team and OHA team reached the same conclusion here, that the safety system cannot completely guarantee safety or control all activities in a large automated production area. This highlights that, no matter the intelligent features and functions, mine service workers, system operators, and all personnel

working in the mine have an important role in ensuring safety and health in the automated production area by following the safety instructions and procedures.

One of the main ideas in the risk-assessment approach under study is that the risk-analysis methods complement each other and add value for decision-making in the risk-management process. In this case, PHA covering the overall system found 69 automation-related hazards or hazardous events. In HAZOP study, 104 deviations were identified with respect to the operation and functionality of the safety system. The OHA team identified 49 hazards or hazardous events related to the specified system operations. When the HAZOP and OHA findings are compared to PHA findings, one can see that 11 new hazardous events were identified in the former and 36 new hazards or hazardous events in OHA.

7.4 Discussion

The mining company was building a new production level for the underground mine and investing in an automatic dump-truck solution for the horizontal ore transportation to the crusher. The system supplier was delivering their first full-scale autonomous ore-transportation system for the customer. The safety-engineering problem was how to identify automation-related hazards, assess risks, and specify safety requirements for the specific customer application at hand. The risk-analysis approach including PHA, HAZOP, and OHA methods and a qualitative risk-estimation method using 5 × 5 risk matrices were applied to solve this problem.

In the PHA, the causes of automation-related hazards and hazardous events were recorded in two categories: human errors and technical failures. The focus in the OHA was on the identification of human errors in selected system operations, and the emphasis in the HAZOP study was on evaluation of the capability of the safety system's diagnostic features to detect possible human errors and safety-critical failures. The precise causes or conditions leading to the human error were not analysed more deeply and systematically. In some cases, the root causes of the human error – such as carelessness, hurrying, stress, difficulty in making a selection, and inexperience with a specific unexpected event – were estimated.

One of the most serious hazard scenarios identified in the PHA in this case was that of an autonomous truck colliding with a service car full of people in a tunnel. It is obvious that this kind of risk must be eliminated in all circumstances, in all stages of the life cycle of the automated system. That may have been one reason these scenarios were not examined more deeply for determination of why the service team must access the production area or how often they need to be in the area. From the methodological standpoint, these questions should be asked to enable better reasoning in the estimation of the probability of the hazardous event. The risk-assessment guidelines for the machinery-safety sector specify the following factors as elements to be taken into account when one is estimating the exposure to a hazard (SFS EN ISO 12100:2010, p. 18):

- The need for access to the hazard zone (for normal operation, correction of malfunctions, maintenance or repairs, etc.)

- The nature of the access (for example, manual feeding of materials)
- The amount of time spent in the hazard zone
- The number of people requiring access
- Frequency of access.

Another difficulty in risk estimation was noticed in this case, in relation to definition of the occurrence of harm. The probability of occurrence of harm was not easy to separate from the probability of hazardous events than can cause harm, while the latter is only one factor in the probability of occurrence of harm as defined in SFS EN ISO 12100 (2010, p. 17). In general, estimation of the probability of occurrence of harm or material damage was supported in the PHA by verbal descriptions of the probability categories. This method was developed and used because use of numerical expressions for probability, such as '$10^6 < P < 10^5$' or '1 hazardous event / 100 years', was considered impractical in this kind of 'one-of-a-kind' application. The general risk-management guidance in IEC ISO 31010 (2009) states that the consequence scale in risk assessment should cover various types of consequence, such as financial loss, safety, environment, and other parameters, depending on context, and that the assessment should cover the range from the maximum credible consequence to the consequence of least concern, and scales with 3, 4, or 5 steps are most common for probability. It is pointed out also that the definitions for probability should be as unambiguous as possible (ibid., p. 83). This is also emphasised in BS 18004 (2008)'s statement that when the organisation's risk-assessment method uses descriptive categories for assessment of severity or likelihood of harm, they should be clearly defined. Clear definitions of terms such as 'likely' and 'unlikely' are necessary for ensuring that all stakeholders interpret them consistently (ibid., pp. 78–79). The system-safety standard MIL-STD-882D (2000) claims, that assigning a quantitative hazard probability to a potential design or procedural hazard is not possible in the early stages of a system-design process. It proposes that the probability of an occurrence of the hazardous event during the planned service life of the system can be estimated per unit of time, per event, in population terms, per item, or by activity (ibid., p. 18).

The same hazard or hazardous event can cause personal-safety risks in the worst case but most probably will lead instead to physical damage or production losses. For such cases, the two types of consequences were recorded and assessed separately. In general, consequences in all three risk analyses (PHA, HAZOP study, and OHA) were classed into two categories: personal-safety impacts and other impacts, such as damage to machines/materials or production loss. Because the focus in the risk analyses was on identifying new automation-related personal-safety risks, this categorisation aided with the risk-estimation and risk-evaluation work. The risk-assessment guidelines for the mining industry cover only safety risks. For example, the NIOSH has developed recommendations as to best practice for mining equipment that uses programmable electronic systems (Sammarco et al. 2001; Sammarco 2005b). In these guidelines, the focus is on

personal-safety issues, and their concept of system safety provides no support for the analysis of other consequences (Sammarco 2005b, p. 23).

Today, the risk-assessment standards SFS EN ISO 12100 (2010) and IEC ISO 31010 (2009) aid in this procedure of assessing the individual consequences of the same hazard separately. According to SFS EN ISO 12100 (2010), risks related to the most likely severity of the harm but also the greatest foreseeable consequence of the harm should be taken into account, even if the probability is not high (ibid., p. 17). The IEC ISO 31010 (2009) standard states that many hazardous events may have a range of outcomes, having different associated probability, with minor problems being more commonplace than catastrophes. The consequence scale in risk assessment should cover diverse types of consequences, related to financial loss, safety, environment, or other parameters, depending on context. The analyst can decide whether the overall rank assigned should reflect the most common outcome, the most serious, or some other combination. According to IEC ISO 31010 (2009), it is appropriate to focus on the most severe consequences, as these pose the greatest threat and are often of most concern, but in some cases, it may be appropriate to record and assess both common problems and unlikely catastrophes, as separate risks. In risk estimation, it is important to note that the probability of the selected consequence is used, not the probability of the event as a whole (ibid., p. 85).

The OHA method was new to the researchers and for the industrial experts. The upper-system-level analysis moved systematically through the system-operation descriptions. The focus was on human error, failures in task performance, and other problems with performing specified work tasks. The risk-assessment standard for machinery, SFS EN ISO 12100 (2010), strongly emphasises that human factors shall be taken into account in risk analysis considering possible human errors. According to the standard, human factors include, among others, the following (ibid., p. 19):

- Interaction of people with the machinery
- Interactions between people
- Stress-related factors
- Ergonomic elements
- People's capacity to be aware of risks in a given situation, depending on their training
- Experience and ability
- Fatigue factors
- Aspects of limitations in abilities (due to disability, age, etc.).

From a system-safety perspective, Vincoli (2006) gives some methodological guidance by naming predictable elements behind human behaviour in system operation. People usually follow procedures that involve minimal mental or physi-

cal effort, minimal time to complete a given task, and elimination of discomfort or monotony and fatigue. Also, Vincoli groups human errors into three types: errors made by the operator in an actual operation situation, system design errors such as not considering human factors enough, and management errors such as inadequate training or unrealistic expectations surrounding the resources for conducting an operations (ibid., p. 94).

Kariuki and Löwe (2007) have studied human factors in process hazard analysis. They claim that, although human failings are a major cause of undesired events in process industries, the shortcomings in design behind incidents arising and the contributions of management failures are not systematically considered. They also claim that a human-factors approach is necessary for sufficient understanding of human errors. Human factors are related to environment, organisational and work task factors, and human characteristics. Human factors' contribution to undesired events can be modelled in terms of latent conditions that result from sub-optimal design and management decisions and from active operator errors. Latent conditions do not directly affect the system functions, but, in combination with operator error, they can cause a hazardous event (ibid., pp. 1765–1766).

Leveson (2011b) has studied and discussed human factors and operator errors extensively in complex system applications in various sectors of industry. Leveson reminds that all human activity takes place within and is influenced by the environment. 'Environment' here refers to both physical and social environment. This is why it is often very difficult to separate design errors from operator error (ibid., p. 39). Leveson also claims that changing the environment would be a more effective way to reduce operator error than the traditional behaviourist approach of using rewards and punishment. In accident causality models, the focus in the human-factors analysis should be shifted from human error (in other words, analysis of deviations from normative procedures) toward analysis of human-performance-shaping features, boundaries of safe performance, and the context wherein system operation takes place and in which deviations might be made (ibid., p. 46). The three-level risk-assessment approach applied in this case and the analysis of the human–machine interaction and human factors at overall machinery application level, upper system level, and lower system level is in line with the above-mentioned guidelines. The categorisation and reasoning related to human factors guide attention to solving the right safety problems and assigning safety measures to the right level, from the overall work-site operating environment down to specific use cases in human–machinery-system interactions.

The HAZOP method applied in this case followed the IEC 61882 (2001) standard's guidelines. The design intent of the procedures in the safety-system operation situations under study was written in the form of a use-case description, a dialogue between a user and the safety system. This turned out to be a clear representation of the operation procedure, assisted with understanding the safety system's functionality and control logic, and also aided in identification of deviations in the HAZOP study. These results seem to bear out the benefits of use-case descriptions that are expressed by Cockburn (2001). Cockburn states that use cases describe coherent stories about how the system will behave in use. Use

cases create value when they posit named user goals that the system will support and are compiled into a list that can be used to aid in communication among the various stakeholders in a project. Use cases are valuable when the design team brainstorm about all the things that could go wrong in the success scenario and discuss how the system should respond. Without discrete use-case description and failure analysis, many errors could go undetected until program testing, if even uncovered then, as programmers do not have time to evaluate all aspects of system behaviour against that desired (ibid., pp. 15–16).

Taking a system-requirement specification and system design point of view, Lauesen (2003) and Lauesen and Kuhail (2012) have studied use cases and compared them with task descriptions. According to Lauesen (2003), task descriptions in the context of user–system interaction refer to the needs of the safety system's users, without specification of any specific dialogue. Lauesen and Kuhail (2012) claim that if use cases are employed too early in the specification of system requirements, they lead to overly restrictive requirements because they force the design a user–system interaction dialogue to occur at a very early stage rather than allow user needs to be specified first. The authors also state that task descriptions form a good basis for the specification of user interfaces and that system functions and detailed user–system interaction dialogue can be added later in the design (ibid., p. 17).

The risk estimation in the project was done in two phases of the risk-reduction process: risks were estimated without any safety measures and then estimated in account of all conceptual and existing-site-specific safety measures. This procedure follows that described in SFS EN ISO 12100 (2010). According to the standard, which is intended for machine designers and manufacturers designing new machinery, the initial risk assessment should be based on the system definition and the intended use of the system, and the risk level should be estimated before protective measures (ibid., p. 11). The risk should be reduced in the first place in line with the three-step risk-reduction process by the manufacturer or by the system supplier, as it was in this case: step 1 ('inherent safety design measures'), step 2 ('safeguarding and complementary protective measures'), and step 3 ('information for use'). The residual risk should then be evaluated in light of the needs for additional safety measures specified and implemented by the user (ibid.).

On the other hand, BS 18004 (2008), which is meant for machinery end users assessing existing machinery / production systems and work sites, states that when one is estimating the likelihood of harm, the adequacy of existing controls should be taken into account and that, especially in risk assessment for new activities, the initial assessment should be based on the intended controls. The standard also points out that the measures in both cases should be clearly documented so that the basis for the assessment and reasoning for risk-reduction decisions will be clear when the assessment is revisited later (ibid., p. 80). On the basis of the risk-assessment results, one can state that in this case these two standards' viewpoints were combined successfully to cover both the system supplier's and the end user's responsibilities for risk-reduction measures.

The incorporation of risk-reduction actions into the system-safety-engineering process for an automated mobile work-machine system for reaching acceptable risk levels differs markedly from what occurs in the case of a single manual work machine. The first risk-estimation round was important for understanding of what could happen in the worst case if nothing is done to prevent the accident. In many cases, the risk could be eliminated by the system supplier's inherent safety measures. The second estimation round was carried out for those risks that had not been reduced to an acceptable level by system supplier actions. The main difficulty was in the estimation of the various measures' impact on the three main factors of the probability of the occurrence of harm as expressed in SFS EN ISO 12100 (2010, p. 17): 'the exposure of person(s) to the hazard', 'the occurrence of a hazardous event', and 'the technical and human possibilities to avoid or limit the harm'.

As the system supplier's expert pointed out, the end user's safety culture and compliance with the safety procedures and instructions play a vital role in reaching and maintaining overall system safety in automated mobile work-machine systems in mines. Not all risk can be eliminated via technical machine-level or even technical safety-system solutions. This view is expressed also in the system-safety literature, by, among others, Vincoli (2006), discussing system safety's connection to industrial safety, and Leveson (2011b), who takes a system-theoretic view of causality and hierarchical safety-control structures (see Vincoli 2006, p. 12, pp. 37–43; Leveson 2011b, pp. 75–83).

In addition to what has been discussed above with respect to this particular case of Finsch mine automated ore transportation, the interviews with the system supplier's experts pointed to three important trends in the mining industry that need to be discussed in any evaluation of the usefulness of the three-level risk-assessment approach and PHA, OHA, and HAZOP methods in such site-specific applications in the mining industry. The three trends are these:

- The machinery-safety and product-safety legislation that affects the mining industry is tightening all the time, and customers are requiring traceable evidence of a systematic and documented risk-assessment process on the part of the system designers and system suppliers.
- The functional safety standard has become the normative standard for safety-related systems in mining-automation applications.
- The LOPA method has entered wide use for the specification of independent protection layers, in allocation of the risk-reduction responsibilities, and to support the specification of safety integrity levels for safety-related parts of the automation systems and machine-control systems in the mining industry.

Given the results and experiences obtained in this case, the three-level approach applied to risk assessment and analysis methods involving systematic documentation practices seem to support development of the system supplier's practices in a manner that meets the increasing customer demands for a traceable risk-assessment process and evidence-based risk evaluation. The approach and methodology employed in this project followed a system-safety approach quite

similar to what Sammarco et al. (2001) and Sammarco (2005b) have recommended for mining equipment using programmable electronic systems.

It is evident in all applications of automation in the mining industry that the safety measures required will depend on many factors specific to the application, as is noted in this case study. The functional safety standard was designed to set out a generic approach for systems composed of electrical, electronic, and programmable electronic (E/E/PE) elements that are used to perform safety functions. The framework of a risk-based approach provided by the standard can be applied also for safety-related systems based on other technologies (SFS EN 61508-1:2011, p. 13). On the basis of the results and experiences obtained in this case study, one can state that the three-level risk-assessment approach augments and supports the functional-safety-engineering practice for system-safety issues. The upper-system-level perspective utilising OHA methodology brings an additional point of view and level of analysis to safety requirements' specification and safety validation. It seems to be an important layer between the overall machinery application level and specific (E/E/PE) safety function level in automated mobile work-machine systems.

The LOPA approach uses a semi-quantitative method for the specification of protection layers and safety integrity levels for safety-related systems. This analysis requires risk-assessment information that covers hazards, causes, and consequences; information on the safety measures in place and proposed new measures; initial and causal event frequencies and protection layer failure probabilities; and definition of tolerable risk. Analysis of protection layers can be applied to support the evaluation processes in a manner consistent with, for example, PHA and HAZOP studies (IEC 61511-3:2003, p. 49; IEC ISO 31010:2009, p. 59).

From a systems-engineering perspective, it can be claimed that this three-level risk-assessment approach and the selected risk-analysis methods (PHA, OHA, and HAZOP) together form a good basis for detailed requirement specification and design of safety-related systems in accordance with the functional safety approach and supported by the LOPA method. From the system-safety perspective, the risk-assessment approach is aimed at ensuring that all safety-related functions are identified and that the risk-based requirements are specified such that they correspond to the real mine-work-site-specific conditions, so that the design of the safety-related functions is informed by correctly determined safety integrity levels.

7.5 Conclusions

According to the case-study results, comments from industrial partners, and the author's observations, the risk-assessment approach applied, involving PHA, OHA, and HAZOP methods and qualitative risk-estimation principles, is suitable and practicable in automated mobile work-machine customer-application projects and supports the system supplier's systems-engineering process. The system supplier has adopted the risk-assessment approach and developed a company-specific application for in-house use focusing on functional safety issues.

The practical method of risk assessment in this case differed from the traditional analysis team sessions described in the standards and system-safety literature. Conducting the analysis work in stages and combining researchers' preparation work efforts and expert group review meetings seemed to work out well and effectively in the customer project's hectic international and multicultural context. The case study's results and experiences show that the improvements and other changes in the risk-assessment approach and analysis methods, in comparison with the earlier cases, seemed to develop the methodology in the right direction:

- Separating personal-safety consequences from other consequences (such as physical damage or production loss) clarified the hazard identification and risk estimation.
- Utilisation of PHA results in OHA and HAZOP studies and more precise description of hazardous events, deviations, and causes and consequences aided in the analysis work. It must be noted that in this case the same two researchers handled all analyses and assessment sessions.
- Descriptions turned out to be practical for this unique automation application. Probability estimation using five categories and application-specific verbal.
- Risk estimation was done in two phases: before any application-specific safety measures and after the proposed system-safety measures. This clarified the estimation of residual risk.
- The proposals for safety measures were categorised clearly into system supplier's actions and mining company's actions. This supported the evaluation of appropriate on-site means of risk reduction.

The innovative way of utilising a laptop-based safety-system simulator in HAZOP sessions turned out to be profitable both for verifying the analysis findings and for providing the ability to test and evaluate proposed modifications and improvements to the safety-system software immediately.

The results of this industrial case study when coupled with the results of case study 1 confirm the great importance of consideration and analysis of human factors with a wider scope and in a more extensive manner in such complex automated mobile work-machine system applications. The analysis of operator errors in OHA- or HAZOP-study-type analyses should be widened to cover the factors related to the actual operation situations, the operation environment, and factors enabling and supporting operation as intended (correct and safe use).

The results of this case study support the system-safety view, which emphasises the importance of the integration of safety-risk-management efforts into the overall system-engineering process and overall production system and into production-environment development efforts. Such mining-automation applications are unique, and safety solutions depend greatly on the mine environment. In complex mobile work-machine systems, safety problems cannot be solved by technical means. Safe operation and maintenance relies strongly on operators' and other stakeholders' risk-conscious behaviour and decision-making.

The objectives of the project under study were to identify potential hazards and hazardous events, assess the risk, and evaluate the safety measures necessary for the autonomous ore-transportation system in the mine. From the mining company's and system supplier's experiences and comments, it can be concluded that these objectives were met. Both the mining company and the system supplier confirmed this opinion by reporting experiences of safe and efficient operation of the system. The three-level risk-assessment approach and the analysis methodology were accepted by the global mining company, which indicates that the approach fits the mining industry's automation projects involving mobile work machines. The generic reference model created at the NIOSH for the mining sector recommends the use of these methods also for surface or underground mining systems employing embedded and networked programmable electronics.

The case project was a good learning process and highlighted several methodological and practical aspects of how to improve the risk-assessment approach and analysis methods. The documentation of the hazardous events identified should be made more specific in the PHA and OHA, to improve analysis, traceability of the safety requirements, and linking of the safety measures to the right risks. This would demand not more work effort but more systematic documentation practices.

The risk-estimation method and the interpretation of the risk levels reached should be developed so as to support the decision-making better in risk evaluation and industry studies involving requirement, functionality, and design analyses in systems-engineering processes. Site-specific information should be used as much as possible in risk analysis, risk estimation, and risk evaluation, to enable correct reasoning based on the actual work-site conditions, practices, and limitations. Insufficient information can lead to conflation of concepts and to difficulties in untangling probability estimates for hazardous events and occurrence of harm.

As the application of a functional safety approach and LOPA methods appear to be becoming *de facto* standards in the mining industry, the three-level approach to risk assessment and analysis methods should be developed to support these common practices.

8. Case study 4: The container-handling-system concept and its application

8.1 Introduction

The fourth case study has two objectives. The first is to evaluate the utility of the three-level risk-assessment approach in relation to the systems-engineering approach. The second is to evaluate the usefulness of PHA, OHA, and HAZOP methods in a complex automated cargo handling application in its system development phases.

VTT conducted a joint research project and a risk-assessment assignment with a cargo handling equipment manufacturer (later 'the system supplier') in 2006–2008. The objective of the research project was further development of the three-level risk-assessment approach and evaluation of the PHA in the conceptual design phase of an automatic container-crane concept (Tiusanen et al. 2008). The project was carried out with the financial support from the Finnish Work Environment Fund. The risk-assessment assignment was an implementation of OHA and HAZOP analyses in a customer-application project for an automatic container-crane system. The objectives of the assignment were to ensure that the application is safe to use and maintain and that it fulfils the site-specific and customer-specific safety requirements and the safety regulation in force in the European Union.

The system supplier was delivering an automatic stacking crane (ASC) system to a container terminal in Germany. Terminal operator Hamburger Hafen und Logistik (HHLA) is transforming Hamburg's Burchardkai container terminal into a semi-automatic terminal with automatic crane systems for containers' stacking and handling (see Figure 31). The containers in any given block are handled by three automatic cranes. Two identical 'inner cranes' use the same tracks, while one 'outer crane' uses a separate track. The outer crane is able to pass both inner cranes. Each crane will be able to operate in the container-storage area and in both land-side and water-side handling areas. In normal operation, one of the inner cranes operates in the land-side handling area and the other in the water-side handling area (see Figure 32). A simplified block diagram of the automatic crane application's modular system architecture is presented in Figure 33.

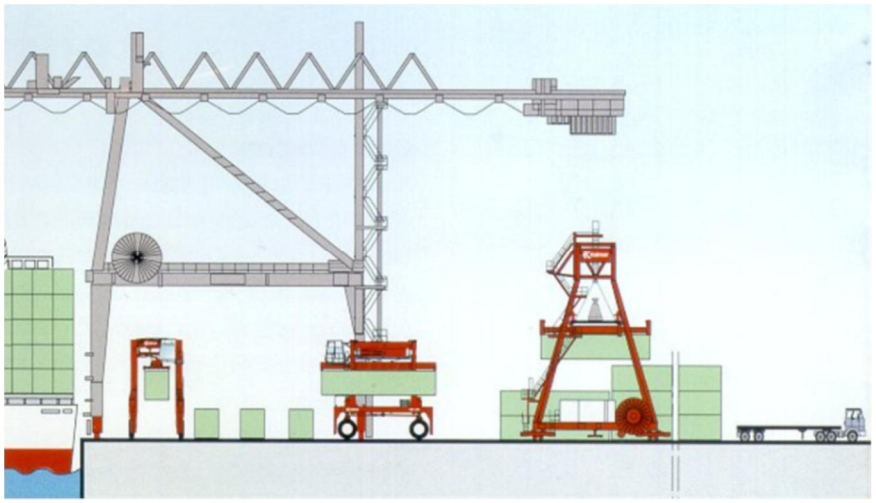


Figure 31. An illustration of the container-handling machinery fleet in an ASC application (Cargotec). Figure used with permission from Cargotec.

Figure 32. Pictures of the ASC in operation at HHLA's Burchardkai container terminal, in Hamburg (Cargotec). Figure used with permission from Cargotec.

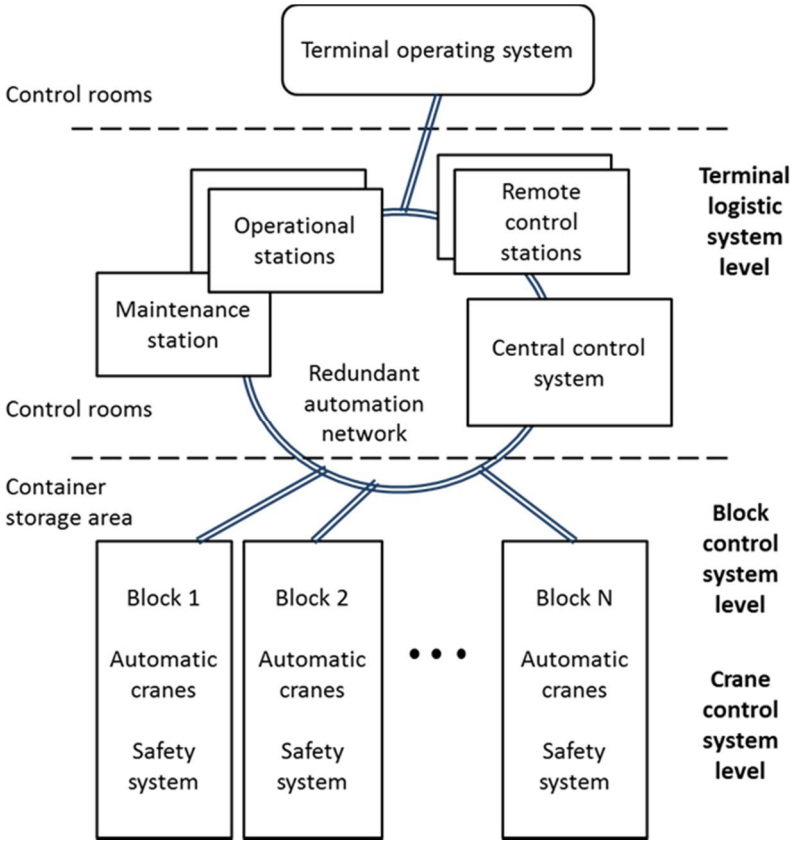


Figure 33. The main ASC modules and a rough overview of the levels in a hierarchical system for container-handling logistics, modified from Cargotec's ASC brochure. Figure used with permission from Cargotec.

The joint research project in the automatic crane system concept development phase and during the risk-assessment assignment in connection with the customer-application project included several risk analyses, at various system levels. Examined in this case study are PHA of one container block, OHA of the overall automatic container-handling system operations, and HAZOP study of the safety system. The following research questions are specified for this case study:

- How well does PHA suit work-site-level hazard identification and risk analysis in the system-specification phase?
- How suitable is the OHA method for the risk analysis of system operations in this context?
- How appropriate is the database tool for data collection and documentation for the HAZOP study?

- How well does the three-level risk-assessment approach applied in the project fit the systems-engineering approach for an automated container-handling system?
- What are the benefits and impacts of the risk-assessment work in this case and more generally in the companies?

8.2 Implementation of the three-level risk-assessment approach

8.2.1 Implementation and results of the PHA

The PHA had two objectives in this case. The first was systematic identification of potential hazards and hazardous events in an automatic stacking-crane block and in its related operation environment in a container-storage area. The second objective was to assess the risks and specify system-safety requirements and the necessary risk-reduction measures at a conceptual level. The scope of the PHA was specified and limited as follows:

- As the *stages of the system life cycle* under study: the system operation and maintenance phase, including manual, semi-automatic and autonomous operation, and maintenance and troubleshooting
- *The block* – including the container stack area; the water-side interchange area, where the straddle carriers access the block and feed the containers to the automatic stacking-crane system; the land-side interchange area, where the cranes unload the containers to the trucks or to the terminal chassis; and the reefer area, where the refrigerated containers are connected to the electric power supply (see Figures 34 and 35)
- *Activities in the block* and connected to it such as testing and checking of the cranes, a straddle carrier's loading and unloading of containers, manual operation of the cranes, tele-operation of the cranes, monitoring and control of the automatic operation, driving of a truck, and maintenance of the crane system during operation
- *Personnel working in the block area,* such as straddle carrier operators, truck drivers, system operators in the control room, crane tele-operators in the control room, reefer area workers, maintenance workers, and other people in the block area
- *Machinery and traffic,* including straddle carriers, stacking cranes, trucks, service vehicles, straddle carriers from other blocks, and other water-side vehicles.

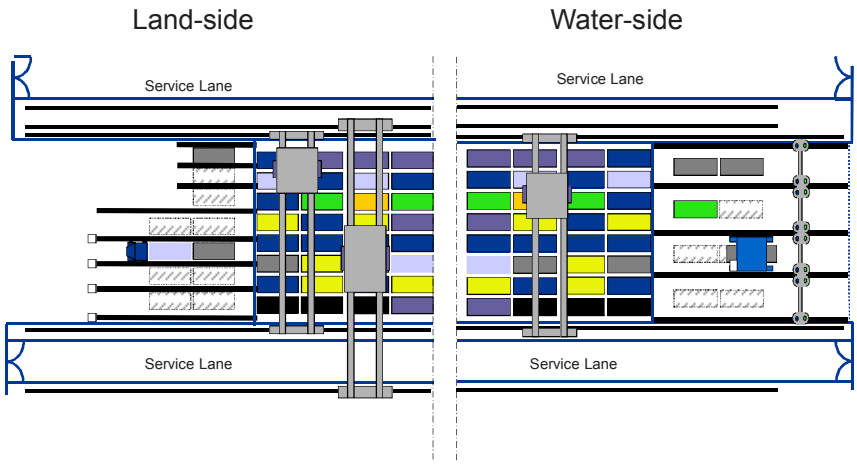


Figure 34. A rough layout drawing of the automatic stacking-crane block (Cargotec). Figure used with permission from Cargotec.

Figure 35. A 3D illustration of the ASC block (Cargotec). Figure used with permission from Cargotec.

In the PHA, the focus was on hazardous events and safety risks related to system-level factors and, especially, on new crane-automation-related issues. Machine-level hazards and safety risks of stacking cranes were available in the PHA. It was also agreed that in the PHA the focus in the hazard identification was on mechanical hazards caused by automatically or tele-operated moving cranes, automatically moving containers, manually operated straddle carriers, and trucks and other vehicles in the interchange areas. The material available in PHA included

layout drawings and 3D modelling pictures of the block concept. The container-handling process and the functionality characteristics of the automatic stacking-crane system were described to the analysis team by the system supplier's automation expert.

The analysis team comprised two automation experts from the system supplier and, from VTT, two researchers, one research trainee, and a technician. The author of this thesis took part in all of the meetings, led the analysis sessions, and documented the results. The team held five half-day analysis sessions during winter 2005–2006. The analysis started with brainstorming sessions for hazard identification and creation of accident scenarios, and it continued with team discussion meetings for specification of causes and consequences, estimation of the risks, and consideration of appropriate safety measures at conceptual level. The PHA results were documented on a worksheet similar to the one used in Case 3.

The risk estimation in the PHA included considering hazardous events before any safety measures. The effects on personal safety and other possible effects on machinery or the block area's infrastructure were analysed separately. To aid in the probability estimation, the categories were concretised with the following hints:

- 1 = Definite — the event happens continuously when the system is operated in the manner specified
- 2 = Very possible — the event can easily occur in normal operating conditions
- 3 = Possible — the event can occur in normal operating conditions
- 4 = Remotely possible — the event is possible only in certain operating conditions
- 5 = Very unlikely — the event is possible if several errors or failures take place at the same time.

The severity of the personal-safety consequences and material damage or loss of production was estimated with the aid of the following hints, which were specified in collaboration with the system supplier.

- 1 = Multi-fatality — more than one person dies
- 2 = Fatality — one person dies or is paralysed
- 3 = Reportable injury, — one person is seriously injured
- 4 = Lost-time injury, — one person is injured (> 3 days of absence)
- 5 = Minor or no injury — there is no more than 3 days' absence
- 1 = Permanent damage — the block is out of use > 1 week
- 2 = Multiple-damage items — the block is out of use > 1 day < 1 week
- 3 = Major cost implications — the block is out of use > 1 shift < 1 day
- 4 = Loss of time/availability — the block is out of use > 1 h < 1 shift
- 5 = Minor/no implications — the block is out of use < 1 h.

The risk rating matrices for the estimation of personal-safety risks and for physical damage and production losses and also the three risk levels (high, medium, and low) were the same as in Case 3 (see Subsection 8.2.1, respectively).

As a result of the PHA, 63 hazardous events were identified. Personal injury was identified for 43 hazards. These include the following items:

- A straddle carrier collides with a service vehicle in the interchange area.
- A straddle carrier collides with an automatic crane in the interchange area.
- A container hanging in the spreader collides with containers in the stack.
- A container hanging in the spreader collides with the reefer area platform.
- A container falls and crushes the truck cabin in the interchange area.

For most of the hazardous events, multiple causes were identified. With 33 hazards, the main cause of the hazardous event was considered to be human error. Technical system failure was the main cause in 24 cases and other causes in six cases. Eleven of the risks to personal safety were assessed as involving high risk, 26 medium risk, and six low risk. In addition to the personal-safety risks, there were 20 incidents identified (and associated estimates made) that were associated with physical damage and breaks in the container-stacking process.

The risk evaluation deemed the appropriate safety measures, according to the sequence for system-safety precedence, to include the following steps (Stephenson 1991, p. 11):

- Design for minimum hazard
- Provide safety devices
- Provide warning devices
- Control with procedures and training
- Assess remaining residual hazards.

The analysis team created 32 proposals for conceptual safety measures. The proposals focused on factors such as the following:

- A block area isolation and access-control system
- A collision-prevention system for automatic cranes
- A tele-operation system that assists in safe container-handling
- Traffic rules and safety instructions for vehicle drivers
- Safety rules and training for maintenance personnel.

The analysis results were transferred to the automation-development team for further evaluation and to be added to the system-requirement specification and for the design of operation concepts and safeguarding solutions.

8.2.2 Implementation and results of the OHA

The objective in the OHA was to identify application-specific hazardous events and specify safety requirements for the automatic crane system. The OHA was carried out concurrently with the system specification and system design. The OHA's scope was the system-operation and maintenance part of the system life cycle, covering the following operations:

- Manual operations in the water-side transfer area
- Automatic crane operation

- Manual operations in the land-side transfer area
- Remotely controlled crane operations in the land-side transfer area
- Manual reefer-area operations
- Other system operations in the control rooms
- Crane maintenance in the block area.

The PHA results were updated and supplemented, and new application-specific hazardous events were identified and analysed. The angle taken in the OHA was that of system-level aspects, and the main goal was to identify and estimate new automation-related safety risks. Hazards and safety risks related to manual crane operations and details of machine-level work tasks were not covered.

The analysis team was composed of the automation design manager, the electrical design manager, and five system designers, from the system supplier, and the author of this thesis and two technicians, from VTT. The team had eight half-day meetings in Tampere in autumn 2006. The meeting schedule was adapted to the main schedule of the system-specification and system-design work. Not all team members were present at all meetings. The author of this thesis took part in all meetings, led the analysis, and documented the results. The OHA method was introduced for the analysis team at the first meeting. Recording of the results employed the same OHA worksheet template as in Case 3 (see Appendix 5).

The operations under study were first described and specified on the basis of the system-specification documents. Human–human and human–technology interactions describing the operations' execution were written in use-case format, of the type used in Case 3. The analysis had two phases. In the first phase, hazardous events, the causes, and their consequences were identified through brainstorming and team-discussion techniques. In the second phase, risks were estimated and proposals for safety measures were generated. In addition to system-specification documents, the OHA team had layout pictures and 3D model diagrams of the automatic crane system.

All told, 143 hazardous events were identified and documented in the OHA. In most cases, multiple causes were identified. Human error was considered the main cause of the hazardous event with 79 hazards. Technical system failure was the main cause with 68 hazards and other causes in 11 cases. Among others, the following causes were identified:

- Failure in handling of a manual straddle carrier or a truck
- Incorrect decision and system operation in the control room
- Failure in a crane tele-operation
- On-site behaviour counter to the instructions during maintenance
- Arising from weather conditions, difficulty in performing a task
- System failure in an automatic crane control function
- Data communication failure.

The probability of the occurrence of harm and the severity of the consequences were estimated with the same five-category risk matrix as in the PHA, and the final rating of risk level used the same three risk categories: low, medium, and high. In

cases wherein there were both personal-safety and physical-damage consequences, the risk estimation was based on the personal-safety consequences. Personal-safety risks before any safety measures were estimated to be high in 50 cases. There were 66 risks estimated to be medium-level risks and four deemed low-level risks. In addition to these risks, 23 incidents were related only to physical damage. The risk evaluation was done in two phases: firstly, with the situation considered before any safety measures and, secondly, in consideration of the planned and proposed safety measures.

Risk-evaluation and risk-reduction iteration followed the system-safety precedence sequence steps mentioned above (ibid., p. 11). The risk-reduction measures possible and appropriate for the system supplier and the container terminal's operator in the specific operation environment at hand were considered. The OHA team created more than 100 proposals partly at the conceptual level, to be applied as a general baseline for automatic stacking-crane applications and partly at application-specific level for this particular customer application. The analysis and evaluation results were directly transferred to the project team for further evaluation and to be used for the technical system specification and for specification of the system operations and work procedures. Proposals focused on factors such as the following:

- Technical means of supporting the driver in following of the traffic rules
- Control measures to prevent access to the automated area
- Technical ways to synchronise manual operations and automatic operations in the block area and keep them secure, along with instructions for their use
- Instructions and technical means of supporting crane tele-operation.

The risk evaluation was then repeated with all of the proposed safety measures taken into account. This risk evaluation indicated that the risks could be reduced such that two risks still remain at 'high' level, 85 risks are at 'medium' level, and 33 could be eliminated or reduced to 'low' level. The OHA report and worksheets were translated into German and then used as working documents in the discussions between the system supplier, terminal operator, and analysis team during the system-design phase. The OHA was updated during the risk-assessment assignment, in view of the updated use-case descriptions and jointly evaluated risk-reduction measures.

8.2.3 Implementation and results of the HAZOP study

The primary safeguarding principles for guaranteed safety of personnel in the automatic stacking-crane system's operation area was designed on the basis of the area's isolation and access control using fences, gates, and safety devices. The safety system keeps personnel from accessing the automated area while automatic operation is in progress. It also prevents uncontrolled entry of machines

to the water-side interchange area and keeps the truck-loading area in the land-side interchange area safe.

The aim of the HAZOP study was to verify the safety-system design against the specified safety-related functionality requirements. The goal was to identify safety-critical deviations in the safety-critical signals in the specified operation situations, estimate the risks, and evaluate the designed safety functions. The HAZOP method was, in essence, the same as used in Case 3. The analysis team was composed of the automation design manager, the electrical design manager, and three system designers (from the system supplier) and two researchers (from VTT). The author of the thesis did not take part in this HAZOP study. The HAZOP method was introduced for the analysis team at the first meeting. Recording of the results employed a data-collection worksheet implemented with an MS Access database application. The development of the database tool and its characteristics in the project is described in Nina Pátkai's Master of Science thesis (Pátkai 2006). The study was done at signal level. The worksheet content was developed from the earlier text document template. The items recorded in the database for each deviation were 'Deviation ID', 'Guide word', 'Deviation description', 'Cause', 'Consequences before safeguards', 'Detection and safeguards', 'Preliminary validation result', and 'Actions recommended'. Pictures of the user interface and an example printed worksheet from the new HAZOP tool are shown in Appendix 6.

The team had 10 full- or half-day meetings in Tampere in summer to autumn 2006. The meeting schedule was adapted to the main schedule of the customer project. Not all team members were present at all meetings. Researchers from VTT led the analysis and documented the results. The team identified 77 deviations. Verification against the functional safety requirement specified for safety-system functions was done in accordance with the reference standard EN 954-1 (1996), applicable at the time. The EN 954-1 standard defined five so-called safety performance categories for safety-related control functions, as follows:

- B: The occurrence of a fault can lead to loss of the safety function.
- 1: The occurrence of a fault can lead to loss of the safety function, but the probability of occurrence is lower than for category B.
- 2: The occurrence of a fault can lead to loss of the safety function between checks. Loss of the safety function is detected by means of a check.
- 3: When a single fault occurs, the safety function is always performed. Some but not all faults will be detected. Accumulation of undetected faults can lead to loss of the safety function.
- 4: When a fault occurs, the safety function is always performed. Faults will be detected in time for preventing loss of the safety function.

For categories B and 1, the principles for achieving safety were characterised mainly by selection of components and via good design and implementation practices. For categories 2, 3, and 4, safety principles were characterised mainly by a focus on system architecture and active failure-detection methods. The EN 954-1

standard has since been superseded by ISO 13849-1 (2009) (see Figure 7), and the safety-performance-category requirements have been included in new performance-level (PL) requirements.

The HAZOP team created 19 proposals for improvements to the safety functions for meeting of the functionality-related safety requirements. The database tool for HAZOP studies was used to support the follow-up reviews and to update the analysis in line with the decisions made during the design of the safety functions.

8.3 Experiences, comments, and observations

8.3.1 The system supplier's experiences and comments

The system supplier's comments were received in the project review meetings during the jointly funded research project (in 2005–2007) and in the project review meetings during the system-safety assignment in 2006–2008. The material on the experiences and comments was augmented for this case study through interviews with three experts in March 2012 (see Subsection 5.5.2).

According to the interviewees, the automatic stacking-crane application was the first of its kind for the company. It was noticed that traditional design practices do not work well enough in large-scale distributed design project with a large amount of subcontracted design work, and a need for the development of formal methods in complex automation development was recognised. The role of the machine's control system changes as the amount of automation increases. There must be several interfaces to other on-board subsystems, such as diagnostic systems and intelligent measurement systems and external higher-level production control systems. 'The complexity of the systems has increased to such a level that traditional machinery-design practices are not enough anymore. The move from the design practices of a single crane application to the design of an automatic stacking-crane system has been huge,' described one of the interviewees.

The interviewed system supplier's experts confirmed that the first three automatic stacking-crane blocks in the container terminal in Hamburg have now been in full operation since October 2010. According to the interviewees, the system supplier has not received any notification of reportable injuries related to the automatic stacking-crane system. One of the interviewees stated: 'We can at least partly conclude that our proactive approach aimed at foreseeing and reducing risks systematically has been beneficial.'

The system supplier has found it valuable that the analysis results and proposals for safety measures in the PHA and OHA and proposals for corrective actions in the HAZOP studies were transferred to the design teams and the information could be utilised directly in the system-requirement specification and system development to a great extent. The project documentation examined in this case study and the interviews elicited, among others, the following comments:

- Systematic top-down analysis of the system has improved the understanding of the overall system operation.
- Analysis sessions have been a good forum for sharing knowledge of system operations and system functions, alongside interdependencies of subsystems.
- The risk-analysis sessions brought out a great many non-safety-related issues that were important for the system specification and system design.
- System-level analysis methods were new for the system designers. In this project, they became familiar with the risk-analysis methods and tools.
- 'The threshold for use of risk analysis will surely be lower in the future,' one of the system supplier's automation experts stated at a project meeting.
- Designers of automation systems, machines, and on-board control systems were brought together in analysis sessions. They had to find a common language for discussing the requirements, design, programming, and testing of the system functions.
- In line with the system-safety concept, the risk analyses are done at the right time and in the right phase of the system-requirement specification and system design, either in the system-platform development project or in the customer-application project.

The risk-assessment approach and risk-analysis methodology have been utilised and also transferred to the company's systems-engineering and project-management practices. The safety-engineering procedure has been developed in light of the experiences and methods from the project. The analysis tools and documentation templates have been modified to suit the documentation and quality standards at the company. 'Modification of this applied system-safety approach to fit our design process and actual work practices will better facilitate and simplify future automation projects,' one of the interviewees said. In the same context, the importance of the risk analyses and their documentation was emphasised by the system supplier. The documentation was said to be important for the logic behind the design decisions and for tracing the conditions and constraints of the safety requirements. The reasoning is not merely grounded in one particular person's way of thinking or experiences.

According to one of the interviewees, the analysis methods were new to the system supplier's designers and also to both customers' and the system supplier's consultants in the project. It was important to introduce such methods as OHA and HAZOP study and explain why they are used, what the outcome of these methods is, and how the results will be utilised in the automation project. After the project discussed here, which was carried out in 2006–2008, the system supplier noticed that the system-safety approach and requirements for risk analysis and related documentation had been passed on to customer demands in the container-handling

automation system sector. In practice, the requirements related to the system-safety approach can now be seen in invitations for tenders in this sector of industry.

PHA, as part of the conceptual design of the automatic crane system, helped to specify the baseline for system-safety requirements. The analysis rubric has not been updated since the project. The OHA report and worksheets turned out to be good work documents and were discussed and updated jointly with the customer almost weekly in the design phase. The OHA aided in customer negotiations. 'It became clear right at the beginning of the project that we had to develop a systematic method of safety engineering. We had to show the customer how we have analysed the system. We had to show the extensive documentation of what we have done and why. Without systematic risk-assessment methodology and documentation, we would have faced difficulties in system validation and system-acceptance negotiations,' said one of the system supplier's experts interviewed.

The OHA document was considered a useful and practicable work document. It describes the system operations and functions at such a level that all system designers, with different technological background, can take part of the analysis and discussion of the system-development proposals and safety measures. In new customer projects, the OHA is updated on the basis of the application-specific issues, and machine-level risk analysis documents are updated only if there will be changes in machine functions.

According to the system supplier, the HAZOP studies conducted in the risk-assessment assignment were extensive and useful. These studies in the project were done mainly for the automation platform, and the results have been utilised in new automation projects; however, HAZOP studies have not been conducted since the automatic stacking-crane application project. The free software tool SISTEMA (Safety Integrity Software Tool for the Evaluation of Machine Applications) has been used for the verification of safety-related functions in machine-control systems. The software assistance provided by SISTEMA is introduced by Huelke and colleagues (2008), among others. Function-level drawings created for the HAZOP studies have proved to be useful not only in risk analyses but also as a way of sharing information within the design teams of the company and its subcontractors. 'This project was a good learning experience and good training for us all. The way of representing the function-level information, as in modules and their interfaces, has been further developed since,' described one of the interviewees.

According to the interviews with the system supplier's experts, further research should be directed toward the improvement of system-safety-information management through, for example, continuation of the development of the database application utilised in the HAZOP studies. Further research should also be directed to the reliability and usefulness of the functionality-related safety design and evaluation criteria in complex machinery applications. The database tool used in the assignment's HAZOP studies has been used in forming a baseline for further development of the functional safety requirement management toolkit in the company. Reuse of the analysis information in new automation projects has been one of the motivations for the development work. Analysis results were placed in traceability matrices for allocation of the safety design and verification actions as

far as software module level. Traceability matrices have been found useful for discussion and management of the allocation of safety measures in collaboration with the customer, especially the safety instructions. There is still need to find or develop a practical tool or set of tools that could manage the information from requirement specification up to the level of test cases.

The interviewees stated that system analysis for reliability-engineering purposes and for safety-engineering purposes are typically carried out separately. The findings have been transferred from safety experts to reliability experts and vice versa. Information exchange between these two engineering activities could have been more systematic. According to one of the interviewees, it would be a good idea to have a reliability-engineering expert at OHA or HAZOP meetings. Another approach might be the risk-analysis leader having enough knowledge of reliability engineering to identify and collect the reliability issues for further analysis.

The risk-estimation methodology has to be modified and calibrated to match the machinery and the system products. The methods described in functional safety standards seem to lead systematically to excessively high performance or safety integrity requirements. 'We are designing and manufacturing not rockets or nuclear power plants but mobile work machines,' said the system supplier's expert. The standards need to be considered guidelines and tools to support the company-specific risk-estimation and risk-evaluation methodology development. Layers-of-protection-centred thinking should be applied in systems-engineering practice. Designers have faced the question of what can be accepted as risk-reduction measures. How much can risk reduction come about through skilled and trained operators and maintenance staff? At the same time, how much should use experiences with a certain machine type, safety data, and reliability data be considered in risk-evaluation and risk-reduction processes?

Testing has a vital role in ensuring conformity to the specified safety requirements. Inclusive safety verification via testing is a laborious task in complex machinery applications with numerous safety-related functions, at several levels of the system. Research should be done to examine the theoretical basics and options for cutting back on integration testing and site acceptance testing through systematic safety verification and safety validation by analysis. Currently available methods using virtual-model-based testing such as hardware-in-the-loop (HIL) testing should be studied more specifically for mobile work-machine systems.

In general, utilisation of virtual models and simulators in system-safety engineering was deemed an important objective for the future. The need for virtual models and simulators is emphasised in the conceptual design of unique complex machinery systems. 'As the role of intelligent and flexible safety systems grows essential, being able to demonstrate the safety-system functions is important. Three-dimensional models, virtual environments, and machine simulators support the communication with the customer from the early conceptual design stage,' said one interviewee.

Risk-assessment efforts, as in this case, typically concentrate on the operation and maintenance phase of development of the automation system. Phases in the system life cycle such as building the infrastructure and machinery on the site,

testing the machinery system, integrating the subsystems, and commissioning the entire application should also be covered in the risk analysis. Analysis of these issues should commence in the early stages of system specification and system design in a customer-application project. The area where an automatic crane system will enter operation resembles a construction work site during the building and testing period. The methodology for risk analysis should be developed to identify and estimate risks related to the work-site elements such as temporary work platform and access arrangements, lifting and moving operations, external personnel, and machinery and vehicle traffic. Typically it is not possible to shut down a specific container-storage area: container-handling operations continue in parallel with the building and testing of the new application.

8.3.2 Observations

The system-safety approach and the analysis methods were new to the system supplier's experts. Quite a lot of effort was expended in the beginning to introduce the methods and work practices. As the methods became familiar and the benefits of the systematic analysis became evident to the analysis team's members, the analysis work moved on efficiently.

The risk-assessment approach and the analysis methods were introduced to the end customer and their safety consultants at the start of the assignment. The acceptance of the approach and the risk-analysis methodology, together with constructive co-operation in the project organisation, was motivating and helped with the system-safety-engineering work in the project consortium. The work followed the customer project's main timetable. The analysis sessions were carried out by means of said team's meetings. Experts with the system supplier participated actively in the meetings, and these meetings served system-safety-training purposes too in the early stages. The opportunity to receive feedback from the end users and their safety consultants was valuable and assisted in giving the documentation more specific and practical form.

The integration of the risk-analysis results into the system-analysis phases of the systems-engineering process applied the system-safety approach. The PHA results were utilised for specification of system-safety requirements in the conceptual design phase. The hazards identified in the conceptual design phase and the conceptual safety solutions were used as a baseline for customer-site-specific OHA. With the PHA, the general needs and conceptual requirements for the overall safety system were identified. In the OHA, the safety risks were analysed in more depth in relation to system operations and the main system functions. Also, the functionality-related safety requirements were proposed in the OHA, including the list of safety-related functions with their required safety performance level. The OHA results were passed on to the system-design team for evaluation of the risks and the means of their reduction. The safety-system HAZOP study then concentrated on verification of the specified safety functions and assessment of their ability to meet the functional safety requirements set.

The PHA was focused on the automatic stacking-crane block and related activities at both ends of the block. The PHA in the conceptual design phase produced a hazard list, accident scenarios, and greater understanding of the main safety risks, especially at the critical interfaces between automation operation and manual machines. One of the main outputs of the PHA was the conceptual safety solutions. The risk-evaluation discussion and creation of conceptual safety measures were carried out from the system supplier's point of view. Because of the nature of the container-handling process and the manual loading and unloading operations, the risk evaluation was extended to beyond the ASC block. The PHA team identified risk-reduction possibilities at a higher terminal operation level too, which could be applicable also in the larger container-storage area where the ASC block was to be situated.

OHA was carried out concurrently with the operation-concept specification work. In this case, the system specifications came from the terminal operator and the system supplier specified the more detailed operation and maintenance concepts and work procedures in the system-design phase. Use-case descriptions were defined for the specified system operations in OHA. These descriptions covered various human–human and human–technology interactions. The human–human interactions in this case include communication and co-operation between control-room operators and of control-room operators with on-site operators and on-site maintenance teams. Human–technology interactions involved such elements as control and monitoring of automatic operations, crane tele-operation, and driving of a manual machine in line with the automation system's guidance. Operation concepts and use cases were analysed in collaboration with the project team's members, with the results passed on directly to the system-design team.

In the OHA, the risk estimation was done in two phases, before and after the proposed safety measures, with the same 5 × 5 risk matrix used in Case 3. The probability categories and categories of harm remained the same, but the severity categories for physical damage were modified to match the context of the type of container-handling application involved. The methodological problem discussed for Case 3 was recognised in this case too with the 70 items in category 1, 'multiple-fatality'. Even though the probability of the occurrence of harm could be reduced to 'very unlikely' (harm can occur only if several errors or failures occur at the same time), the risk remains of 'medium' level. Colour codes ('traffic lights') were used to highlight the risk levels (high, medium, and low) in OHA documentation. That was considered more informative than numeric values taken from the matrix elements. It also helped those involved to recognise the difference and change between risk-level estimates before and after the safety measures.

The HAZOP study of the safety system was performed in the system-design phase to verify safety functions. This study was done at signal level. Function-level drawings were created by the system supplier, and again the drawings turned out to be informative work documents for the analysis. From the systems-engineering point of view, it could be noticed that they added value, forming a baseline for the system design and providing a tool for sharing of information among several hardware- and

software-design groups. The changes, including improvements, proposed and those accepted were transferred directly to the system-design stage.

Recording of the HAZOP study's results applied a data-collection worksheet implemented with an MS Access database application. This was the first attempt to use such a tool in HAZOP studies in this context. According to the researchers' comments during the analysis in this case and again in the interviews in 2012, this experiment provided many good user experiences and improvement proposals not only for risk-analysis documentation but also addressing how to improve the database-centric information management in systems engineering in general. The present researcher's experiences and observations were mainly positive. This tool yielded benefits in the HAZOP analyses, in the following respects, among others:

- Time savings due to ease of data input and of reuse of the existing data
- The tool enabling users to search for important data from the analysis, in addition to modifying and copying of input data
- Easy linking and simple access to material – for example, linking of use-case descriptions to function-level descriptions of design intent
- Assistance for more systematic practice in analysis sessions, pop-up-type checklist-style menus, and integrated session protocol sheets supporting the practical analysis work
- The capability of utilising database features for reporting applications
- Easy modification of reports in comparison to work with Word documents
- A more appropriate tool when data are in databases and published in forms such as PDF documents rather than Word or Excel files.

The HAZOP study sessions were utilised not only for the risk analysis but also in the design and evaluation of the safety system under study. The study sessions formed a good forum for the team's discussion and sharing of information on the safety system's functions and features. The team reviewed changes made in the design, and they discussed and evaluated alternative operation- and function-oriented solutions. Analysis of consequences of deviations in HAZOP studies succeeded well in an analysis team comprising experts from various design teams, who worked with system, hardware, and software design. The risk-estimation method with its three risk levels supported the creation of the list of proposals for actions and their prioritisation.

8.4 Discussion

The system supplier's work involved designing and manufacturing an automatic container-handling system for their customer. The co-operative work on risk assessment was planned and conducted to support the development and design of the new, unique container-handling application using three automatic cranes in

one block. The three-level risk-assessment approach and the well-known safety-engineering methods PHA, OHA, and HAZOP study, together with the modified 5 × 5 risk matrix method of risk estimation, were agreed upon for addressing the system-safety-engineering needs and problems. The system-safety work started early in the conceptual phase and continued throughout the system-development phase, up to the verification of safety-system elements and safety-critical parts of the system control functions.

Systems-engineering guidelines do not name specific analysis methods for system-safety activities, but it is strongly emphasised that the initial hazard analysis for the system of interest should be started as early as possible in the conceptual design phase and should be continued throughout the system life cycle (SE Handbook 2011, p. 325). Also, ISO IEC 26702:2007 (p. 41) specifies that in the requirements analysis sub-process of the systems-engineering process (see Figure 12), the project must account for system-design features that create significant risks of death, injury, acute or chronic illness, or disability. The project should also account for design features that reduce operators' or the maintenance personnel's job performance. Since the systems-engineering process is meant to be applied iteratively throughout the system life cycle, these issues should be considered from the early concept-level requirement analyses.

The system-analysis phases in the systems-engineering process are requirement-related studies and assessment, functionality-related studies and assessment, and design-trade studies and assessment (ISO IEC 26702:2007, p. 12). In this case, the three risk-analysis and risk-estimation methods were utilised in various system-related phases in the life cycle and for system-analysis purposes. In the concept and (partly) the preliminary system-design phases, PHA was used mainly for the requirement specification, in the creation of the list of hazards and accident scenarios and in preparation of the preliminary estimation of risks. As the customer-specific application project began, the preliminary design continued and detailed subsystem design started. The OHA was used partly for application-specific specification of safety requirements and partly for the subsystem functionality-related trade studies and assessments. The OHA was used to identify and analyse hazardous events related to system operations and the main system functions in more detail. In this project, HAZOP studies were used for design-trade studies and assessment, to support the detailed subsystem design and fabrication. The HAZOP study that is examined in this case study was used to analyse deviations from the design intent behind the safety-related functions or critical signals and to validate the functionality-related safety designs.

According to the system-safety literature, the bulk of the system-safety activity in the conceptual phase consists of the preparation of a preliminary hazard list (PHL). The preliminary analysis of hazards should be carried out and updated in the system's design phase (Stephenson 1991, pp. 15–16; Stephans 2004, pp. 64–65). Stephans (2004) emphasises that, even though the primary purpose of PHA in the design phase is to analyse previously identified hazards and to propose safety measures to reduce the risks, the hazard analysis should be continued throughout the design phase. The focus should be on the identification of new hazards and

hazardous events, especially in relation to system interfaces and changes in system design (ibid., p. 65). In large hierarchical systems with several levels of subsystems or in large distributed systems, analysis methods such as subsystem hazard analysis (SSHA) or system hazard analysis (SHA) can be used to supplement and update the PHA. These techniques can be considered technology-oriented analyses. The aim of SSHA is to go into hazards associated with one or more subsystems in more detail (Vincoli 2006, p. 85). In automated mobile-machinery applications, SSHA could be conducted for safety-critical subsystems such as primary safety systems and tele-operation systems.

In this case, the PHA was carried out in the concept phase, with the hazard identification, preparation of the PHL, and preliminary estimation of risks being combined. The timing and outcome of the PHA suited the systems-engineering process well. The PHA was limited in scope to a one-automatic-container-crane block and covered all the main interfaces to manual machine operations associated with that block. Preliminary proposals for safety measures for various layers of protection were discussed: system supplier's measures to safeguard and control the automated area and requirements for the end user to take the measures necessary in the surrounding infrastructure for the overall system to be operated and maintained safely. The PHA results formed the baseline for system-safety requirements and provided information to the system designers for system-performance and system-design specifications. In that sense, the preliminary risk analysis and the risk-estimation work in this case follow the approach described by Roland and Moriarty (1983, p. 195).

In the system-safety literature, the stated purpose and objectives, along with the guidelines for the timing of the OHA, vary. Vincoli (2006, p. 93) expresses the purpose of OHA as being to identify all hazards in system operation that are inherently dangerous to personnel or involve human error that could be hazardous. The OHA should also recommend risk-reduction alternatives for tasks or operations that are controlled by means of written procedures. According to Stephans (2004, pp. 66, 82), OHA can be used to analyse hazards associated with the maintenance and operation of the system. Special emphasise should be placed on human factors, procedures, training, and the human–machine interfaces. In a way, these definitions already carry presumptions as to the information and documentation required, including that necessary for the successful execution of OHA. It is commonly stated that operating hazard analysis (also called operating and support hazard analysis, or O&SHA) should be done as early as possible in the design phase (Stephenson 1991, p. 78; Vincoli 2006, p. 95). On the other hand, it is stated also that OHA should be considered an important system-safety activity in the system production phase, when system design is nearly completed and the operation and support procedures have been developed (Vincoli 2006, p. 95). Stephans (2004, p. 82) indicates that the ideal timing for OHA is largely dependent on the nature of the system in question. In some cases, updates to an existing production system or facility might be involved, while in others a totally new system, including prototyping and testing, is being developed. In the latter type of case, the OHA

may be conducted late in the design phase and updated periodically throughout system development and production.

Systems-engineering guidelines emphasise the role of human–systems integration work (HSI) in systems engineering in complex industrial applications. It has been said that HSI consists of the interdisciplinary technical and management processes that integrates human considerations across all system elements. Human–systems integration is said to bring human-centred discipline and concerns to the systems-engineering process iteration and improve the system design and system performance in general (SE Handbook 2011, pp. 328–331). From the overall systems-engineering standpoint, human–systems integration has quite a wide scope, encompassing the following human-centric domains, among others: manpower, personnel, training, human-factors engineering, operation environment, safety and occupational health, habitability, and survivability (ibid., pp. 332–337). All of these domains have their own specific analysis and assessment methods and tools that could be utilised in the systems-engineering process and system-analysis phases. The experiences and observations from this case and comments from the system supplier's experts interviewed indicate that the OHA-type analysis method implemented turned out to be a practical tool for integration of the above-mentioned important human–systems-integration elements. Personnel involved expressed that the analysis and assessment of system operations and procedures with OHA supported the development of system-operation concepts, safety requirements' specification, evaluation of operation procedures, and proposed safety measures related to them.

In this case, the risk estimation in OHA followed the same two-phase method employed with OHA in Case 3. Firstly, risks were estimated before any safety measures; then they were estimated with all proposed conceptual, application-specific, and existing-site-specific safety measures taken into account. Although the container-handling process and the machinery were well known to the system supplier's experts, the operation and maintenance concepts in this case were new. In fact, the operation and maintenance procedures were, in part, created and defined in parallel with the risk-analysis work. For these reasons, difficulties were faced in the first estimation of the factors affecting the probability of the occurrence of harm: people's exposure to the hazard, the occurrence of a hazardous event, and the technical and human possibilities for avoiding or limiting the harm (SFS EN ISO 12100:2010, p. 17). The risk estimation became even more complicated with the estimation of the impact of the various safety measures, such as technical means of safeguarding, warnings, instructions, and traffic rules, in terms of the three main factors in the probability of the occurrence of harm.

The risk-estimation method implemented, using the 5 × 5 matrix and three risk levels, led to discussion and confusion among the analysis teams, especially with respect to the assignment of risk levels in the matrix. For many hazards, regardless of numerous risk-reduction measures on the part of the system supplier and terminal operator, the risk level could not be reduced to 'low'; it remained at 'medium', especially in the case of the 'multiple-fatality' severity category. As was discussed above for case study 3, this can be considered a methodological issue

associated with how the matrix is built. However, in the case of catastrophic events causing multiple fatalities, the risk-estimation result remaining at medium level should indicate that the risk evaluation ought to be raised to a higher level in the system hierarchy, where the measures and safety solutions can be more effective. Risk evaluation in such cases should also lead to discussion and consideration of how to minimise the number of people exposed in hazard zones. It is quite obvious that, when several people are exposed to the hazards, the risk of some of them being injured increases if something unexpected happens.

The practical experiences and observations of risk-estimation difficulties in this case are in line with the conclusions Louis Anthony Cox, Jr. (2008), has come to with respect to the utility of risk matrices in risk-management decision-making. He claims that risk matrices do not necessarily support good risk-management decisions or effective allocation of risk-reduction resources. According to Cox (ibid.), risk-management decisions cannot be based in principle only on mapping of ordered category ratings of severity and probability factors to recommendations for actions or priorities. Risk matrices should be used with caution. The reasoning and judgement behind the risk level, just as much as the information related to each matrix element, should be carefully explained for those interpreting the risk-estimation results (ibid., p. 510). This reflects the approach that is emphasised in BS 18004 (2008), according to which the ALARP ('as low as reasonably practical') safety-engineering principle and cost-effectiveness analysis should be applied for risks of between acceptable and unacceptable level, for finding appropriate and effective safety solutions (ibid., pp. 84–85).

Vincoli (2006) has developed the risk-estimation matrix further for the system-safety process by applying hazard severity categories and hazard probability levels from MIL-STD-882D (2000) (see Figure 36). In that matrix, there are four severity categories, five probability categories, and four risk levels. The probability represents qualitative estimation of the likelihood of occurrence of harm caused by an uncontrolled or uncorrected hazard relative to the lifetime of the item or system in question. Risk levels are expressed thus: red denotes unacceptable risk (changes must be made), orange is for undesirable risk (make changes if possible), yellow means 'acceptable with management review', and green stands for 'acceptable without review' (Vincoli 2006, pp. 14–16). The risk-classification principle clearly directs the risk-evaluation decision-making and connects it to the correct level of project management or company management.

	Severity			
Probability	Catastrophic I	Critical II	Marginal III	Negligible IV
Frequent (A)				
Probable (B)				
Occational (C)				
Remote (D)				
Improbable (E)				

Figure 36. Risk-estimation matrix modified from Vincoli (2006, p. 16).

One of the system supplier's experts who were interviewed for this case study summarised the discussion of risk-estimation methodology by expressing that standards and theoretical models need to be considered to be guidelines and tools for supporting the company-specific risk-estimation and risk-evaluation method development. The methods must be calibrated to match the internal and external context of the company. He also referred to the ALARP approach and emphasised that layers-of-protection thinking should be applied more extensively in system-safety engineering and risk evaluation.

In this case, HAZOP studies were carried out in team meetings and the results were recorded by means of a database application instead of in Word documents or Excel sheets. The data-collection method and worksheet template were implemented with MS Access database application. User experiences were described as positive both by the researchers who used the tool and by the system supplier's expert who took part in HAZOP sessions. The database tool supported the systematics of HAZOP study, saved time, and brought the analysis data's management to a new, more practical and appropriate level. According to Dunjó et al. (2010, p. 28), most HAZOP studies in the process industry are carried out by expert teams and are subject to the availability of expertise, experience, and creativity. Knowledge should be gained from the experience of various parties, and HAZOP structure for systems that represent equivalent technology could be standardised. The HAZOP standard (IEC 61882:2001) should be improved and updated to reflect the state of the art in the industry.

The idea of a database-based tool for HAZOP studies is not new or unique. Knowledge-based HAZOP tools have been developed over the years to aid in or even automate HAZOP analysis; however, many of them have been created to support and automate process hazard analysis in production systems in the process or chemical industry (Pátkai 2006, p. 23; Dunjó et al. 2010, p. 26). Though there are many commercially available documentation and data-management tools designed specifically for HAZOP analysis, it seems difficult to find solutions that are easy to use and tie in with the systems-engineering and system-design tools and software and with hardware-development environments seen among

mobile-machine manufacturers and their subcontractors. Informed in part by experiences from this case, the system supplier has continued the development of methods and database tools to support system-safety-information management from safety-requirement specifications to test cases and functional safety validation.

The evolution of HAZOP methodology has been studied through a review of literature on HAZOP research and development in the process industry over the last 15 years (Dunjó et al. 2010). Three main areas of recent research interest were identified: sharing of analysis experience, methods suitable for programmable electronic systems, and expert systems for automating HAZOP studies. Results from the process-industry sector emphasise also that research should be devoted to such issues as human factors, for better identification of events caused by human error; deviations and hazardous scenarios created by programmable electronic systems, to enable support for functional safety engineering and evaluation of levels of safety integrity; and standardisation and automation of HAZOP studies, to allow application of the latest knowledge of process engineering, dynamic simulation, and artificial intelligence (ibid., p. 28).

The future research needs expressed for risk-analysis methodology in this case are consistent with the above-mentioned results from the process-industry sector. The importance of systematic consideration of human factors and identification of critical human errors in system operations were discussed in upper-system-level analysis by means of OHA. Control-system design and testing methods that employ virtual-model-based testing, such as hardware-in-the-loop testing, can be considered to be an application of automated HAZOP study wherein failure modes are simulated or physically injected at the system interfaces and the system respond is recorded and analysed automatically.

8.5 Conclusions

The objective of the case study was to evaluate the usefulness of the three-level approach to risk assessment in relation to the systems-engineering approach and the utility of PHA, OHA, and HAZOP methods in the complex automated cargo-handling application in early parts of its life cycle.

From the analysis results, comments from the system supplier, and observations, it can be concluded that the three-level risk-assessment approach and the risk-analysis methods met the objectives well, providing the project team with applicable and systematically supported information for risk-conscious decision-making. One can also conclude that the risk analysis and risk evaluation brought added value to the system-analysis stages of the supplier's systems-engineering process and aided in meeting application-specific system-safety requirements and ensuring safe operation of the complex automated mobile-machine application. The system supplier's experts interviewed stated that they had not been notified of any reportable injuries associated with the automatic stacking-crane system.

The system supplier indicated that the three-level risk-assessment approach and the analysis methodology were accepted by the end customer, which suggests that the approach fits the automation projects using automated mobile work machines in a container-terminal environment. The system supplier has even noticed that the system-safety approach to analysis methodology and the related documentation principles applied have trickled down to customer demands in the container-handling automation system sector. In practice, the requirements related to the system-safety approach can now be seen in invitations for tenders in this branch of industry.

The PHA was carried out in the conceptual design phase, combining the hazard identification, preparation of the preliminary hazard list, and preliminary estimation of risks. The timing was appropriate for the system-development project, and the outcome of the PHA and the preliminary risk estimation formed a baseline for the hazard list and for preliminary safety requirements and conceptual solutions for automatic stacking-crane applications.

The upper-system-level risk analysis of system operations and main system functions was carried out with OHA and a two-phase risk-estimation procedure. It can be concluded that they fulfilled the system-safety objectives set for that level because the system supplier stated that they have adopted the OHA method and developed a company-specific applications of it for new system-development projects and for customer-application projects.

The HAZOP methods utilising function-level drawings and a new database tool for data collection and documentation worked out well with respect to the automation platform and for safety-system-validation purposes. Systematic methodology and support tools received positive feedback both from the system supplier's experts and from researchers. The database tool added value to the HAZOP studies by improving the systematics of the data collection, reporting, and reuse of the data. The system supplier used the database tool for a baseline for further development of the company's functional safety requirement management toolkit and for integration of the analysis data into other system-design tools. The analysis of consequences of deviations in the HAZOP studies succeeded well in multi-technology analysis teams.

The case project made a valuable contribution to the development of the three-level risk-assessment approach and to the risk-analysis methodology. In this case, the focus was on risks related to the operation and maintenance of the system of interest. The system supplier stated that the scope of the systems engineering and risk analysis should be widened to encompass also system installation, building, and testing phases on-site. The work site is, in practice, a long-term construction site and cannot be considered or analysed as a production system in these parts of the life cycle. The system-level risk-management co-operation becomes all the more important in such large-scale machinery applications. System safety is an issue of the project's risk management, a matter of system-safety engineering for the system of interest, and an issue involving the end user's occupational health and the on-site safety management.

The risk-estimation methodology and the interpretation of the risk levels output in the risk-estimation results should be developed so as to support the decision-making in risk evaluation and trade studies better in requirement, functionality, and design analyses in systems-engineering processes. Our risk-estimation method as utilised in this case seems to lead to excessively high requirements as to performance levels or safety integrity levels. The risk-estimation method should be tailored to and calibrated for the machinery and system of interest, along with the internal and external context of the company. Applications of the functional safety approach and of layers-of-protection thinking seem to have become *de facto* standards also in this branch of industry. The three-level risk-assessment approach and analysis methods should be developed to support these common practices.

The results indicate that further research should be directed toward the improvement of system-safety-information management by such means as continued development of the database application utilised in the HAZOP studies. Further research should also address the reliability and usefulness of the functional safety design and evaluation criteria in complex machinery applications.

9. Discussion

9.1 The usefulness of the three-level approach to risk assessment

This chapter discusses the usefulness of the three-level approach to risk assessment in light of the case studies' results. This evaluation of usefulness can be formulated as a question: Did the three-level approach to risk assessment support the company in reaching their safety-engineering goals and solving the system-safety problem? Utilising the case-study research method described above and the case-study material available, the evaluation in this study considers the benefits and impacts of the approach for the systems in question and for the companies' safety-engineering practices. Here, case-study results, experiences, comments, and observations as to usefulness are summarised and discussed, case by case. Possible similarities and differences between cases are discussed.

Case 1: The existing ore-transportation system

The objective of the risk-assessment work in Case 1 was to evaluate the safety of an automated ore-transportation system and to assess its conformity to the European machinery-safety directive in force at the time. The target system was a semi-automatic LHD machine application in an underground iron mine in northern Sweden. This system was the first of its kind in production use. That the mining company accepted the approach to risk assessment and the analysis methods suggests that the approach suits the evaluation of automated mobile work machines in the mining industry. The mining company stated that the analysis and assessment work gave them valuable information about the automation-related risks and on the current status of the safety risks of the semi-automatic ore-transportation system. The top-down approach to risk analysis at three levels of the system supported the overall safety evaluation and conformity assessment of the complex automated mining-machine application. The case-study results confirm that, with the aid of system thinking, the traditional risk-analysis methods PHA and HAZOP study were successfully directed at identification of new unforeseen hazards and hazardous events and of possible indirect effects causing hazardous relations and consequences. System thinking supported risk evaluation

and specification of improvement proposals for development of the safety functionality at an appropriate level of the system hierarchy. The interview results revealed that no automation-related accidents caused by the automated machinery had been reported to the machine manufacturer at any point between completion of the risk-assessment assignment and the system's decommissioning a few years ago. It can be claimed that the approach to risk assessment at three levels, no matter the recognised weaknesses in the analysis and assessment methods, was appropriate and supported the safety evaluation and conformity assessment of the semi-automatic LHD machine application.

Case 2: The ore-transportation-system concept

The system-safety work in Case 2 was designed to examine potential automation-related safety risks for the new automated mining-machinery concept and to specify safety requirements for the system under development. The target system concept included control of the autonomous LHD machines and dump trucks in underground mine tunnels and all of the automation system elements in the control room. The PHA and HAZOP methods were utilised to cover the system concept from overall system level down to the on-board control system level. According to the machine manufacture's comments, the approach to risk assessment added value to the automated ore-transportation system concept's development and system-verification work. The system designers indicated that the project was a good learning process. Systematic analyses throughout the work on the automation-system concept helped us to understand subsystem operations, system functions, and interrelations between subsystems. Also, reports and subsystem analysis documents formed a good baseline for the technical construction file and conformity assessment of the system concept. The machine manufacturer stated that most of the results were directly transferable to the mine-automation development team for consideration in system-development work. The documented approach and analysis methods were directly applicable in new research and development projects and further automation-system analysis. It can be assumed that the approach applied at three levels of the system, supported the machine manufacturer's system-development and safety-engineering work, regardless of the recognised weaknesses in the analysis and assessment methods used. According to the machine manufacturer, no accidents associated with the relevant automated ore-transportation systems had been reported to said manufacturer since the first application entered use, about 10 years ago.

Case 3: The ore-transportation application

In Case 3, the objectives of the risk-assessment assignment were to identify and analyse automation-related safety risks and case-specific safety factors in an underground diamond mine in South Africa. The goal was to specify safety requirements for the application and determine the necessary risk-reduction measures for the application and allocate them. The automatic ore-transportation system utilising autonomous dump trucks was unique, the first of its kind in the

underground mining industry. The risk assessment at three system levels and the analysis methods were accepted by the global mining company, which suggests that the approach is a good match for automation projects related to automated mobile work machines in the mining industry. According to the case-study results, comments from industry partners, and observations, the three-level approach to risk assessment, applying PHA, OHA, and HAZOP methods and qualitative risk-estimation principles, was suitable and practicable in the customer project. The top-down approach to risk assessment supported the system supplier's systems-engineering process in the automated mobile work-machine system. The utilisation of PHA results for OHA and HAZOP studies and the precise descriptions of hazardous events, deviations, and causes and consequences aided in the analysis work. The generic system-safety-engineering model created at NIOSH for the mining industry recommends the use of these methods for safety-critical surface or underground mining systems employing embedded and networked programmable electronics (Sammarco et al. 2001; Sammarco 2005b). According to the mining company's and system supplier's experiences and comments, the objectives of the risk-assessment work were reached. Both the mining company and the system supplier confirmed this opinion by reporting experiences of safe and efficient operation of the system. The system supplier adopted the three-level approach to risk assessment and developed a company-specific application of it. The overall system-safety work is being further developed to mesh better with the functional safety engineering objectives. Application of a functional safety approach and LOPA thinking seem to now be *de facto* standards in the mining sector. The three-level approach to risk assessment and analysis methods should be developed to support these common practices.

Case 4: The container-handling-system concept and its application

The approach to risk assessment was further developed and evaluated in the joint research project in co-operation with the cargo-handling-equipment manufacturer (the system supplier) in Case 4. The system supplier was developing an automatic stacking-crane concept at the time. Later, that supplier delivered a customer-specific application of the concept to a terminal operator in Germany. Co-operation continued with the risk-assessment assignment related to the customer application. The system supplier stated that the approach to risk assessment utilising analysis methodology at three levels of the system was accepted by the end customer, which points to the approach as suitable for automation projects using automated mobile work machines in a container-terminal environment. The system supplier noticed that the system-safety approach, analysis methods, and documentation principles have been passed on to customer demands in automation projects in the global container-terminal industry. It was noted that both application of the functional safety approach and LOPA thinking seem to have begun becoming *de facto* standards also in this sector of industry. According to the results of Case study 4, comments from the system supplier, and the author's observations, the three-level approach to risk assessment and the risk-analysis methods fulfilled

the objectives specified for the projects. The system supplier has adopted parts of the approach and methodology and developed a company-specific application of it for new system-development projects and for customer-application projects. The top-down approach at three levels of a system provided applicable and systematic reasoning for risk-conscious decision-making for the system concept's development and for the customer-application design. It can be claimed that the system-safety work added value to the system-analysis phases of the supplier's systems-engineering process and aided in defining of the application-specific system-safety requirements and verifying of the safety-related functions. The system supplier reported not having received any reports of reportable injuries related to the automatic stacking-crane system.

9.2 The usefulness of the risk-analysis methods

This chapter discusses the usefulness of the three risk-analysis methods (PHA, OHA, and HAZOP study) as utilised in the case projects. The basis for the evaluation criteria in this study lies in the available case-study material and the case-study research method employed. In this study, the evaluation involves considering benefits, possible limitations, and pros and cons of the methods in their intended use in the relevant stage in the system life cycle in the case projects. The discussion covers issues such as how the work proceeded, how much effort was needed, how many and what kinds of hazards were identified, and how many proposals were created.

Case-study results, experiences, comments, and observations related to the hazard-identification and analysis methods are summarised and discussed for each analysis method. Factors affecting the quality of the risk-analysis methods, such as definition and limiting of the objectives; specification of the analysis method; organisation of the analyses; their execution, and reporting on the analyses are discussed not systematically but on the basis of experiences and observations, when doing so is relevant. Also similarities and differences between the finding or case specific issues in the results are discussed. No comparison of results between cases is conducted, because the cases were all unique and their objectives were specified in line with the phase in the system life cycle that was relevant.

9.2.1 Discussion of the PHA method

In Case 1, PHA was applied for evaluation of the existing semi-automatic ore-transportation system. The analysis team was composed primarily of experienced mine operators and service workers. The company representatives had experience of risk-analysis team work, job-safety analyses, and safety analyses of work equipment and machines. Overall risk analysis of the target system had not been carried out before. According to PHA-team comments and researchers' observations, the method, using brainstorming and scenario-analysis techniques, systematic job-safety analysis, and team-discussion technique, was practical and

efficient for analysis of the operation situations and in identification of potential hazards of the existing automated mobile machine system in the mine. The case studies' results support the view expressed by writers on system safety such as Leveson (2003, pp. 7–8) and Vincoli (2006, pp. 37–38) that PHA is an applicable method not only for new complex system concepts but also for such systems in actual use. The results highlight that the scope of the PHA should have covered automation-related work tasks on the machine too, such as troubleshooting of the on-board control systems and maintenance of the on-board automation components. Also, improvements for more systematic and unambiguous documentation of the results were proposed for the PHA method.

In case 2, the main objective of the PHA in the conceptual design phase of the automated ore-transportation system was to identify potential hazards and analyse the possible consequences in the underground production environment. The scope of the PHA was the full life cycle of an automated production area. The analysis methodology was the same as in case 1. The PHA team's members in this case were the manufacturer's automation experts and system designers. According to the industrial partners' comments and the author's observations, the analysis method utilising brainstorming sessions and team discussions was easy to learn and suitable for hazard identification and analysis for an automated mobile work-machine system in its conceptual design phase. This result supports general system-safety guidelines according to which PHA is especially usefull in the concept-design phase (Vincoli 2006; Stephenson 1991; Roland and Moriarty 1983). This result is also in line with the generic system-safety reference model developed for the mining industry, which implies the utility of PHA in early phases of the system life cycle (Sammarco et al. 2001; Sammarco 2005b). According to this case study, precision in the descriptions (of hazards, causes, and consequences) on analysis worksheets and in the reports is important and affects the reliability of the analysis results. The levels of consequences should be determined accurately, and separation of personal-safety effects from other consequences, such as physical damage or production loss, is essential for the risk estimation and evaluation.

Case 3 was a customer-application project. The objectives of the PHA in this case were to identify hazards and hazardous events of the autonomous ore-transportation system in the customer-specific environment on a new production level in the underground mine. The practical work method in this case differed from the traditional analysis-team sessions described in standards and in system-safety literature. Researchers prepared the analyses, and the draft results were distributed within the project team and discussed in review meetings with mine-safety experts, system designers, and automation experts. Conducting the PHA in stages and synthesising researchers' preparation work with the expert group's review meetings worked out well and effectively in this hectic international and multicultural customer-project context. Clear delineation between personal-safety consequences and consequences such as physical damage or production loss clarified the hazard identification and aided in risks' estimation and evaluation. The results of this case study confirm our view of the importance of consideration and analysis of human factors with a wider scope and in a more extensive way in such

complex automated mobile work-machine system applications. The documentation of the hazardous events identified should be made more specific in PHA, to improve analysis reliability, traceability of the safety requirements, and linking of the safety measures to the correct risks in the risk-evaluation process. This would entail not more work effort but more systematic documentation practices.

In Case 4, the PHA was carried out in the conceptual design phase for the complex automated cargo-handling application. The PHA combined the hazards' identification, preparation of the preliminary hazard list, and preliminary estimation of the risks. Automation experts from the system supplier and researchers with VTT formed the PHA team. The PHA method, utilising brainstorming sessions for hazard identification and creation of accident scenarios in combination with team discussions for specifying causes and consequences, worked out well. The timing of PHA was fitting for the system-development project and the outcome of PHA and formed a baseline for the hazard list for automatic stacking-crane applications. The PHA results were utilised in specification of system-safety requirements in the conceptual design phase. The hazards identified in the conceptual design phase and the conceptual safety solutions were used later as a baseline in customer-site-specific OHA. In this case, PHA was focused on risks associated with the operation and maintenance of the system of interest. The system supplier stated that the scope of the risk analysis in a terminal context should be broadened to cover also system installation, building, and testing phases on the site. The risk-analysis results from these phases could be then utilised also for the entire project's risk management and for the end user's on-site occupational health and safety management.

9.2.2 Discussion of the OHA method

We carried out operation-hazard analysis for the first time in case 3 in this research. The upper-system-level HAZOP study method applied in cases 1 and 2 was replaced with OHA. The objective in OHA with respect to the hazard identification was to identify potential hazards and hazardous events in the system's operation procedures in the selected phase in the system life cycle in terms of both human error and technical failures. The analysis was carried out by means of the OHA application developed specifically for the automated mobile work-machine systems (Tiusanen et al. 2005). It was based on methodology guidelines in the system-safety literature (Stephans 2004; Stephenson 1991; Roland and Moriarty 1983). Special focus was put on the communication between the system operators and service personnel, interactions between system operators and the automation system interface, and execution of manual or remotely performed tasks. The work method in the OHA followed the procedure used in this case's PHA. Researchers prepared the analyses, and the draft results were distributed within the project team and discussed at review meetings with the system designers and automation experts. Keeping personal-safety consequences and other

consequences (e.g., damage to materials or production losses) separate clarified the hazard identification and risk estimation also in OHA.

According to the results of Case study 3, the OHA, in the form in which it was carried out in this case, seems to be suitable and practicable in automated mobile work-machine customer-application projects in the mining industry and supports the system supplier's systems-engineering process. The results of this industry case study confirm the present author's view as to the importance of consideration and analysis of human factors with a wider scope and more extensively in such complex automated mobile work-machine-system applications. Comparing OHA with HAZOP study for upper-system-level risk analysis aimed at analysis of system operations, one finds that OHA provides support for the creation of new views of operation situations and human factors. The approach of HAZOP study is limited to the designed, intended use of the system, and in this sense OHA is a PHA-type hazard-identification and analysis method (Roland and Moriarty 1983, p. 210). It seems that the analysis of operator errors should be broadened to cover the factors related to the operation situations, operation environment, and factors enabling and supporting the intended, correct, and safe operation. Leveson (2011b) proposes that the analysis of humans' role in accidents should be focused not on human error or violation of rules but on the mechanisms generating the relevant behaviour in the dynamic operation context. Traditional task analysis could be replaced with cognitive work analysis or cognitive task analysis (ibid., p. 46).

In Case 4, OHA was carried out concurrently with the system-specification and system-design work for the automatic-stacking-crane-system customer application. The objective of the OHA in this case was to identify automation-related hazardous events in system operations and maintenance procedures. The hazardous events, their causes, and the consequences were identified by means of brainstorming and team-discussion techniques. The analysis team was composed of automation designers, system designers, and researchers. Use-case descriptions covering various human–human and human–technology interactions were defined for the specified system operations in OHA. The OHA report including worksheets was considered a useful and practicable work document, describing the system operations and functions at such a level that all system designers, with diverse technological backgrounds, can take part in the analysis and discussion. The OHA report turned out to be good work document also in project meetings with the customer. OHA report was discussed and updated in collaboration with the customer as the system design progressed. The results of this case study support the commonly expressed view that OHA should be done as early as possible in the design phase (Stephenson 1991; Vincoli 2006). It can be claimed that the OHA met the system-safety objectives set for the level in question, because the system supplier reported having adopted the OHA method and developed tailored applications of it for new system-development projects and for customer-application projects.

9.2.3 Discussion of the HAZOP method

The upper-system-level HAZOP study in case 1 focused on analysis of existing system operations, looking at both possible system-operator errors and the possible technical problems. The HAZOP team, made up of experts from the mining company, the machine manufacturer, and subsystem suppliers, had six one-day analysis meetings in Sweden. Although a HAZOP method in line with IEC 61882 (2001) was new for all industry members of the team, it can be claimed that the HAZOP method using team discussions and supported by system architecture drawings worked out well in the upper-system-level analysis of deviations in subsystem interfaces. The results are in line with those reported by Redmill et al. (1999). The HAZOP technique can be applied to operational systems just as well as system designs. It involves a structured team-work-based technique that is effective for exploring interactions between parts of a system (ibid., pp. 24–25). Because there were several analysis teams, with insufficient co-ordination among them, the PHA results were not utilised systematically in the HAZOP study. While that led to additional work, the analyses' overlap brought new views to the safety evaluation.

The objective of the lower-system-level HAZOP study in case 1 was to identify and assess safety-related deviations in the automated LHD on-board control functions in use. A HAZOP team composed of experts from the mining company, machine manufacturer, and on-board subsystem suppliers had four one-day analysis meetings in Sweden and four half-day tele-meetings. The HAZOP study conducted according to IEC 61882 (2001) did fit well in the analysis of functionality deviations of the on-board machine-control system. According to the mining company, the HAZOP studies put experts with all interested parties in the automation-development project in touch and led them to discuss potential problems and devise possible solutions and improvements. The mining company also pointed out that the proposed corrective actions and proposals for improvement specified in the project were valuable and that many of them were realised in the system-development project in co-operation with the machine manufacturer and subsystem suppliers. The new innovative function-level drawing concept turned out to be essential to efficient performance of the analysis. The traditional worksheet document turned out to be laborious to create and maintain. The overall results emphasised that clear and adequate description of the analysis findings, hazards, causes and consequences, and assessment results is especially vital in such a complex automation application system, wherein the information is shared with several partners and specialists in many fields of technology.

In Case 2, the upper-system-level HAZOP study was carried out in the conceptual design phase of the autonomous ore-transportation system. The objective in this HAZOP work was to ensure that possible deviations (human error or technical problems) in the designed system operations and in the main system functions could not create safety risks in the automated production area. The HAZOP team, composed of automation experts and researchers, had seven full-day meetings.

The system architecture drawings applied in this case turned out to be essential for integration of all function-specific information into one document and for sharing of information within the analysis team. A HAZOP method following IEC 61882 (ibid.) was new to all industry members of the team, but the automation expert learned the method easily in the first couple of analysis sessions. Given the case-study results, one can claim that the HAZOP method following standard procedure and also the team discussions supported by system architecture drawings worked out well in the analysis of operation-time human error and deviations in subsystem interfaces. The results support those described by Redmill et al. (1999). The HAZOP approach is applicable in analysis of new systems and novel technologies and for exploring interactions between subsystems (ibid., pp. 24–25). These results also support the generic system-safety reference model developed for the mining industry, which suggests using HAZOP studies early in system design for the identification of possible hazardous events (Sammarco et al. 2001, p. 5; Sammarco 2005b, p. 20).

The aim of the lower-system-level HAZOP study in case 2 was to identify possible functionality deviations in CAN-bus-based on-board control systems and analyse the effects on machine operation in both automatic and manual operation. The HAZOP team was composed of automation experts with the machine manufacturer, control-system experts with the subcontractor, and researchers. A methodological problem was faced early in the HAZOP study of the on-board control system. Analysis at signal level turned out to be too laborious for the purpose at hand and for the resources available for the analysis. The study was performed at function level instead; while better coverage could have been achieved via application of both signal- and function-based studies, only one of the two could be selected in practice. A HAZOP method following IEC 61882 (2001) was new for all industry members of the team, but the analysis method in this case too turned out to be applicable and efficient once it had been adapted to the case's purpose and practised in the first few analysis sessions. Some methodological weaknesses and inaccuracies were recognised during the study sessions, along with documentation shortcomings. The definitions of the analysis levels, hazards, deviations, and causes and consequences should be clear. Personal-safety and other consequences (such as physical damage or production losses) should be separated. Since the systematic identification and analysis of deviations is laborious, the study sessions should be handled such that the right resources and the expertise needed in each particular session are present. Optimal use of the limited expert resources is important and improves the motivation for the work. According to Case study 2's results, the HAZOP studies highlighted many important system characteristics, system features, and improvement possibilities beyond the safety-related realm. These were used for improvements to the functionality, usability, and reliability of the system. It was also pointed out that most of the results were directly transferable to the mine-automation development team to be considered in the system-development work.

In Case 3, the aim of the HAZOP study was to identify safety-critical deviations of the safety system in its system-design phase. After identification and analysis of

deviations, done by researchers, the analysis results were reviewed in three meetings by the system designers from the safety-system supplier and an automation expert from the system supplier. The operation procedures under study took the form of a simplified written use-case description wherein the operator's actions and safety system's responses are listed in chronological order. The integration of researchers' preparation efforts and expert-group review meetings functioned well and was effective in the networked-customer-project context. Detailed use-case descriptions that included the preconditions for the operation situation and the intended dialogue in the human–system interface helped to make the analysis more systematic. It also aided in more precise specification of the deviations, causes, and consequences, which was rendered essential by the complexity of the entire automation system and the sheer number of operation modes and operation situations. The innovative way of utilising a laptop-based safety-system simulator in HAZOP study sessions turned out to be profitable both for verifying the analysis findings and for allowing immediate testing and evaluation of proposed modifications and improvements to the safety-system software.

The aim of the HAZOP study in Case 4 was to verify the safety-system design against the specified functional safety requirements. The HAZOP work was carried out in the system-design phase of the new automatic stacking-crane system by a team composed of automation and electrical experts, system designers, and researchers. A HAZOP method in line with IEC 61882 (ibid.) was familiar to the team's industry members on account of the earlier studies related to the system of interest. The recording of results employed a data-collection worksheet implemented with the MS Access relational database application. The HAZOP study sessions were utilised not only for the risk analysis but also in design and evaluation of the safety system under study. The study sessions formed a forum for the team's discussion and internal sharing of information on safety-system functions and features. The team reviewed changes made in the design, and they discussed and evaluated alternative operation and functionality solutions. The HAZOP method using function-level drawings and a new database tool for data collection and documentation worked well for safety-system-validation purposes.

The database tool added value to the HAZOP studies by improving the systematics of the data collection, reporting, and reuse of the data. The systematic methods and supporting tools received positive feedback both from the system supplier's experts and from researchers. The system supplier utilised the database tool as a foundation for further development of a functional safety requirement management toolkit for its own use and for integration of analysis data into other system-design tools. The results indicate that further research should be devoted to the improvement of system-safety-information management through, for example, continued development of the database application.

9.3 Risk estimation and risk evaluation

This section of the chapter discusses the case-study results related to the risk-estimation and risk-evaluation methods utilised in the case projects. Implementation of the methods and practices, experiences from the industry, and observations are summarised and discussed case by case.

9.3.1 Case 1: The existing ore-transportation system

The risk-estimation method in the first case was a simplified modification of the method presented in the risk-assessment standard EN 1050 as valid at the time of the study (1996). Risk estimation was done with a 3 × 3 matrix. Estimation was performed once with assumption of the situation in the absence of any protective measures. Risk level was categorised at three levels for prioritisation of the necessary actions for reduction of the risks to an acceptable level. Practical experiences and comments from case 1 showed that risk estimation using three categories for probability of the occurrence of harm and for severity was simple and general enough for qualitative expert estimation at overall system level to yield risk-prioritisation input to the risk-evaluation process. It was observed that the method's simplicity and variation in the category definitions caused lack of clarity and led to differences in interpretations, thereby decreasing the reliability and quality of the analysis results. It was not clear which probability the PHA team was estimating, the probability of occurrence of harm or the probability of a hazardous event. In the HAZOP teams, the same confusion arose with respect to the probability of a dangerous deviation (dangerous failure) or of any given deviation occurring in general. The definitions for severity and probability categories should have been specified clearly and been the same in all analyses, for the results to be comparable. The simple multiplication of severity by probability obscured the significance of the severity factor and made it difficult to evaluate the risk.

In this case the preliminary risk evaluation was carried out in the PHA and HAZOP meetings. The analysis groups evaluated the risks also and discussed the needs and possibilities for risk reduction. The industry experts discussed the proposed actions and assigned them to the corresponding stakeholders associated with the semi-automatic ore-transportation system context – i.e., to the relevant parties responsible for the development, operation, and maintenance of the system in the mine. Proposals were created in line with the three-step risk-reduction principle that was presented in the Machinery Directive, Directive 98/37/EC (1998), and in the basic machinery safety-design standard of the day, EN 292-2 (1995). The same required procedure, 'the principles of safety integration', exists, with the same content, in the present Machinery Directive (Directive 2006/42/EC 2006) and in the risk-assessment and risk-reduction guidelines applied today for machinery (SFS EN ISO 12100:2010). The evaluation results were then conveyed to the project-management and mine-management teams for further evaluation. According to the case-study results, this procedure for risk estimation and risk evaluation

worked out well. The mining company stated after the risk-assessment project that the results of the project clarified the main areas in which the system improvements need to be focused to ensure safety of the system and conformity with the Machinery Directive's essential health and safety requirements.

9.3.2 Case 2: The ore-transportation-system concept

The risk-estimation method in Case 2 was the same as that in Case 1. The experience and observations confirmed the same problems related to the simple three-category method and the documentation practice applied at the time of the project. Another issue that created confusion in the risk estimation was that of the personal-safety consequences and other consequences (physical damage, production loss, impact on the operating environment, etc.) not being clearly separated in the PHA or HAZOP documentation. Risk estimation assuming a situation without any protective measures supported the safety engineering and risk evaluation in the early system-design phases, but risk estimation should have been performed and documented also after the planned safety measures and proposed further measures were specified, to support the risk-reduction process.

In Case 2, the preliminary risk evaluation was carried out at the PHA and HAZOP meetings. The system designers and automation experts discussed the possibilities for risk reduction from the machine manufacturer's point of view. The main objective in the risk-assessment and risk-reduction processes in this case was to create a safety-requirement specification for the primary and independent safeguarding system that isolates the automated area and functional safety requirements for the safety-critical functions that were identified in the automated mobile work-machine concept. It was noticed during the meetings that application of the three-step risk-reduction principle was proving hard to manage in the case of the complex machinery-automation system. Deficiencies in the risk-analysis methods applied at the time caused problems near the end of the risk-assessment process. It was difficult to perceive and decide upon the appropriate level of the safety measures. Allocation of risk-reduction measures to inherent system functions, functions related to on-board safety, safety instructions, warnings, and system-operation development were new issues for the system designers. The results clearly reflect the new challenges in such complex machinery concepts' definition and requirement specification. On the other hand, the results emphasise the importance of a systematic approach to risk assessment with operational and functional analysis perspectives that bring these aspects out.

9.3.3 Case 3: The ore-transportation application

In case 3, the researchers performed the preliminary risk estimation and risk evaluation in the PHA. In the HAZOP study and in the OHA, the results were reviewed by the industrial expert group. Risks were estimated by means of a 5 × 5 matrix, and estimation was done in two stages: assuming no safety measures and con-

sidering the existing, planned, and proposed safety measures. That is, firstly, the severity of consequences and the likelihood of harm were estimated in terms of the automated system and its environment without any specific risk-reduction measures. Secondly, the risk-reduction measures designed and created in the system concept by the system supplier were recorded. Needs for additional site- and application-specific risk-reduction measures were examined and proposed in light of both system supplier's actions and mining company's actions. Effects on personal safety and possible effects on machinery or production-area infrastructure were analysed separately. Current risk-assessment standards SFS EN ISO 12100 (2010, p. 17) and IEC ISO 31010 (2009, p. 85) support this procedure of assessing individual consequences of the same hazard separately.

Five categories for the probability of harm and the severity of the consequences were used in the risk estimation. Three risk levels (high, medium, and low) were used for risks' ranking. The probability of occurrence of harm was mixed with the probability of hazardous events than can cause harm. The estimation of the probability of occurrence of harm or physical damage was supported by written descriptions of the probability categories; the categories were specified with the system supplier. The IEC ISO 31010 (ibid., p. 83) and BS 18004 (2008, pp. 78–79) standards emphasise that when descriptive categories are used in assessment of severity or likelihood of harm, they should be clearly defined. MIL-STD-882D (2000, p. 18) proposes that the probability of an occurrence of harm or physical damage during the planned life expectancy of the system can be described in terms of potential occurrences per unit time, events, population, items or activity.

The risk evaluation took into account the existing safety measures and safety functions specified for the automated ore-transportation system concept, then considered the needs for mine-specific and machinery-system-specific safety measures. The three-step risk-reduction principle was adopted from then-current machinery safety standard EN 292-1 (1995), which has been replaced with SFS EN ISO 12100 (2010). This procedure was amended, however, with ideas from the system-safety precedence sequence described by Stephenson (1991, p. 11) and by Roland and Moriarty (1983, p. 39). The main difficulty was in the estimation of the impact of the various measures on the three main factors in the probability of the occurrence of harm as described in SFS EN ISO 12100 (2010, p. 17): 'the exposure of person(s) to the hazard', 'the occurrence of a hazardous event', and 'the technical and human possibilities to avoid or limit the harm'.

Our case-study results and experiences seem to indicate that the changes made to the approach to risk-assessment and analysis methods took the methods in the right direction from the previous cases. Probability estimation using five categories and application-specific written descriptions turned out to be practical in this unique automation application. The risk-assessment results showed that some risks remained at 'medium' level after the proposed safety measures, and a specific methodological problem was recognised with severity category 1 (for multi-fatality incidents): even though the probability of the occurrence of harm could be reduced to 'very unlikely' (harm can occur only if several errors or failures occur at the

same time), the risk remains 'medium'. This caused confusion later in the risk-evaluation process.

The case-study results emphasise that the interpretation and explanation of the implications of the final risk-level results should be developed such that they give better support to the decision-making in risk evaluation and trade studies in requirement, functional, and design analyses in systems-engineering processes. The decision-makers must understand what the results mean. Site-specific information should be used as much as possible in risk analyses, risk estimation, and risk evaluation, to enable appropriate reasoning based on the actual work-site conditions, practices, and limitations. Insufficient information can lead to conflation of concepts, as in probability estimates for 'hazardous event' and 'occurrence of harm'.

These results indicate that in some cases the risk evaluation should be raised to a higher level in the system hierarchy, where the measures and safety solutions can be more effective. This links the system-safety-engineering efforts to the systems-engineering process (ISO IEC 26702 2007) and system-hierarchy model called 'system-of-systems' (SE handbook 2011, p. 11). The overall machine-automation application can be considered the system of interest, in which system elements produce safety-engineering problems that cannot be solved by the individual systems alone. This approach is emphasised also in BS 18004 (2008). Risk levels between 'acceptable' and 'unacceptable' should lead to employment of the ALARP safety-engineering principle and cost-effectiveness analysis for finding of appropriate and effective safety solutions (ibid., pp. 84–85).

9.3.4 Case 4: The container-handling-system concept and its application

In Case 4, the risk-estimation method was the same as that used in case 3, utilising two phases and separate estimation of personal and other effects. Five categories for probability of harm and severity of the consequences were used and three risk levels. The probability categories were specified together with the system supplier. The case-study results, the output of the risk-estimation method, and the interpretation of the risk-estimation results indicate that the levels should be developed for better support of the decision-making in risk evaluation and trade studies in requirement, functional, and design analyses in systems-engineering processes. The methodological problem with severity category 1 that was discussed above for case 3 was recognised in this case. The system supplier stated that standards need to be considered to be guidelines and tools to support the company-specific risk-estimation and risk-evaluation methods' development. A simple improvement in the documentation was developed for this case. Colour codes ('traffic lights') were used to highlight the risk level (high, medium, or low) in the OHA documentation. These were considered more informative than numeric values taken from the matrix elements. They also aided in recognition of the difference and change between estimated risk levels before and after safety measures.

Vincoli (2006) has enhanced risk-estimation matrices for the system-safety-related process by applying hazard-severity categories and hazard-

probability levels from MIL-STD-882D (2000). The method uses four severity categories, five probability categories, and four risk levels. The principle for classification of the risk level in this model is an attempt to direct the decision-making in the risk-evaluation process to the correct level in project management or company management Vincoli (2006, pp. 14–16). Cox (2008) has examined risk matrices supporting decision-making in the risk-management process and discusses the limitations and problems associated with the use of risk matrices in risk management. Although recommended in international risk-management standards, risk matrices should be used with caution. Four types of problems linked to risk matrices have been identified: poor resolution, errors, sub-optimal resource allocation, and ambiguous inputs and outputs. Risk-management decisions cannot be based only on rating of risks' frequency and severity factors. The judgement inherent in risk ranking should be carefully explained (ibid., p. 510).

The practical experiences of risk assessment in this case support Cox's conclusion that, for optimal resource allocation in risk management, other factors and quantitative information should be considered, among them the cost of various safety measures, the risk reduction achieved, budget constraints, and interactions between risks and safety measures (ibid.). The risk-estimation methods and the interpretation of risk estimates (risk levels) should be developed so as to provide better support for the decision-making in risk evaluation and trade studies in requirement, functional, and design analyses in systems-engineering processes. The risk-estimation method as utilised in this case seems to lead to excessively high requirements for performance levels or safety integrity levels. According to the results of the case studies, the risk-estimation method should be tailored and calibrated to suit the machinery and the system of interest, and it should match the internal and external context of the company.

9.4 Other findings

Some noteworthy and interesting findings emerged during the case-study research: These were related to allocation of risk-reduction measures in complex machinery applications; identification, analysis, and evaluation of human factors; the scope and coverage of risk analyses in relation to relevant stages in the system life cycle; and analysis and management of system-availability and system-reliability issues identified in the risk-analysis sessions. These issues were not emphasised in the case-study research but do have implications for the development and further use of the approach taken to risk assessment and to risk-analysis methods in this context.

The findings in Case studies 1, 3, and 4 support the tendency toward integration of system-safety management efforts into the overall systems-engineering process and overall production-system and environment development efforts. The results showed that mining-automation applications and automated container-handling applications are unique and that safety solutions in such contexts depend greatly on the operation and maintenance concepts and on operating

environment. The findings also point out the importance of LOPA principles in risk reduction for automated mobile work-machine systems. These findings also highlight the necessity of integrating risk-evaluation and risk-reduction perspectives systematically into the overall systems-engineering decision-making. The results are in line with findings described in the literature according to which safety problems in complex socio-technical systems cannot be solved by technical means alone. Safe operation and maintenance relies strongly on operators' and other stakeholders' risk-conscious behaviour and decision-making just as much as on work conditions that support and enable safe work methods (Vincoli 2006, pp. 12, 37–43; Leveson 2011b, pp. 75–83).

The results of case studies 1, 3, and 4 confirm the importance of the consideration and analysis of human factors in complex systems. Analysis results showed that situations can arise in normal operation of the automated mobile work-machine systems wherein system safety assurance relies almost entirely on human actions. This indicates that, regardless of all intelligent technical features and functions, the system operators, service workers, and all personnel working in the automated production area have an important role in ensuring safety and health by following the safety instructions and procedures. The analysis of human factors should be widened from operator errors to cover also the factors related to system implementation; operation and maintenance; operating environment; and elements enabling or preventing correct, intended, and safe operation (Leveson 2011b, p. 46).

In Cases 3 and 4, which were customer-application projects, the risk assessment covered mainly the operation and maintenance phase of the system life cycle. Such large-scale customer-specific machinery applications are constructed, integrated, and tested for the first time as a whole on the final operating site. This is in stark contrast to individual manual or automated machine applications, which are built and tested in the factory. It was found that the scope of system-safety activities should be extended to cover also on-site system installation, building, and testing phases. The work site at a mine or a container terminal is, in practice, a construction-work site for a long time and cannot be considered or analysed as a final production system in these stages. This emphasises the need for system-level risk-management co-operation in such large-scale machinery applications. System-safety issues are, in addition to the safety engineering of the system of interest, related to the overall investment project's risk management and an issue of the end user's occupational health and safety management on the site.

The results of case 1 show that the analysis of maintenance tasks in the automated production area should have covered better the work done beside the machines. Troubleshooting of the on-board control system and maintenance of the on-board automation components are new automation-related maintenance work tasks partly done on top of the machine. They may require co-operation between the maintenance staff at the machines and operators in the control room, and they have potential to bring new safety risks, such as a risk of falling down, of burning, or of unexpected machine movements. In this case, system troubleshooting and daily maintenance issues were covered in the PHA pertaining to the whole under-

ground production area. Actions in system-fault situations were touched upon from the operator point of view in the HAZOP study of system operations.

Systematic analysis of system operations and system functions via PHA, OHA, and HAZOP studies in all cases studied elicited a great deal of information that was not directly related to safety but did have links to system availability, system usability, or system reliability. According to the interview results, system analysis for reliability-engineering and safety-engineering purposes is typically carried out separately in the mobile-work-machine-manufacturing industry. Also, interviewees told us that the information exchange between these two engineering groups could have been more systematic. Valuable information for system-availability development can be lost even very early in the system life cycle if not passed on for system-analysis input in the systems-engineering process. These findings are in line with the results of recent studies of system availability and of system-reliability issues in complex mobile machinery in early stages of design. According to Jännes (2011, p. 58), mobile-work-machine manufacturers consider it important to develop system safety and system availability such that they are mutually supportive. Ahonen et al. (2012, pp. 40–43) state that in R&D projects intended for development of applications of entirely new technology, it is essential to carry out overall system-level availability-related risk analysis in the conceptual design phase. The availability-risk assessment in the conceptual phase should be based on system functions, not on system architecture or system components.

Applying a bottom-up analysis method in reliability engineering later in the life cycle may not bring out these issues, because the objectives and analysis method are not aligned with each other. Some development ideas were expressed by the experts interviewed: A reliability-engineering expert could join the system-safety working group and supplement their work at PHA, OHA, or HAZOP meetings. Another approach might be to increase safety engineers' reliability-engineering knowledge so that they have skills in identifying reliability issues for further analysis and evaluation. To allow systematic utilisation of this valuable information, the companies could establish and maintain an overall RAMS management process that brings system-availability and system-safety information together. Railways' safety-critical systems are among the contexts in which RAMS management programmes have been developed and standardised (EN 50126-1:1999).

Management of the vast quantities of risk-assessment information and documentation is one challenge presented by such large and complicated machinery-automation applications. To improve the work practices' efficiency, it should be made easy to modify and reuse previous risk-analysis templates and documents. Linkage to previous higher-level analysis and assessment results to the new lower-level analysis worksheets and documents and, finally, linking of the results to the essential safety and health requirements should also be supported by the data-management system. In this study, the experiences of the use of a database tool for the collection and management of risk-assessment results were promising in this connection, as were related comments. The database tool, developed concurrently with case project 4, was tested in the HAZOP studies. This researcher's experiences and observations were primarily positive: the database supports

efforts to form a systematic and traceable chain of evidence from overall safety-requirement specifications down to detailed requirements for safety functions. Many improvement proposals were created not only for risk-assessment documentation but also for the concept of database-centric information management in systems engineering in general.

10. Evaluation of the study

The research and development work and testing of the approach and the methods have been done in close co-operation with globally operating working-machine manufacturers in Finland, their international subcontractors, and their customers and system end users. In practice, the research work started in 2000 and is ongoing. Research and development of the approach to risk assessment for automated mobile work-machine systems has been carried out in several jointly funded research projects in Finland and in confidential contract research assignments in Finland and other countries over this long span of time. This has presented its own challenges to the research work, including issues such as international co-operation and communication, confidentiality, and continuity and scientific validity of the research. On the other hand, all these challenges, the real needs and practical safety-engineering problems in co-operating companies, and the open and constructive attitude among research teams at VTT and in the companies' project teams have kept the author's motivation high over the years.

The research work followed a constructive research approach, and the case-study research was qualitative in nature. Evaluation of scientific research typically includes assessment of the validity and reliability of the research and evaluations of its practical and scientific contribution. Validity refers to whether the research truly measures what it was intended to measure or how 'truthful' the research results are (Golafshani 2003, p. 599). Because of the innovative problem-solving nature of constructive research, its scientific validity should be evaluated on the basis of the *novelty and relevance* of the results (Kasanen et al. 1991, p. 305; Olkkonen 1993, p. 76; Lukka 2000, p. 122; Oyegoke 2011, p. 579). According to Eskola and Suoranta (2005, p. 219), relevance of a piece of research refers to the *practical usefulness* and the *general importance* of the research results. In this study, the novelty and general importance are evaluated in view of the trends in automation development for mobile machinery applications, current research in this field, and development of the relevant international safety-engineering guidelines and standards. The practical contribution of the study is evaluated in terms of the usefulness of the three-level approach to risk assessment and of the case projects' results within the co-operating companies and in automated mobile machinery applications more generally.

The case-study research method applied in this study is based on qualitative analysis and evaluation of the findings. Nahid Golafshani (2003, p. 601) states that the most important evaluation criterion for any qualitative study is its *quality*. Stenbacka (2001, p. 555) states that quality evaluation in qualitative research should examine the *validity, generalizability, and carefulness* of the research. According to Stenbacka (ibid., p. 552), reliability in quantitative research pertains to the measurement method's ability to produce the same research result time after time and the results should be independent of the researcher. In that sense, reliability has no relevance in the evaluation of qualitative research, because it is not possible to separate the researcher and the research method. On the other hand, Yin (2009) states that reliability is one of the common validity tests used widely in case-study research. Reliability in the context of case-study research refers to the case-study protocol being designed and documented such that a later investigator should arrive at the same findings and conclusions. The goal is to minimise error in the investigation and biases in the study (ibid., p. 45). In this study, the reliability of the PHA, OHA, and HAZOP risk-analysis methods was not the subject of research; the question had to do with understanding their applicability in the risk-assessment process for complex automated machinery applications. The quality of the case-study research was evaluated for its validity, the case-study results' generalisability, and the care taken in the research work.

10.1 The novelty and general importance of the study

This study is the first scientific research into risk-assessment issues associated with complex automated mobile work machine applications in this extent. The machinery systems under study in this research have all been the first of their kind in the world. Interest in this subject was piqued in late 1990, when the first autonomous mobile machine concepts were introduced, and interest in the system-safety approach has increased in tandem with the rapid development of automation technology and the growth in systems' complexity. Today the subject is topical in many interest groups in industries that manufacture and apply mobile machines.

Research into system-level risk-management issues and system-safety factors has been conducted in many other lines of business, such as the defence, aviation, space, and process industry. Results of these studies have been reported by, over the years, such authors as Roland and Moriarty (1990), Toola (1992), Leveson (1995, 2004, 2012), Stephans (2004), and Vincoli (2006). A lot of research has been carried out and published on automation-technology development for mobile machinery. However, only a few studies, among them works by Pukkila (1999), Paques et al. (1999), Sammarco et al. (2001), Sammarco (2002), Alanen et al. (2004), and Tiusanen and colleagues (2008, 2013a), have been published on issues of safety or risk assessment in the context of automated mobile work-machine systems.

At the moment, the development of automation technology is said to be one of the main business drivers in both sectors of industry considered in this study.

Actors around the world are attempting to create a moveable equivalent of the static manufacturing assembly line for mining. The goals for this technology are to speed up production, improve safety, and reduce costs (Jämsä-Jounela & Baiden 2009). Some of the largest underground mines use unmanned or tele-operated loading machines, dump trucks, and ore-transporting trains (Bellamy & Pravica 2011; Fiscor 2008). Also, Jämsä-Jounela and Baiden (2009, p. 1009) point out that mines and mineral-processing plants develop integrated process-control systems capable of improving plant-wide efficiency and productivity. According to Ericsson (2012, pp. 2–3), technological development in mining in recent years has been grounded in strategies to scale up equipment, increase automation of processes, and utilise continuous processes. There is strong pressure on manufacturers to deliver technologies and equipment that are safer and less polluting.

Some years ago, Günther and Kim (2006, p. 438) stated that there is an ongoing trend in the development of seaport container terminals to use automated container-handling and transport technology. Manually driven cranes are going to be replaced by automated ones, and automated guided vehicles are often used instead of manually operated carts. The system operators in their control room can be far from the container-stacking area and load the container on a truck by means of remote control. Scott (2012, p. 85) states that in marine terminals the equipment automation is focused on the shift toward unmanned vehicles such as automated stacking cranes, horizontal-transport vehicles, and automated guided vehicles. The future of automation will see a focus on optimising the whole terminal process rather than just a part of it (e.g., the yard or gate operations). Because of the increasing size of container ships, more efficient and automated operations are needed in port yards. Globally, there are about 1,400 container ports, of which 20 are already fully or highly automated. It is estimated that about 1,000 more have potential in terms of automation development (Raunio 2013, pp. 16–17).

Standardisation in machinery safety and functional safety engineering guidelines has developed strongly in the last 10 years. There is still a lack of automation safety engineering guidelines for automated mobile work-machine systems and autonomous machinery applications. In ISO's standardisation committee 127 ('Earth-moving machinery'), there is a work item on these issues called 'Autonomous Machine Safety', with the aim being to develop general safety guidelines for machines that run without operators, but the work is still in its early phases. Requirements related to functional safety requirements and engineering practices are becoming more widespread also in machinery applications. The results of our study confirm that the identification of safety-related functions and allocation of safety requirements related to complex machinery applications still require research and development of practical methods and perhaps a dedicated application standard for automated mobile machinery applications. Findings from this study could be used in the development of safety-engineering guidelines for automated or autonomous mobile work-machine systems.

In Finland, mobile work machines represent one of the most significant fields of industry. There is great variety in the mobile work machines developed and manufactured in Finland. The Forum for Intelligent Machines (FIMA) is a national net-

work for mobile work-machine manufacturers, specialist companies, system integrators, and research institutes. The main areas of FIMA's research are automated functions of work machines, measurement techniques, multi-machine operations, remote operation, new design methods, and energy-efficiency of work machines (FIMA 2007). Safety elements have been and are today strongly evident in most of these areas.

10.2 Practical contributions

The practical contribution of the study is evaluated on the basis of the usefulness of the three-level approach to risk assessment and the case projects' results in the co-operating companies and in general in mobile machine applications. Olkkonen (1993, pp. 77–79) and Kasanen, Lukka, and Siitonen (1993, p. 250) propose three levels of criteria (evidence) for evaluation of the practical usefulness of constructive research's results, to reveal the relevance of the outcome of the research. Providing weak evidence of the results' usefulness is that the solution works – in other words, that the objectives were reached with the solution constructed. Stronger evidence is found in the target organisation's adaptation and use of the solution or parts of it. The strongest evidence is found in the solution being adopted and utilised in other organisations, ones not involved in developing it. From these general criteria, the evaluation for this study is formed as follows:

- The first evaluation criterion is that the system-safety problem is solved in accordance with the approach and the risk-analysis methods developed.
- A stronger criterion is that the machine manufacturer or system supplier has implemented the approach or part of it in its systems-engineering practices.
- The third and strongest criterion is that third parties, companies that did not participate in the development of the approach, implement it at least partially in their processes.

In this study, dealing with safety of automated machinery, the most important outcome of the research and development work and, indeed, the point of all risk-assessment efforts, is the final result – a safe system, wherein safety risks are reduced to an acceptable level, even though this is deemed only weak evidence. Was this goal reached in the case projects? The results of case study 1 showed that no automation-related accidents caused by the automated machinery had been reported to the machine manufacturer at any point between completion of the risk-assessment assignment and the system's decommissioning, a few years ago. According to the system supplier in case studies 2 and 3, no accidents related to the automated ore-transportation systems had been reported to it since the first application entered use, about 10 years ago. The system supplier in case study 4 reported not having been informed of any reportable injuries related to the automatic stacking-crane system. From this evidence, it can be concluded that the

safety-engineering problems in all four case projects were solved and, therefore, that the first evaluation criterion is met.

Critical reflection on the findings and intensive interaction with the co-operation partners in implementation and testing of the problem-solving constructions during the research process is a key criterion for high-quality constructive research (Lukka 2000, p. 125). The present research was conducted in close co-operation with industrial partners. Experts from industry participated both in constructing the system-safety approach and in implementing the methods in the various case studies. Among the objectives were to transfer safety-engineering expertise from researchers to safety engineers in industry and, simultaneously, to transfer industrial experience and application-specific expertise to researchers. This interaction was aimed at improvements in risk-management processes and safety-engineering practices not only in the case companies but also within VTT.

According to the results, the approach and methods have been adopted to some extent in the co-operating companies. The mining company in Case 1 stated that the analysis and assessment work gave them valuable information about the automation-related risks and the current status of the safety risks of the semi-automatic ore-transportation system. The machine manufacturer and system supplier of the automated mining machine applications pointed out in Cases 1, 2, and 3 that most of the results were directly transferable to the mine-automation development team for consideration in the system-development work. The system supplier adopted the three-level approach to risk assessment and developed a company-specific application of it. The overall system-safety work has been developed further, to match the functional safety engineering objectives better. The mining company in Case 3 stated that, with the aid of the systematic risk-assessment work, they were able to specify and implement necessary safeguarding functions and other means to guarantee the safe operation and maintenance of the automated ore-transportation system. The system supplier of the automatic stacking-crane applications in Case 4 has adopted parts of the approach, also developing a company-specific application of it for new system-development projects and for customer-application projects. The new method of modelling and integration of function-level information that was created as part of the research and development work has been adopted and further developed in the co-operating companies. It can be claimed that the second, stronger evaluation criterion is met.

The third and strongest criterion has to do with the generalisability of the results. The approach and method have been adopted in companies that did not take part in the case projects or in research and development work in jointly funded research projects associated with this research. It was indicated by the system supplier that the system-safety approach, analysis methods, and documentation principles have become mirrored in customer demands in the automation projects in the global container-terminal industry.

Evidence of the generalisability of the results has been seen in a different field of application of mobile machines – automated material handling in a deep repository for spent nuclear fuel. After the fourth case project, VTT applied the three-

level risk-assessment concept with its PHA, OHA, and HAZOP approaches and risk-matrix-based estimation method were applied at the Swedish Nuclear Fuel and Waste Management Company (SKB) for two automated mobile machinery applications in Sweden, in 2009 and in 2012–2013. The systems under study were designed for automated spent nuclear fuel deposition in the deep underground repository, and both were still in their prototype development and testing phase. In this case, the machines considered were standalone units that display characteristics of an automated mobile work-machine system. These machines were designed for automatic operations and to be capable of autonomous operation. Features include several operation modes and on-board automation and control systems. According to discussions in 2013 with the experts in charge of machinery-system development at SKB, the company is applying the three-level approach to risk assessment, with the PHA, OHA, and HAZOP methods, in its system-safety engineering process. From this evidence, it can be claimed that also the third evaluation criterion is met.

10.3 The quality of the case-study research

In this study, the quality of the case-study research is evaluated in terms of its validity and through discussion of the care applied in the research work. Yin (2009, pp. 40–45) introduces four perspectives from which one can test the validity of case-study research. These, commonly used to establish the quality of empirical research in the social sciences, are called construct validity, internal validity, external validity, and reliability.

Construct validity is associated with identification of the correct operational measurements for the concepts under study (ibid., p. 40). Yin (ibid., p. 42) points out three aspects to be considered in the context of construct validity: multiple sources of evidence, a chain of evidence, and the review of case-study reports. Yin (ibid., p. 102) also lists the six most commonly used sources of evidence in case studies: documentation, archival records, interviews, direct observations, participant observation, and physical artefacts. Patton (1999, p. 1192) emphasises the importance of ‘triangulation’ and associated principles in the gathering and analysis of qualitative data. Several methods are needed because each method reveals different aspects of empirical reality. Triangulation increases the credibility of the results and allows for cross-source validity checking. Data-collection methods such as interviews, observations, and document analysis are expected in qualitative enquiry. Golafshani (2003, p. 604) and Eskola and Suoranta (2005, pp. 68–70) point out that another sort of triangulation can be employed also: taking into account several investigators’ or peer researchers’ interpretations. In our work, the case-study materials were composed of case-project documentation such as plans, analysis documents, protocols, meeting memos and project reports, results of the interviews of key persons at the partner companies, documented researcher observations from the case projects, and interviews with researchers involved in the case projects. The research was conducted over a long

time span, which does means that the cases are old (2000–2008). Also, the interviews with experts were conducted in 2012, several years after the case projects. On the other hand, the time frame of the research and development work provides the possibility of evaluating the results and impacts from a wider perspective, which is considered an essential characteristic of the constructive research approach and of qualitative research in general (Lukka 2000, p. 124).

Stenbacka (2001, p. 555) emphasises careful selection of informants (here, interviewees), people who are relevant for the study and also capable of generalising the case-specific issues and findings. In this study, the interviewees were selected to represent the knowledge of the case project in question, the safety-engineering practices in the company, and the company's automation development. In addition to project documentation, publicly available information about the case projects and systems under study was examined. Accident and near-accident statistics for the systems in Case studies 1, 3, and 4 were not available in this study. The information for gauging the safety performance of the systems is based on what was reported in the interviews with the system suppliers' experts. The chain of evidence – in other words, the traceability of the findings – was implemented such that the findings from each case study were grouped systematically under the following themes: descriptions of the system under study; descriptions of the implementation of the approach to risk assessment, risk analyses, and risk-estimation tasks; experiences and comments from the companies; and observations. Accordingly, the findings can be traced back to the original case-study material. In addition, the draft case-study reports were reviewed by the key experts from the co-operating companies, for avoidance of any misunderstandings or errors as to facts. This review of the report and a request for permission to publish are part of the common practice at VTT when confidential customer assignments are involved.

The case-study research method applied in this study was focused on two issues: the usefulness of the three-level approach to risk assessment and the usefulness of the risk-analysis methods chosen. The former was evaluated through finding of possible benefits of the approach for the case project and for the systems studied. Also, the impacts on the partner companies' safety-engineering practices were examined. The evaluation of the risk-analysis methods was based on findings, both positive and negative, from project documentation and interviews, complemented with researchers' observations.

The usefulness of the risk-analysis methods was studied by examining findings related to pros and cons of the methods, analysis practices in the case projects, and factors affecting the quality of the risk-analysis methods. The objective of the case-study research was to examine the applicability and utility of the selected methods in hazard identification and analysis, risk estimation, and risk evaluation with respect to new automation-related system-level issues. The number of hazards identified, types of hazards, risk levels, the number and type of proposed safety measures, and the work effort required for the analysis sessions were examined and recorded. In combination with researchers' observations and industry partners' comments on the usability issues associated with the methods, they give

a general picture of the applicability and usefulness of the methods in each case. The intention was not to compare results between cases, since each case was unique and the results are, therefore, case-specific. Neither were direct or indirect costs of risk-assessment efforts in case projects estimated in this study.

Internal validity in case-study research is associated with explanatory or causality studies aimed at uncovering the causal relations whereby certain conditions are believed to lead to other conditions, as distinguished from false relations (Yin 2009, p. 40). Internal validity was not the main concern in this study, because the case studies in this project are mainly of an exploratory and descriptive nature. The objective of this research has been to study and evaluate the usefulness of the approach taken to risk assessment and risk analysis in complex mobile machinery applications. The aim was not to attempt to explain or prove that the approach and the methods by which certain safety measures were selected or created caused the systems to become safe or fulfil certain safety regulatory requirements. On the other hand, some of the research findings have a natural relationship with causal relationships such as problems identified in risk estimation being linked to inadequate definitions and documentation in the hazard-identification phase or the risk-estimation method's simplicity causing problems in the risk-evaluation phase because the consequences for humans and for equipment were not separated clearly.

External validity is related to the question of whether the findings can be generalised beyond the case study in question (ibid., p. 43). A study may, of course, involve more than one case; multiple-case designs should follow the same 'replication logic' used for repeating of scientific experiments. In this research, with its four case studies, the replication logic was implemented in such a way that in each case study, the evaluation of the approach to risk-assessment concepts and the selected methods was repeated in line with the same case-study protocol. Study of Cases 1 and 2 was used to examine the usefulness of the approach and the methods in the first form of their implementation, and case studies 3 and 4 were used to examine the usefulness of their second form. Each case study had specific objectives and its own research question. In this study, all of the cases involved different systems, but each involved the fundamental characteristics of an automated mobile work-machine system (see Subsection 1.1) and represented different stages in the life cycle of such systems: The first case was of an existing and operating ore-transportation system. The second case featured an autonomous ore-transportation system in its conceptual design phase. The third was a customer application of the autonomous ore-transportation system, and the fourth case covered both the conceptual design and customer-application design phases of an automatic stacking-crane system. From the external-validity point of view, the use of these four studies supports the generalisation of the research results, bringing multiple perspectives to the evaluation of the approach and methods in the same automated mobile work-machine context.

According to Yin (ibid., p. 45), *reliability* in case-study research refers to the possibility of replicating the processes of the study. The aim is to ensure that if another researcher follows the same procedures and conducts the same case

studies, he or she should end up with the same findings and conclusions. As was mentioned above, Stenbacka (2001) argues that in this sense reliability has no relevance in the evaluation of qualitative research, because it is not possible to separate the researcher and the research method (ibid., p. 552). In this study, it was impossible in practice for other researchers to test the reliability of the case studies by repeating them in the way Yin (2009) describes. There were no resources available for this. Accordingly, the evaluation of reliability must be based only on the possibility of repeating the case study; i.e., it can be based on evaluation of the study protocol, data collection, research method, and documentation. Was the work done carefully and documented such that it would be possible to repeat the case study? Stenbacka (2001, p. 555) names carefulness as one of the key elements in evaluation of the reliability of qualitative research and emphasises that thorough description of the entire research process is an indicator of good quality. With qualitative approaches, the identification of relevant findings and interpretation of the findings are strongly dependent, then, on the researcher. In this study, all cases were studied via the same protocol. This includes the case-study design, data-collection plan, method of data analysis, and systematic format for reporting on the findings and analysis results. The chain-of-evidence principle discussed for content validity is most relevant also from the reliability point of view. Systematic and thorough documentation is used to make the research process visible and increases the trustworthiness of the research in this study.

10.4 The scientific contribution of the research

The scientific contribution of this study can be considered from two perspectives. Firstly the study contributes to the development of the approach to risk assessment and its integration with the work of the academic communities in the machinery-safety, functional safety, and system-safety sectors. Secondly the case-study research results provide new valuable information and experiences in how the risk-analysis and risk-estimation methods were utilised, how practicable and useful they were, and what kinds of problems were faced in the case projects in the various phases of the system life cycle.

The three-level approach to risk assessment supplements the standardised risk-assessment process in machinery-safety engineering practice by bringing in the top-down hierarchical structure for risk analyses and the new system-level risk-assessment angles. Safety risks change when human–machine interactions are transformed into human–system interactions and as use of a manual machine gives way to operation of an automated system. The three-level approach to risk assessment also widens the scope of the traditional risk-assessment process in the machinery sector by assessing risks related to the full work-site environment in which the automated machinery application is to operate. In this sense, it adds perspectives from industrial safety engineering practice to machinery safety engineering practices in order to cover the overall system-safety aspects and to evaluate and allocate risk-reduction measures from both the manufacturer's and end

users' point of view. This is especially important for the assessment of the new phases in the life cycle specific to automation systems, such as assembly, testing, commissioning, and start-up of a unique application at the work site.

The new concept of this three-level approach to risk assessment integrates and utilises elements from current safety-engineering practices and the systems-engineering approach. The three-level system hierarchy adopted from the general systems-engineering V-model (overall system level, upper system level, and lower system level) was a good fit for the levels of risk assessment in the automated mobile work-machine systems. This new approach supplements and incorporates the machinery-safety engineering approach, which concentrates on the machine-level safety issues; the functional safety engineering approach, which focuses on safety-related control systems; and the industrial safety engineering approach, which looks at the overall work-site-safety issues.

This study confirms the utility of the system-safety-engineering efforts in the development of complex socio-technical systems. Systematic analysis covering the entire automation system helped us to understand subsystem operations, system functions, and interrelations between individual subsystems in the existing automatic mobile work-machinery application. Top-down system thinking supported risk evaluation and specification of risk-reduction measures at an appropriate level of the system hierarchy and system operations in the conceptual design phase of the automated mobile work-machinery application. The holistic approach and system thinking aided in making connections between risk-analysis results and in forming of a well-reasoned and traceable chain of evidence for the risk-evaluation decision-making in customer-specific machinery applications.

According to the case-study results, PHA-type analysis is applicable for the overall production-area analysis and for analysis of system operation and maintenance tasks. Both PHA and OHA can utilise traditional risk-analysis meetings to identify hazards and estimate risks, or the process can be carried out iteratively, in two phases: drafting by safety experts and then review by the risk-analysis team. Also, PHA should cover the construction, testing, and commissioning phases in the system life cycle, which bring issues not found with manual machine applications. For analysis of operation and maintenance concepts in the early parts of system development, OHA is useful. The approach is similar to PHA, and its scope enables more extensive analysis of human factors than allowed by HAZOP studies, which typically focus on possible deviations such as human error. The upper-system-level perspective in OHA forms an applicable level of concepts for the discussion of system-safety issues between the system supplier and the customer and also in the automation-project team among experts of diverse technology backgrounds.

HAZOP studies supported by system architecture modelling are applicable for the analysis of upper-system-level functionality and especially for identification of safety-related deviations in the interfaces between subsystems; In particular, HAZOP study is applicable for on-board control system analysis. The new way of modelling and integration of system information into function-level drawings and the utilisation of use-case descriptions support the HAZOP studies and form a common platform for sharing of information within networked control system de-

sign teams. Signal-based HAZOP study of on-board control systems goes into details and is laborious, so it would be better to start with function-level HAZOP study, moving on to more detailed studies only if necessary. A single hazard or deviation can have several consequences. It is important to document them all and distinguish between personal-safety and other consequences.

Risk estimation using three or five categories for the probability of occurrence of harm and for the severity of the harm is simple and rough enough for experts' qualitative use in overall system-level risk estimation to yield risk-prioritising input to the risk-evaluation process. Although risk matrices are recommended in international risk-management standards, this study confirms that risk matrices should be used with caution. The simple multiplication of severity and probability factors obscures the significance of the severity factor and makes it difficult to evaluate the risk or allocate the appropriate risk-reduction measures. In such complex machinery applications as those studied here, it is difficult to perceive which probability to estimate, that of occurrence of harm or the probability of a hazardous event. This weakens the reliability of the risk estimation and may lead to faulty interpretations of the results. Simplification of the probability factor in a risk matrix causes problems in the risk-reduction process when one is looking for the best possible way to reduce the risk. It would be better to use the current standard procedure and separately estimate the probability factors: the probability of a hazardous event, the frequency of exposure to the hazard, and the possibility of avoiding the hazard.

Risk assessment is a continuous process in the systems-engineering approach as considered in this work. The case studies' results emphasise that risk evaluation needs to be performed before any new risk-reduction measures are carried out and after the risk-reduction measures that were already planned or implemented. The risk-reduction measures should be specified separately for the system supplier and for the end user, to allow allocation of appropriate safety measures. The case-study results also emphasise the importance of the principles linked to implications and interpretation of the levels of risk achieved. The risk-evaluation information is to support the decision-making trade studies of requirement, functional, and design analyses applied in systems-engineering processes. If necessary, the risk evaluation and the decision making should be raised to a higher level in the system hierarchy, one at which the measures and safety solutions can be more effective.

10.5 Ideas for further research

Research and development work on the three-level approach to risk assessment has continued since 2000 and is still ongoing. In the course of this long-term research process, ideas for further research have arisen, stemming especially from issues of the practical implementations of the approach and risk-assessment methods in several case projects.

In the first place, research into the applicability and usefulness of the three-level approach to risk assessment and the qualitative risk-assessment methods should

be continued, for more experiences and feedback for further development of the approach and methods. Research should be continued with new machinery applications in the mining and container-handling industry and in other sectors of industry that utilise automated mobile work machines or similar machinery systems.

Research into the system-safety approach and risk-assessment methods should be continued, to support the integration with the functional safety engineering approach, which requires quantitative evidence for the specification of safety integrity levels for safety-related system functions implemented with electric, electronic, or programmable electronic systems. From a functional safety perspective, there is need for the specification of independent protection layers and of safety integrity levels for the safety-related functions. One interesting research question would involve the applicability of a semi-quantitative analysis approach such as LOPA in the context of automated mobile work-machine systems for analysis of the risk reduction produced by each layer of protection.

In this study, the scope was delimited as system-level operations and functions of the machinery applications, with special focus on assessment of the risks caused by automation-related new hazards and new hazardous events. The importance of human factors in automated mobile work-machinery applications was recognised from the very beginning of the research work. The results support the view emphasised in the system-safety literature that in complex automation systems, well-trained operators observing, communicating, and making decisions in everyday operation and maintenance situations should be considered an important factor in safe operation and maintenance, not only a potential factor in errors and causing of hazardous events. There is need for further research on human factors in complex automated mobile work-machine systems, to ensure safe and efficient performance and for management of the increasing complexity of full automation-system entities. Leveson (2012, p. 28) has defined types of complexity with respect to safety in an interesting manner that explores interactive, non-linear and dynamic complexity, and complexity related to how systems are modularised. Further research could be directed to study of the significance of these dimensions of complexity in this context and to study how the approach to risk assessment should be developed to enable one to identify, analyse, and evaluate the risks caused by these factors.

In this work, cost–benefit evaluation of the safety solution was not done in the case studies, because our focus was on the usefulness of the approach and methods, not on the specific safety solutions in the unique machinery applications. According to the systems-engineering approach, risk-management decisions in the system-development phase are made step by step as the system development proceeds. In practice, the decisions to reduce the safety risks identified and estimated are based on comparison of alternative solutions at different layers of protection. Inadequate information or poorly reasoned estimates of the costs and effectiveness of risk-reduction measures in system-service-life perspective can lead to false and impractical solutions. In fact, the Machinery Directive encourages manufacturers to seek the best possible safety solutions thus: ‘The essential health and safety requirements should be satisfied in order to ensure that machinery

is safe; these requirements should be applied with discernment to take account of the state of the art at the time of construction and of technical and economic requirements' (Directive 2006/42/EC 2006, p. 25). The case-study results emphasise that in complex automated mobile work-machine systems there is need for an ALARP-type safety-engineering principle (SFS EN 61508-5:2011, p. 47; BS 18004:2008, p. 84) to support the evaluation of risk-reduction measures in terms of benefits and costs. The research question could be that of how to apply the ALARP principle in combination with qualitative risk-estimation methods in the risk-assessment process during the development of automated mobile work-machine systems.

The modelling of system information, its integration into function-level drawings, and the utilisation of use-case descriptions improved the HAZOP studies and form a common platform for the sharing of information in the networked control system design teams. The database tool added value to the HAZOP studies by improving the systematics of the data collection, reporting, and reuse of the risk-assessment information. Three-dimensional modelling and simulation tools have developed strongly over the last decade. These should provide significant support for the system development early in the life cycle just as much as for risk-assessment efforts in PHA and OHA. Further research and development effort is needed with respect to the computer-aided tools supporting systematic utilisation of the overall risk-assessment process, data collection and analysis, documentation, and reporting of the results. The research work done on the machinery-safety engineering process reference model and tools for the development of machine-control systems (Hietikko et al. 2010) should be continued and guided in the direction of system-safety-engineering and systems-engineering approaches. The use of a simulator-assisted design approach utilising 3D models and simulator environments in system-safety-engineering work for automated mobile work-machine systems has been demonstrated by Tiusanen and colleagues (2013b). This research too should be continued, with attention to the simulator-assisted systems-engineering approach.

The systematic analysis of system operations and system functions in PHA, OHA, and HAZOP studies in all cases in this project revealed much information that was not directly related to safety but did have a bearing on system availability, system usability, or system reliability. If this is not utilised, valuable information necessary for the battle against uncertainties related to the implementation of new technology in mobile work-machine systems could be lost, even in the early phases of the system life cycle, with the overall competitiveness of technologically innovative and progressive automation applications thereby being spolt. Further research and development efforts are needed for finding practical answers to how to integrate system-safety and system-availability analysis and evaluation practices early in the system life cycle and link this with the above-mentioned cost–benefit analysis of risk-reduction and risk-management measures in automated mobile work-machine systems. This could be an interesting step forward in the efforts targeted at development of an overall RAMS management programme for mobile work-machine systems.

11. Conclusions

The results of this study confirm that the safety-engineering problems in the design and development of automated mobile machinery systems can be solved through application of a system-safety approach and utilisation of a systematic risk-analysis and risk-evaluation process. Risk assessment is not a single phase in the system life cycle but an essential part of the systems-engineering process and supportive of decision-making in various phases in the system life cycle. In the development of automated mobile work-machinery systems, the methods of hazard identification, hazard analysis, risk estimation, and risk evaluation should be adapted to support the systems-engineering decision-making process at different system levels, depending on what is the objective of the risk assessment and what is the purpose of use of the assessment results.

One can conclude from the results of this study that risk assessment of an automated mobile work-machine system can apply the three-level approach to risk assessment and use the selected methods: PHA, OHA, and HAZOP methods are applicable for system-level hazard identification and hazard analysis. The risk-estimation methods and risk-evaluation practices need to be developed to be more appropriate for the specific needs of risk-assessment activities at the various levels of systems engineering and in the individual phases in the system life cycle. The three-level approach to risk assessment brings key elements from machinery safety, industrial safety, and system-safety-engineering practices. Its usefulness and benefits have been demonstrated by means of study of four cases, representing different machinery applications, different companies, and different technologies.

This study confirms results in earlier system-safety literature: when the risk analyses and risk evaluations are systematically linked to the overall systems-engineering problem-solving process and consistent with the objectives and requirements set for each phase in the system life cycle, system-level elements that create safety risks at various levels of the system can be identified at the right time and the risk-reduction measures can be assigned to the appropriate level of the organisation for evaluation.

A PHA-type analysis method is applicable for the overall production-area analysis and in analysis of system operation and maintenance tasks. The PHA should cover also the construction, testing, and commissioning parts of the system life cycle – phases that are new in automated mobile work-machine systems as com-

pared to manual applications. The OHA is useful for the analysis of operation and maintenance concepts in the early phases of the system development and should be carried out as early as possible. The approach is similar to that of PHA, and the scope enables analysis of human factors that is more extensive than that in HAZOP studies, which typically focus on possible deviations such as human error. The upper-system-level perspective in OHA forms a suitable level of concepts for the discussion of system-safety issues between the system supplier and the customer and also for discussions within the automation-project team, which involves experts whose background is in quite different fields of technology.

HAZOP studies are applicable for the analysis of upper-system-level functions and on-board control system functions, especially in the identification of safety-related deviations in interfaces between subsystems. The modelling and the integration of system information into function-level drawings, along with the utilisation of use-case descriptions, supports the HAZOP studies and helps to form a common platform for the sharing of information within the networked control system design teams. The database tool developed added value to the HAZOP studies by improving the systematics of the data collection, reporting, and reuse of the risk-assessment information.

Risk matrices are relatively simple and easy to use for risk estimation and also recommended in international risk-management standards. However, the study confirms that risk matrices should be used with caution. The simple multiplication of severity and probability factors understates the significance of the severity factor and renders it hard to evaluate the risk or allocate appropriate risk-reduction measures. Simplification of the probability factor in the risk matrix causes problems in the risk-reduction process when one is seeking the best possible way to reduce the risk. It would be better to use the current standard procedure and estimate the probability factors separately. The results from the case studies emphasise the importance of solid interpretation of the final risk levels and their implications, as this supports the decision-making in risk evaluation and trade studies in requirement and functional analyses and the design synthesis in systems-engineering processes. Also, risk-assessment results and risk-reduction proposals should show a clear distinction between system supplier's actions and end-user actions.

The case-study results emphasise that risk assessment in unique automated mobile work-machine customer applications should be understood as a top-down process wherein upper-work-site-level assessment results represent input and requirements for the next level, ensuring that the system-safety requirements and risk-reduction solutions are based on the actual site-specific factors involved, not merely on theoretical worst-case scenarios.

The results of this study can be utilised among mobile work-machine manufacturers, system suppliers, end users of automated mobile work-machinery systems, and safety experts. The results of this study serve as a good foundation for the future applications and development of a system-safety approach in complex automated machinery applications. From the results of this study, one can determine how the approach to risk assessment might be usefully planned and imple-

mented, and the risk-analysis methods could be utilised in complex automated machinery applications other than mobile work-machine systems.

Standardisation of machinery safety and functional safety engineering guidelines has developed strongly over the last decade. Automation safety engineering guidelines for automated or fully automatic mobile work-machine systems are still absent, however. The results of this study can be used in the development of risk-assessment guidelines for individual automated mobile work machines or entire autonomous mobile work-machine-fleet applications.

References

Ahonen, T., Jännes, J., Kunttu, S., Valkokari, P., Venho-Ahonen, O., Välisalo, T., & Franssila, H. (2012). *Dependability management – from standard to practice.* VTT Technology 69 (in Finnish). Espoo: VTT. http://www.vtt.fi/inf/pdf/technology/2012/T69.pdf

Alanen, J. (2010). Assessing safety of CAN-communications systems. *In the proceedings of the 6th International Conference on safety of Industrial Automation Systems (SIAS 2010). June 14–15, 2010, Tampere, Finland.*

Alanen, J., Hietikko, M., & Malm, T. (2004). *Safety of Digital Communications in Machines.* Espoo: VTT Technical Research Centre of Finland.

Amaral, L., & Uzzi, B. (2007, July). Complex system – A new paradigm for the interactive study of management, physical, and technological systems. *Management science, 53*(7), 1033–1035.

Bellamy, D., & Pravica, L. (2011). Assessing the impact of driverless haul trucks in Australian surface mining. *Resources Policy, 36*(2), 149–338.

Boucher, M., & Kelly-Rand, C. (2011). *System Design Get it Right the First Time.* Aberdeen Group Inc. Retrieved October 1, 2013, from ftp://ftp.usmp.edu.pe/separatas/FIA/posgrado/doctorado/2011-2/Gestion%20de%20la%20Infraestructura%20de%20TI/articulos/Aberdeen%20System-design-engineering.pdf

BS 18004. (2008). *Guide to achieving effective occupational health and safety performance.* BSI.

Burger, D. (2006). Integration of the mining plan in a mining automation system using state-of-the-art technology at De Beers Finsch Mine. *Journal of the South African institute of Mining and Metallurgy, 106*, 553–560.

Cockburn, A. (2001). *Writing Effective Use Cases.* Addison-Wesley.

Cox Jr, L. A. (2008). What's Wrong with Risk Matrices? *Risk Analysis, 28*(2), 497–511.

Directive 2006/42/EC. (2006). Directive 2006/42/EC of the European parliament and of the council of 17 May 2006 on Machinery. European Commission. *Official Journal of the European Union*, L 157, pp. 24–86.

Directive 2009/104/EC. (2009). *Directive 2009/104/EC of the European parliament and of the council of 16 September 2009 concerning the minimum safety and health requirements for the use of work equipment by workers at work.* European Commission. Official Journal of the European Union, L 260, pp. 5–19.

Directive 89/391/EEC. (1989). *Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work.* European Commission. Official Journal of the European Union, L 183, pp. 1–8.

DoD DAU. (2001). *Systems Engineering Fundamentals.* Department of Defence. Defence Acquisition University Press.

Dunjó, J., Fthenakis, V., Vilchez, J. A., & Arnaldos, J. (2010). Hazard and operability (HAZOP) analysis. A literature review. *Journal of Hazardous Materials 173 (2010)*, 19–32.

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. *Academy of Management Review, 14*(4), 532–550.

EN 50126-1. (1999). *Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Basic requirements and generic process.* Standard.

Endsley, M. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors, 37*(1), 32–64.

Ericsson, M. (2012). *Mining technology – trends and development.* POLINARES Consortium.

Eskola, J., & Suoranta, J. (2005). *Johdatus laadulliseen tutkimukseen, 7. painos.* Jyväskylä: Vastapaino.

FAA ATO. (2006). *National Airspace System, System Engineering Manual.* Federal Aviation Administration, Air traffic Organisation.

Fadier, E., & De la Garza, C. (2007). Towards a proactive safety approach in the design process: The case of printing machinery. *Safety Science 45 (2007)*, 199–229.

FIMA. (2007). *FIMA Forum for Intelligent Machines – Research*. Retrieved September 24, 2013, from http://www.hermiagroup.fi/fima/in_english/research/

FIMA. (2011). *FIMECC EFFIMA FAMOUS – Future Semi-Autonomous Machines for Safe and Efficient Worksites.* Retrieved 12 17, 2013, from FIMA – Forum for Intelligent Machines ry, Tutkimusprojektit: http://www.hermiagroup.fi/fima/tutkimusprojektit/famous/

FIMECC. (2012). *FIMECC EFFIMA – Energy and Life Cycle Cost Efficient Machines*. Retrieved September 24, 2013, from http://www.fimecc.com/content/effima-energy-and-life-cycle-cost-efficient-machines

Fiscor, S. (2008). Finsch Automates Diamond Mining. *Engineering and Mining Journal, 209*(1), 36–43.

Fraser, I. (2009). Guide to application of Directive 2006/42/EC – 1st Edition. European Comission.

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The qualitative report, 8*(4), 597–607.

Granholm, G. (2013). *A look into the life-cycle design of complex systems.* VTT Technology 121 (in Finnish). Espoo: VTT. http://www.vtt.fi/inf/pdf/technology/2013/T121.pdf

Gustafson, A. (2011). *Automation of Load Haul Dump Machines.* Luleå: Luleå University of Technology.

Günther, H.-O., & Kim, K.-H. (2006). Container terminals and terminal operations. *OR Spectrum, 28*, 437–445.

Hedberg, J. A., Malm, T., Kivipuro, M., & Sivencrona, H. (2006). *Methods for Verification & Validation of time-triggered embedded systems.* Oslo: Nordic Innovation Centre.

Heikkilä, A.-M., Murtonen, M., Nissilä, M., & Virolainen, K. (2007). *The quality of risk analyses: requirements for the customer and for the conducter of the analyses.* Espoo: VTT Technical Research Centre of Finland.

Hietikko, M., Alanen, J., & Malm, T. (2010). A safety process reference model and tool for the development of machine control systems. *In the proceedings of the 6th International Conference on safety of Industrial Automation Systems (SIAS 2010). June 14–15, Tampere, Finland.*

Hietikko, M., Malm, T., & Alanen, J. (2009). *Functional safety of machine control systems. Instructions and tools for the creation of standard process.* VTT Research Notes 2485 (in Finnish). Espoo: VTT.

Hietikko, M., Malm, T., & Alanen, J. (2011). Risk estimation studies in the context of a machine control system. *Reliability Engineering and System Safety, 96, 7 (2011)*, 767–774.

Hietikko, M., Malm, T., & Saha, H. (2013). Evaluating performance levels of machine control functions. *CAN newsletter. CAN in Automation, 2 (2013)*, 32–37.

Hollnagel, E. (2008). Risk + barriers = safety? *Safety Science, 46*, 221–229.

Huelke, M., Hauke, M., & Pilger, J. (2008). *SISTEMA: a Tool for the Easy Application of the Control Standard EN ISO 13849-1, White paper.*

Hyötyläinen, R. (2005). *Practical interests in theoretical consideration – Constructive methods in the study of the implementation of information systems.* Espoo: VTT Technical Research Centre of Finland.

IEC 60204-1. (2000). *Safety of machinery – Electrical equipment of machines – Part 1: General requirements.* IEC.

IEC 61511-1. (2003). *Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements.* IEC.

IEC 61511-2. (2004). *Functional safety – Safety instrumented systems for the process industry sector – Part 2: Guidelines for the application of IEC 61511-1.* IEC.

IEC 61511-3. (2003). *Functional safety – Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels.* IEC.

IEC 61882. (2001). *Hazard and operability studies (HAZOP studies) – Application guide.* IEC.

IEC 62278. (2002). *Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS).* IEC.

IEC ISO 31010. (2009). *Risk management – Risk management techniques. Interna-tional Organization for Standardization (ISO).* IEC/ISO.

IEEE 1233. (1998). *IEEE Guide for Developing System Requirements Specifications.* IEEE.

ISO 11850. (2011). *Machinery for forestry – General safety requirements.* ISO.

ISO 14121. (1999). *Safety of machinery. Principles for risk assessment.* ISO.

ISO 14121-1. (2007). *Safety of machinery. Risk assessment. Part 1: Principles.* ISO.

ISO 20474-1. (2008). *Earth-moving machinery – Safety – Part 1: General requirements.* ISO.

ISO 26262-2. (2011). *Road vehicles – Functional safety – Part 2: Management of functional safety.* ISO.

ISO 31000. (2009). *Risk Management – Principles and guidelines. International Organization for Standardization (ISO).*

ISO Guide 73. (2009). *Risk management – Vocabulary.* ISO.

ISO IEC 12207. (2008). *Systems and software engineering – Software life cycle processes.* ISO.

ISO IEC 15288. (2008). *Systems and software engineering – System life cycle processes (IEEE Std 15288-2008); Second edition.*

ISO IEC 16085. (2006). *Systems engineering – Risk management (IEEE Std 16085-2006).*

ISO IEC 26702. (2007). *Systems engineering – Application and management of the systems engineering process (IEEE Std 1220-2005); First edition.*

ISO IEC Guide 51. (1999). *Safety aspects – Guidelines for their inclusion in standards.* ISO/IEC.

ISO IEC TR 24748-1. (2010). *Systems and Software Engineering – life cycle management – Part 1: Guide for life cycle management.* ISO.

ISO TR 14121-2. (2007). *Safety of machinery. Risk assessment. Part 2: Practical guidance and examples of methods.* ISO.

ISO TR 19961. (2010). *Cranes – Safety code on mobile cranes.* ISO.

Jämsä-Jounela, S.-L., & Baiden, G. (2009). Automation and Robotics in Mining and Mineral Processing. In *Springer Handbook of Automation* (pp. 1001–1013). Springer.

Jännes, J. (2011). *Availability and safety management in early design phases* (in Finnish). Tampere: Tampere University of Technology.

Kaplan, S. (1997). The words of risk analysis. *Risk analysis, 17*(4), 407–417.

Kaplan, S., & Garrick, J. (1981). On The Quantitative Definition of Risk. *Risk Analysis, 1*(1), 11–27.

Kariuki, S., & Löwe, K. (2007). Integrating human factors into process hazard analysis. *Reliability Engineering and System Safety 92 (2007)*, 1764–1773.

Kasanen, E., Lukka, K., & Siitonen, A. (1991). Konstruktiivinen tutkimusote liiketaloustieteessä. In *Liiketaloudellinen aikakauskirja 3.* Pp. 301–329.

Kasanen, E., Lukka, K., & Siitonen, A. (1993). The constructive approach in management accounting research. *Journal of Management Accounting Research, 5*, 243–264.

Kivistö-Rahnasto, J. (2000). *Machine safety design. An approach fulfilling European safety requirements.* VTT Publications 411. Espoo: VTT Technical Research Centre of Finland.

Kuivanen, R. (1995). *Methodology for simultaneous robot system safety design.* VTT Publications 219. Espoo: VTT.

Lammi, J. (2007). *Developing a UI Design Pattern Library – A Case Study at eCraft.* Espoo: Helsinki University of Technology.

Lauesen, S. (2003). Task descriptions as functional requirements. *IEEE Software, 20*(2), 58–65.

Lauesen, S., & Kuhail, M. (2012). Task descriptions versus use cases. *Requirements Engineering, 17*(1), 3–18.

Leveson, N. (1995). *Safeware.* Addison-Wesley.

Leveson, N. (2003). *White Paper on Approaches to Safety Engineering.* Retrieved April 7, 2011, from http://sunnyday.mit.edu/caib/concepts.pdf

Leveson, N. (2004). A New Accident Model for Engineering Safer Systems. *Safety Science, 42*(4), 237–270.

Leveson, N. (2011 a). Applying systems thinking to analyze and learn from events. *Safety Science 49 (2011)*, 55–64.

Leveson, N. (2011 b). *Engineering a Safer World. System Thinking Applied to Safety.* Cambridge: The MIT Press.

Leveson, N. (2012). Complexity and safety. *Complex Systems Design & Management CSDM 2011*. Pp. 27–39.

Lewis, H. (1990). *Technological risk.* New York, NY: W. W. Norton & Company, Inc.

Lukka, K. (2000). The key issues of applying the constructive approach to field research. In T. Reponen, *Management expertice for the new millenium. In commemoration of the 50th anniversary of Turku School of Economics and Business Administration. Serie A-1*. Pp. 113–128.

Lundteigen, M., Rausand, M., & Utne, I. (2009). Integrating RAMS engineering and management with the safety life cycle of IEC61508. *Reliability Engineering and System Safety 94 (2009)*, 1894–1903.

Malm, T., Hämäläinen, V., & Kivipuro, M. (2001). *Safety and reliability of roll handling in paper mills.* Espoo: VTT Teachnical Research Centre of Finland.

Malm, T., Vuori, M., Rauhamäki, J., Vepsäläinen, T., Koskinen, J., Seppälä, J., & Katara, M. (2011). *Safety-critical software in machinery applications.* Espoo: VTT Technical Research Centre of Finland.

MIL-STD-882D. (2000). *Standard Practice for System Safety.* Department of Defence.

NASA. (2007). *NASA systems engineering handbook. Technical Report NASA/SP-2007-6105.* Washington, DC: U.S. National Aeronautics and Space Administration.

Nielsen, J. (1993). *Usability Engineering.* Boston, MA: Academic Press.

Olkkonen, T. (1993). *Johdatus teollisuustalouden tutkimustyöhön. Report 152 (in Finnish).* Espoo: Teknillinen korkeakoulu, Tuotantotalouden laitos, tuotantotalouden laboratorio.

Oyegoke, A. (2011). The constructive research approach in project management research. *International Journal of Managing Projects in Business, 4*(4), 573–595.

Paques, J.-J., Durka, J.-L., & Bourbonnière, R. (1999). Practical use of IEC 61508 and EN 954 for the safety evaluation of an automatic mining truck. *Reliability Engineering and System Safety*, 127–133.

Pátkai, N. (2006). *A Data Management Tool for Conducting HAZOP Studies. Master of Science Thesis.* Tampere: Tampere University of Technology, Department of Mechanical Engineering, Institute of Occupational Safety Engineering.

Patton, M. (1999, December). Enhancing the quality and credibility of qualitative analysis. *Health services research, 34*(5 Part II), 1189–1208.

Pukkila, J. (1999). *Implementation of Mine Automation: The importance of Work Safety and Motivation.* Espoo: Finnish Academy of Technology.

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science, 27*(2), 183–213.

Raunio, H. (12. April 2013). Kontti kulkee käsin koskematta. *Tekniikka & Talous*. Helsinki: Talentum Media Oy.

Rausand, M. (2011). *Risk Assessment: Theory, Methods, and Applications.* Hoboken, NJ: John Wiley & Sons, Inc.

Rausand, M. (2014). *Reliability of safety-critical systems. Theory and applications.* Hoboken, NJ: John Wiley & Sons, Inc.

Rausand, M., & Utne, I. (2009). Product safety – Principles and practices in a life cycle perspective. *Safety Science 47 (7) 2009*, 939–947.

Redmill, F., Chudleigh, M., & Catmur, J. (1999). *System Safety: HAZOP and Software HAZOP.* Chichester: John Wiley & Sons Ltd.

Renn, O. (1998). The role of risk perception for risk management. *Reliability Engineering and System Safety, 59*, 49–62.

Reunanen, M. (1993). *Systematic safety consideration in product design.* Espoo: VTT.

Rohweder, L. (2008). Konstruktiivinen tutkimusote pedagogiikan kehittämisessä. Kohti kestävää kehitystä. In *Pedagoginen lähestymistapa. Opetusministeriön julkaisuja 2008:3* (in Finnish).

Roland, H., & Moriarty, B. (1983). *System safety engineering and management.* Hoboken, NJ: John Wiley & Sons.

Roland, H., & Moriarty, B. (1990). *System Safety Engineering and Management (2nd Edition).* Hoboken, NJ: John Wiley & Sons.

Rouhiainen, V. (1990). *The quality assessment of safety analysis.* Espoo: VTT Technical Research Centre of Finland.

Saaranen-Kauppinen, A., & Puusniekka, A. (2006). Tapaustutkimus. In *KvaliMOTV – Menetelmäopetuksen tietovaranto. http://www.fsd.uta.fi/menetelmäopetus/.* Tampere: Yhteiskuntatieteellinen tietoarkisto.

Sammarco, J. J. (2002). Addressing the Safety of Programmable Electronic Mining Systems. *Industry Application Conference 13–18 Oct. 2002. 37th IAS Annual Meeting*. Pp. 692–698.

Sammarco, J. J. (2005a). Operationalizing normal accident theory for safety-related computer systems. *Safety Science, 43 (2005)*, 697–714.

Sammarco, J. J. (2005b). *Programmable Electronic mining Systems: Best Practice Recommendations. Part 6: 5.1 System Safety Guidance.* National Institute for Occupational Safety and Health (NIOSH).

Sammarco, J., Fisher, T., Welsh, J., & Pazuchanics, M. (2001). *Programmable Electronic Mining Systems: Best Practice. Part 1: 1.0 Introduction.* Pittsburgh: NIOSH.

Scott, J. (2012). Trends in marine terminal automation. *Port Technology International, Edition 54*, 82–85.

SE Handbook. (2011). *Systems Engineering Handbook A guide for system life cycle processes and activities.* San Diego: INCOSE.

SFS 5974. (2011). *Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control.* SFS.

SFS EN 61508-1. (2011). *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements.* Sesko ry.

SFS EN 61508-4. (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and Abbreviations.* SFS.

SFS EN 61508-5. (2011). *Functional safety of electric/electronic/programmable electronic safety-related systems. Part 5: Examples of methods for the determination of safety integrity levels.* SFS.

SFS EN 62061. (2005). *Safety of machinery: Functional safety of electrical, electronic and programmable electronic control systems.* SFS.

SFS EN ISO 12100. (2010). *Safety of machinery. General principles for design. Risk assessment and risk reduction.*

SFS EN ISO 13849-1. (2007). *Safety of machinery. Safety-related parts of control systems. Part 1: General principles for design.* SFS.

SFS IEC 60300-3-9. (2000). *Dependability management. Part 3: Application guide. Section 9: Risk analysis of technologicial systems.* Sesko ry.

Silius, K.;& Tervakari, A.-M. (2003). *Verkkopalveluiden käyttökelpoisuuden arviointi. Portaalipäivä 20.11.2003.* (In Finnish.) Digitaalisen median instituutti, Hypermedialaboratorio, Tampereen teknillinen yliopisto.

Stenbacka, C. (2001). Qualitative research requires quality concepts of its own. *Management Decision, 39*(7), 551–555.

Stephans, R. (2004). *System safety for the 21st century.* Hoboken, NJ: John Wiley & Sons.

Stephenson, J. (1991). *System safety 2000: A practical guide for planning, managing, and cunducting system safety programs.* Hoboken, NJ: John Wiley & Sons.

Sundquist, M. (2013). Toiminnallisen turvallisuuden kehittäminen. *Automaatiopäivät 2013, SAS julkaisusarja nro 42.* Suomen Automaatioseura ry.

Tervakari, A.-M. (2008). *Evaluation model for usefulness*. Retrieved June 25, 2013, from http://hlab.ee.tut.fi/hmopetus/vpkk-oppimateriaali/3-arviointimalleja/3-3-malleja-ja-kriteereja/3-3-3-kayttokelpoisuuden-arviointim

Tiusanen, R. (1999). Safety of CAN-bus applications in working machines. *Proceedings of the first Conference on Safety of Industrial Automated Systems (SIAS). Montreal, CA, 5–7 Oct. 1999.* Pp. 201–205. Montreal: IRSST.

Tiusanen, R. (2000). Risk assessment of automated working machinery. *Proceedings of the 7th International Conference on Human Aspects of Advanced Manufacturing: Agility & Hybrid Automation – III.* Pp. 333–336. Krakow: Jagiellonian University.

Tiusanen, R. (2006). Operating hazard identification in automated mining machine systems. In V. Rouhiainen, *Safety and reliability. Technology theme – Final report*. Pp. 77–83. Espoo: VTT.

Tiusanen, R. (2013b). Systems Engineering Approach to Risk Assessment of Automated Mobile Work Machine Applications. *Proceedings of the 8th World Congress on Engineering Asset Management, WCEAM 2013.* To be published by Springer.

Tiusanen, R., Helin, K., & Karjalainen, J. (2005). Operating Hazard Analysis for automated mining machine systems. In M. Nuutinen & J. Luoma, *Human practice in the life cycle of complex systems. Challenges and methods.* VTT Publications 582. Pp. 26–32. Espoo: VTT.

Tiusanen, R., Hietikko, M., Alanen, J., Pátkai, N., & Venho, O. (2008). *System safety concept for machinery systems.* Espoo: VTT.

Tiusanen, R., Malm, T., & Ronkainen, A. (2012). Adaptive safety concepts for automated mobile work machine systems: simulator assisted research approach. *Proceedings of the 7th International Conference on the Safety of Industrial Automated Systems (SIAS 2012).* Montreal: IRSST.

Tiusanen, R., Malm, T., & Viitaniemi, J. (2013a). Simulator assisted design approach for adaptive safety concepts in automated mobile work machine systems. *Proceedings of the Automation XX Seminar Automation without borders – beyond Future.* Helsinki: The Finnish Society of Automation.

Toola, A. (1992). *Safety analysis in conceptual design of process control. VTT publications 117.* Espoo: VTT Technical Research Centre of Finland.

Uusisalo, J. (2011). *A case study on effects of remote control and control system distribution in hydraulic mobile machines.* Tampere: Tampere University of Technology.

Vilenius, J. (2007). *Characteristics of valve controlled hydraulic power transmission in teleoperated skid steered mobile machine.* Tampere: Tampere University of Technology.

Vincoli, J. W. (2006). *Basic Guide to System Safety.* Hoboken, NJ: John Wiley & Sons, Inc.

VNa 400/2008. (2008). *Valtioneuvoston asetus koneiden turvallisuudesta.*

VNa 403/2008. (2008). *Valtioneuvoston asetus työvälineiden turvallisesta käytöstä ja tarkastamisesta.*

Yin, R. (2009). *Case Study Reseach. Design and Methods. 4th ed. Applied Social Research Methods Vol 5. 2009.* SAGE Publications, Inc.

Appendix 1: The PHA worksheet template used in Case 1

Nr	Arbetsuppgift							
Område	Risk	Orsak	Konsekvens	S	P	R	Säkerhetsåtgärder	Ansvar
DEL B Arbetet under produktion								
B 1 B 2 B 3	Skrotning, bergförstärkning Ventilation Vägunderhåll							
B 4	Schaktunderhåll, Normalt procedur							
B 5	Maskin inspektion							
B 6	Förebyggande underhåll maskin							
B 7	Salvskrotning, efter varje skjutning							
B 8	Säkerhetssystem							
B 9	1000 V och 220 V systemen							

Appendix 2: The HAZOP worksheet template used in Case 1

Studie överskrift: **HAZOP analys av LUCS, LRCS, LDS och RRCS**	**Datum:**
Referens bild:	**Team medlemmar:**
Part 5: Signaler till och från LRCS	**Uppdaterad**

Element 1: Rubrik text
Funktionens syfte:

No.	Avvikelser (med styr ord)	Orsaker	Konsekvenser	Upptäckning och skyddsåtgärder	Korrektiva åtgärder

Element 2: Rubrik text
Funktionens syfte:

Appendix 3: The PHA worksheet template used in Case 3

HAZARD IDENTIFICATION AND RISK ASSESSMENT FINSCH BLOCK 4					RISK RANKING (no controls in place) Person risks are marked **Bold**			MANUFACTURER OR SUPPLIER'S STRATEGIES OR CONTROLS	RECOMMENDED CONTROLS TO BE IMPLEMENTED BY THE MINE MANAGEMENT	RISK RANKING (with Supplier and Mine controls in place)		
No	TASK	HAZARD	CAUSE OF RISK	EFFECT OR CONSEQUENCE	P	S	R			P	S	R
1.	Machinery and sub system testing in workshop area											
1.	System integration and testing in production area											

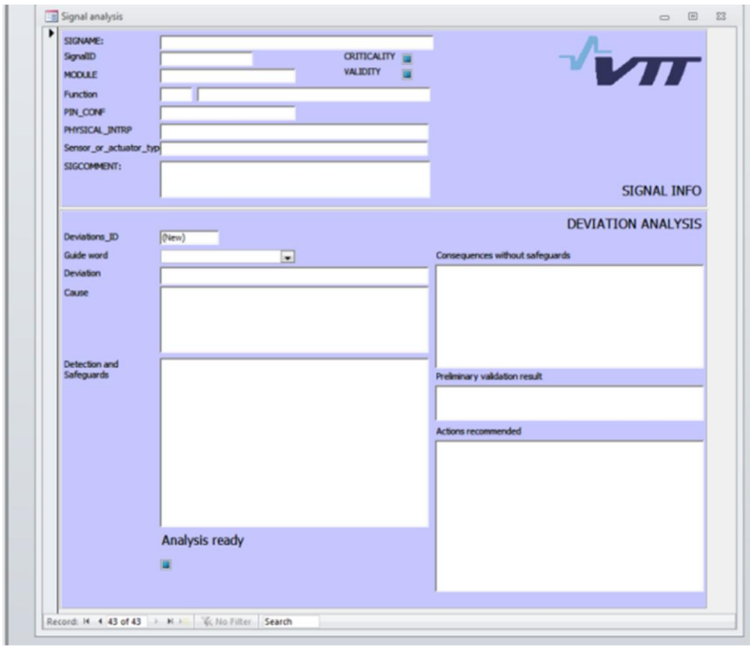
Appendix 4: The HAZOP worksheet template used in Case 3

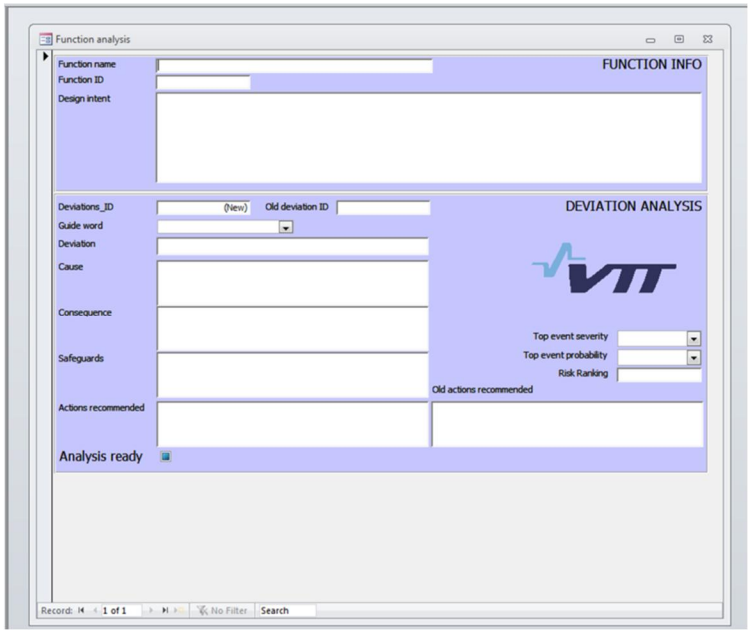
HAZOP STUDY: ACS Use Cases *FINSCH MINE BLOCK 4*			RISK RANKING *(no controls in place)* *Person risks are marked* **Bold**			*Detection and safeguards*	*Comments and proposals for corrective actions*	RISK RANKING *(with Supplier and Mine controls in place)*		
No.	*Deviation with guide word*	*Causes*	*Consequences*	***P***	***S***	***R***			***P***	***S***	***R***
1. Heading **Design intent:**											
2. Heading **Design intent:**											

Appendix 5: The OHA worksheet template used in Case 4

OPERATING HAZARD ANALYSIS AND RISK ASSESSMENT (OHA) *Automatic Stacking Crane System*				RISK RANKING (without safety measures)			SAFETY MEASURES	RISK RANKING (with safety measures)		
OPERATION / WORK TASK										
No	HAZARD	CAUSE	CONSEQUENCE	P	S	R		P	S	R
1. Heading										
1.1 Sub-heading Description										
1.1.1										
1.2 Sub-heading Description										
1.2.1										

Appendix 6: The HAZOP worksheet templates used in Case 4





Series title and number

VTT Science 69

Title	**An approach for the assessment of safety risks in automated mobile work-machine systems**
Author(s)	Risto Tiusanen
Abstract	Needs to improve productivity and cost efficiency are driving the development in industrial sectors using mobile work-machines towards automated work-machine systems and production process control.The shift from manually operated mobile work machines toward automated mobile work-machine systems takes machinery-safety considerations to a new, system safety, level. New safety concerns are associated with automation-related threats and possible unexpected hazardous events. Regardless of the extensive international standardisation efforts in machinery safety, there are not yet safety-engineering or risk-assessment guidelines specific to complex automated mobile work-machine systems. The aim of this study has been to provide new information on how the risk-analysis methods in current use can be utilised for reaching the system-safety objectives and to increase the quality and effectiveness of safety-engineering work. The main goal of this study was a practical approach for system-level safety-risk assessment in automated mobile work-machine systems. Constructive research approach has been applied for the construction of the risk assessment approach. Evaluation of the usefulness of the overall approach and risk analysis methods has been done following the qualitative case-study research methods. The empirical research material consists of four case project documentation, interview results and observations. The result of the study is a new three-level approach for the assessment of safety risks. The results of the study show that the three-level approach to risk assessment is applicable for automated mobile work-machine systems and the selected methods are applicable for system-level hazard identification and risk analysis. The approach and the methods have been adopted in case companies. The developed approach integrates key elements from system safety, machinery safety and industrial safety engineering practices. The case-study research results provide new valuable information and experiences in how the risk-identification and risk-estimation methods were utilised in the case projects in various phases of the system life cycle. The results can be utilised among mobile work-machine manufacturers, system suppliers, end users of the machinery systems, and safety experts.
ISBN, ISSN	ISBN 978-951-38-8172-6 (Soft back ed.) ISBN 978-951-38-8173-3 (URL: http://www.vtt.fi/publications/index.jsp) ISSN-L 2242-119X ISSN 2242-119X (Print) ISSN 2242-1203 (Online)
Date	November 2014
Language	English, Finnish abstract
Pages	200 p. + app. 6 p.
Name of the project	
Commissioned by	
Keywords	Risk management, system safety, risk, hazard, mobile work machine, automation
Publisher	VTT Technical Research Centre of Finland P.O. Box 1000, FI-02044 VTT, Finland, Tel. 020 722 111

Julkaisun sarja ja numero

VTT Science 69

Nimeke	**Lähestymistapa automatisoitujen työkonejärjestelmien turvallisuusriskien arviointiin**
Tekijä(t)	Risto Tiusanen
Tiivistelmä	Työkoneita käytetään laajalti eri teollisuudenaloilla ja hyvin erilaisissa teollisissa ympäristöissä. Työn tuottavuutta ja kustannustehokkuutta pyritään parantamaan nostamalla työkoneiden automaatiotasoa ja automatisoimalla työprosessien ohjausta. Muutos manuaalisesti ohjatuista työkoneista kohti automatisoituja työkonejärjestelmiä siirtää koneiden turvallisuustarkastelun uudelle järjestelmäturvallisuustasolle. Turvallisuuden näkökulmasta huolta tässä muutoksessa aiheuttavat erityisesti uudenlaiset automatisointiin liittyvät uhat ja mahdolliset odottamattomat vaaratilanteet. Huolimatta turvallisuussuunnittelun laaja-alaisesta kansainvälisestä standardointityöstä vielä toistaiseksi ei ole käytettävissä turvallisuussuunnittelun tai riskien arvioinnin ohjeita kompleksisia automatisoituja työkonejärjestelmiä varten. Tämän tutkimuksen tarkoituksena on ollut tuottaa uutta tietoa siitä, miten riskianalyysimenetelmiä nykymuodossaan tulisi käyttää järjestelmäturvallisuustavoitteiden saavuttamiseksi ja kuinka parantaa turvallisuussuunnittelun laatua ja tehokkuutta. Tutkimuksen keskeinen tavoite oli käytännöllinen järjestelmätason lähestymistapa automatisoitujen työkonejärjestelmien turvallisuusriskien arviointiin. Tutkimustyö on edennyt konstruktiivisen tutkimusotteen mukaisesti. Riskin arvioinnin lähestymistavan ja valittujen riskianalyysimenetelmien käyttökelpoisuutta on evaluoitu kvalitatiivisen tapaustutkimuksen menetelmin. Empiirinen tutkimusaineisto koostuu neljän case-projektin dokumentaatiosta, haastatteluista ja havainnoista. Tutkimuksen tuloksena syntyi uusi kolmitasoinen lähestymistapa turvallisuusriskien arviointiin. Tulokset osoittavat, että kolmitasoinen lähestymistapa soveltuu käytettäväksi automatisoitujen työkonejärjestelmien turvallisuusriskin arviointiin ja valitut menetelmät soveltuvat järjestelmätason vaaratekijöiden tunnistamiseen ja niiden analysointiin. Lähestymistapa ja menetelmät on otettu käyttöön soveltuvin osin case-yrityksissä. Kehitetty lähestymistapa yhdistää keskeisiä elementtejä järjestelmäturvallisuuden, koneturvallisuuden ja työturvallisuuden käytännöistä. Case-tutkimusten tulokset antavat uutta arvokasta tietoa siitä, kuinka riskin tunnistamisen ja arvioinnin menetelmiä käytettiin case-projekteissa kohdejärjestelmien eri elinkaaren vaiheissa. Tuloksia voivat hyödyntää liikkuvien työkoneiden valmistajat, järjestelmätoimittajat, konejärjestelmien loppukäyttäjät ja järjestelmäturvallisuuden asiantuntijat.
ISBN, ISSN	ISBN 978-951-38-8172-6 (nid.) ISBN 978-951-38-8173-3 (URL: http://www.vtt.fi/publications/index.jsp) ISSN-L 2242-119X ISSN 2242-119X (Painettu) ISSN 2242-1203 (Verkkojulkaisu)
Julkaisuaika	Marraskuu 2014
Kieli	Englanti, suomenkielinen tiivistelmä
Sivumäärä	200 s. + liitt. 6 s.
Projektin nimi	
Rahoittajat	
Avainsanat	Riskien hallinta, järjestelmäturvallisuus, riski, vaara, työkone, automaatio
Julkaisija	VTT PL 1000, 02044 VTT, puh. 020 722 111

An approach for the assessment of safety risks in automated mobile work-machine systems

The shift from manually operated mobile work machines toward automated mobile work-machine systems takes machinery-safety considerations to a new, system safety, level. The aim of this study has been to provide new information on how the risk-analysis methods in current use can be utilised for reaching the system-safety objectives and to increase the quality and effectiveness of safety-engineering work. The main goal of this study was a practical approach for safety-risk assessment in complex mobile work-machine systems. The result of the research work is a new three-level approach and system-level analysis methods for risk assessment.

The results of the case-studies show that the three-level approach to risk assessment is applicable for automated mobile work-machine systems and the selected methods are applicable for system-level hazard identification and risk analysis. The developed approach integrates key elements from system safety, machinery safety and industrial safety engineering practices. The approach and the methods have been adopted in case companies and the results can be utilised widely in mobile work-machine industry, end users of the machinery systems, and safety experts.

ISBN 978-951-38-8172-6 (Soft back ed.)
ISBN 978-951-38-8173-3 (URL: http://www.vtt.fi/publications/index.jsp)
ISSN-L 2242-119X
ISSN 2242-119X (Print)
ISSN 2242-1203 (Online)

VTT publications

VTT employees publish their research results in Finnish and foreign scientific journals, trade periodicals and publication series, in books, in conference papers, in patents and in VTT's own publication series. The VTT publication series are VTT Visions, VTT Science, VTT Technology and VTT Research Highlights. About 100 high-quality scientific and professional publications are released in these series each year. All the publications are released in electronic format and most of them also in print.

VTT Visions
This series contains future visions and foresights on technological, societal and business topics that VTT considers important. It is aimed primarily at decision-makers and experts in companies and in public administration.

VTT Science
This series showcases VTT's scientific expertise and features doctoral dissertations and other peer-reviewed publications. It is aimed primarily at researchers and the scientific community.

VTT Technology
This series features the outcomes of public research projects, technology and market reviews, literature reviews, manuals and papers from conferences organised by VTT. It is aimed at professionals, developers and practical users.

VTT Research Highlights
This series presents summaries of recent research results, solutions and impacts in selected VTT research areas. Its target group consists of customers, decision-makers and collaborators.