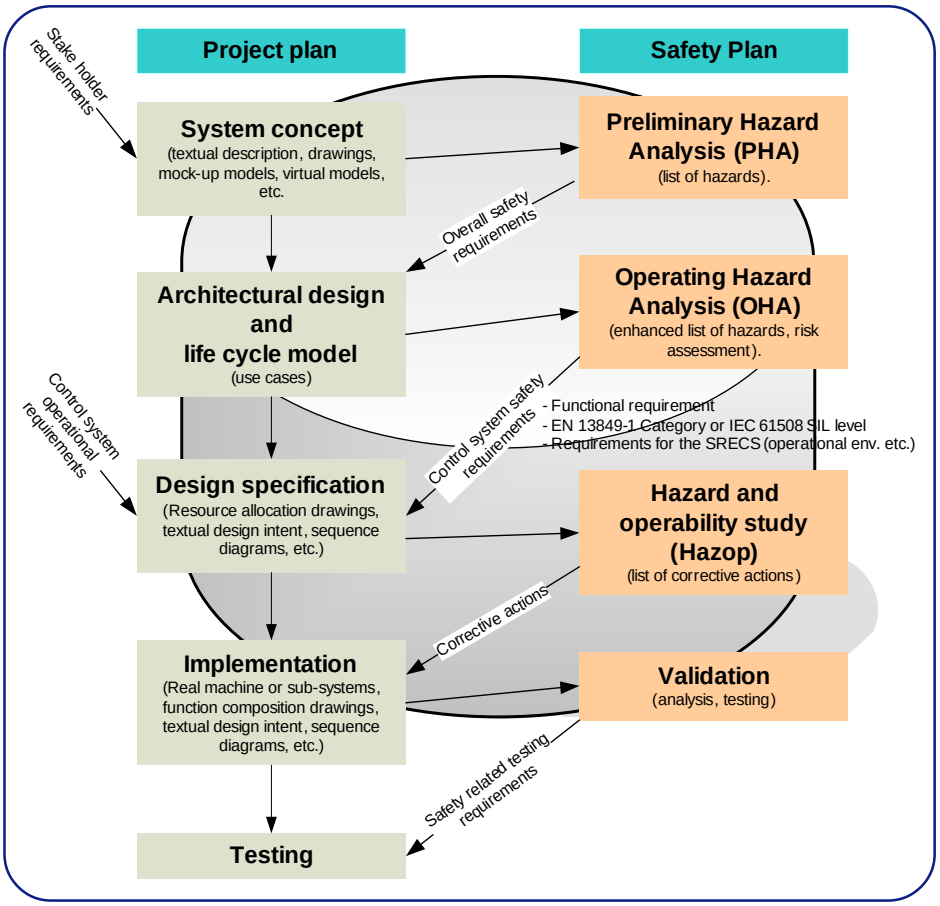

Risto Tiusanen, Marita Hietikko, Jarmo Alanen, Nina Pátkai & Outi Venho

System Safety Concept for Machinery Systems

VTT TIEDOTTEITA – RESEARCH NOTES 2437

System Safety Concept for Machinery Systems

Risto Tiusanen, Marita Hietikko, Jarmo Alanen,
Nina Pátkai & Outi Venho

ISBN 978-951-38-7214-4 (soft back ed.)
ISSN 1235-0605 (soft back ed.)

ISBN 978-951-38-7215-1 (URL: http://www.vtt.fi/publications/index.jsp)
ISSN 1455-0865 (URL: http://www.vtt.fi/publications/index.jsp)

JULKAISIJA – UTGIVARE – PUBLISHER

VTT, Vuorimiehentie 3, PL 1000, 02044 VTT
puh. vaihde 020 722 111, faksi 020 722 4374

VTT, Bergsmansvägen 3, PB 1000, 02044 VTT
tel. växel 020 722 111, fax 020 722 4374

VTT Technical Research Centre of Finland, Vuorimiehentie 3, P.O. Box 1000, FI-02044 VTT, Finland
phone internat. +358 20 722 111, fax +358 20 722 4374

VTT, Tekniikankatu 1, PL 1300, 33101 TAMPERE
puh. vaihde 020 722 111, faksi 020 722 3495

VTT, Teknikvägen 1, PB 1300, 33101 TAMMERFORS
tel. växel 020 722 111, fax 020 722 3495

VTT Technical Research Centre of Finland, Tekniikankatu 1, P.O. Box 1300, FI-33101 TAMPERE, Finland
phone internat. +358 20 722 111, fax +358 20 722 3495

Technical editing Anni Repo

Edita Prima Oy, Helsinki 2008

Tiusanen, Risto, Hietikko, Marita, Alanen, Jarmo, Pátkai, Nina & Venho, Outi. System Safety Concept for Machinery Systems [Järjestelmäturvallisuuskonsepti työkonejärjestelmien riskien hallintaan]. Espoo 2008. VTT Tiedotteita – Research Notes 2437. 53 p.

Keywords system safety, risk management, machinery systems, working machine, HAZOP

Abstract

There are several new trends for moving machines that will affect also on the requirements for the safety and reliability of machines. Working machines will become more and more evidently a part of the production process. When the machines are remotely controlled and the machine control is developing towards machine fleet control and management, the focus on machine safety issues changes to system safety issues and the risk management of the whole operational environment. In future, automated, remote controlled and autonomously moving machines will no longer be stand-alone machines but rather are parts of the automated production systems and when developing those, the whole production process and operation environment have to be considered. There is a need for knowledge about how to specify system safety requirements and system reliability requirements for the unique machine application at different levels. There is also a need for new procedures on how to manage system safety and reliability risks through the whole life cycle of the system.

The scope of this study has been to develop a generic concept and procedure for the safety risk management of automated working machine systems, which tends to take into account interactions between human, technology and environment when specifying safety requirements to the system and designing, implementing and maintaining safety solutions. Special attention has been paid to describing the risk management process, the needed methods and tools and information management.

The developed “System Safety Concept” and safety requirement management is related to Systems engineering and the concept follows the System life cycle model and Risk assessment principles (IEC 60300-3-9, ISO 14121). The control and automation system parts comply with IEC 61508, ISO 13849 and IEC 62061 principles. As a result of this research, a data management tool for conducting HAZOP studies on the MS Access 2002 platform was developed from the viewpoint of the System Safety concept.

Laajennettu tiivistelmä

Liikkuvien työkoneiden osalta on tunnistettavissa useita trendejä, jotka tulevaisuudessa vaikuttavat myös koneiden turvallisuudelle ja käyttövarmuudelle asetettaviin vaatimuksiin. Työkoneet ovat yhä selvemmin muuttumassa osaksi tuotantoprosessia, ja niiden elinikäisen turvallisuuden ja käyttövarmuuden osuus lisäarvon tuottamisessa kasvaa merkittävästi. Koneiden etäkäyttö lisääntyy, ja työprosessi tulee muodostumaan yhä useammin koneiden muodostamasta tuotantoketjusta. Siirryttäessä yksittäisen koneen ohjaamisesta konejärjestelmän hallintaan siirtyy myös turvallisuuskysymysten painopiste koneturvallisuudesta konejärjestelmän ja sen toimintaympäristön riskien hallintaan.

Tulevaisuuden automatisoidut, etäohjatut ja jopa autonomisesti liikkuvat koneet eivät enää ole yksittäisiä työkoneita, vaan ne ovat asiakasohjautuvasti räätälöityjä järjestelmiä, joita kehitettäessä ja suunniteltaessa on tarkasteltava koko tuotantoprosessia ja sen toimintaympäristöä.

Tarvitaan uutta osaamista määritellä turvallisuus- ja käyttövarmuusvaatimukset järjestelmien sovellustasolla ja toimintotasolla. Tarvitaan myös uusia menettelytapoja hallita automatisoidun konejärjestelmän turvallisuuteen ja käyttövarmuuteen liittyvät riskit konejärjestelmän koko elinkaaren ajan.

Tämän tutkimuksen tarkoituksena oli kehittää automatisoitujen työkonejärjestelmien turvallisuusriskien hallintaan uutta geneeristä lähestymistapaa, joka pyrkii huomioimaan ihmisen, teknologian ja ympäristön vuorovaikutukset järjestelmän turvallisuusvaatimusten määrittelyssä ja turvallistavien ratkaisujen suunnittelussa, toteuttamisessa ja ylläpidossa. Lähestymistavan kuvauksessa huomioidaan erityisesti riskien hallinnan prosessi, tarvittavat menetelmät ja työkalut sekä tiedonhallinnan periaatteet.

Hankkeen yhteydessä tutkittiin erityisesti poikkeamatarkastelun (HAZOP) soveltamista konejärjestelmän käyttötilanteiden (use cases) ja ohjausjärjestelmän toimintojen (functions) analysointiin sekä ohjausjärjestelmien turvallisuuskriittisten signaalien analyysiin.

Hankkeessa kehitettiin relaatiotietokanta järjestelmän turvallisuuskonseptiin kuuluvalle analyysimenetelmälle. Järjestelmäturvallisuuskonseptin laajuuden vuoksi työssä päädyttiin keskittymään HAZOP-poikkeamatarkastelumenetelmään, siitä toteutettavan tietokannan vaatimusten määrittelemiseen ja tietokannan toteuttamiseen.

Case-kohteena järjestelmäturvallisuuskonseptin testauksessa oli Kalmar Industries OyAB:n kehittämä automaattinen konttinosturijärjestelmä.

Hankkeen tuloksena saatiin menettelytapa työkonejärjestelmän turvallisuusriskien hallintaan. Menettelytapaa kuvaa nimi ”järjestelmäturvallisuuskonsepti” (System Safety concept, ks. esim. lähde MIL-STD 882C), joka tarkoittaa niitä toimenpiteitä, joiden avulla konejärjestelmästä saadaan niin turvallinen kuin on mahdollista järjestelmän suunnitellussa käyttöympäristössä, suunnitelluilla käyttötavoilla ja käytettävissä olevalla nykyteknologialla.

Järjestelmäturvallisuuskonsepti ja turvallisuusvaatimusten hallinta liittyvät oleellisena osana vaatimustenhallinnan yleisempään toimintatapaan (System engineering) ja noudattelevat konejärjestelmän elinkaarimallia (System life cycle model) sekä riskin arvioinnin periaatteita (IEC 60300-3-9, ISO 14121). Koneiden ohjaus- ja automaatiojärjestelmän osalta järjestelmäturvallisuuskonsepti noudattelee toiminnallisen turvallisuuden kansainvälisten standardien IEC 61508, ISO 13849 ja IEC 62061 periaatteita.

Kehitetyn järjestelmäturvallisuuskonseptin kolme keskeistä analyysimenetelmää ovat seuraavat:

- ”Alustava vaara-analyysi” (Preliminary Hazard Analysis, PHA), jota käytetään konejärjestelmän ja sen käyttöympäristön keskeisten vaarojen tunnistamiseen, analysointiin ja riskien arviointiin.
- ”Tehtäväkohtainen vaara-analyysi” (Operation Hazard Analysis, OHA), jossa tarkastellaan järjestelmän käytön ja kunnossapidon toimintokuvausten (Use cases) mukaisia tilanteita ja niihin liittyviä virhemahdollisuuksia, häiriöitä ja vikatilanteita. Tarkasteltavia käyttötilanteita ovat mm. järjestelmän installointi, testaus ja käyttöönotto, järjestelmän käyttö (operointi), päivittäiset työt automaatio-alueella, ennakoivan kunnossapidon työt sekä vianhaku- ja korjaustyöt.
- ”Ohjaus- ja automaatiojärjestelmän poikkeamatarkastelu” (Hazard and Operability analysis, HAZOP), jossa analysoidaan systemaattisesti ohjausjärjestelmän turvallisuuteen liittyvät toiminnot ja varsinaiset turvatoiminnot (System level safety-related functions, safety functions).

Hankkeessa kehiteltiin myös edellä mainittujen analyysimenetelmien tulosten linkittämistä toisiinsa ja ohjausjärjestelmän turvallisuusvaatimusten määrittelyyn ja allokointiin (Safety Requirement Specification, EN 13849-1). Tämä edellyttää, että em. analyysit tehdään tuotekehitysprojektin tai asiakasprojektin oikeassa vaiheessa, jolloin analyysien tuottamaa tietoa voidaan hyödyntää projektin seuraavissa vaiheissa konkreettisina mitattavina turvallisuusvaatimuksina, suunnitteluperiaatteina tai turvallistavina toimenpide-ehdotuksina. Näin menetellen asetetut vaatimukset ja sovellettavat ratkaisut perustuvat konejärjestelmän todellisiin turvallisuusriskeihin.

Tärkeä uusi osa-alue tässä järjestelmäturvallisuuskonseptissa on tunnistaa konejärjestelmän installointiin, integrointiin ja käyttöönottoon liittyvät vaarat ja arvioida niihin liittyvät riskit. Tyypillisesti tarkastellaan vain koneiden tuotantokäyttöä ja kunnossapitoa. Käyttöönottovaiheessa ei vielä ole käytössä kaikkia tuotannon aikaisia suojausteknisiä ratkaisuja ja turvallisuus joudutaan varmistamaan muilla järjestelyillä ja erilaisilla toimintaohjeilla.

Karkea riskiluokitus (kolme seuraustasoa ja kolme todennäköisyystasoa, joista sitten suoraan kertomalla saadaan riskitaso: R = S x P) riittää hyvin alustavassa vaaraanalyysissä (PHA) tunnistettujen vaarojen aiheuttaman riskin arviointiin. Tehtäväkohtaisessa analyysissä (OHA) käytettiin 5 x 5 riskimatriisia. Määrittelemällä tasot yksikäsitteisesti saatiin selkeästi esille seurausten vakavuuden ja todennäköisyyden merkitys.

Järjestelmäturvallisuuskonseptiin liittyvien analyysien ja riskienarvioinnin tekemistä ja tulosten hyödyntämistä tukemaan kehitettiin relaatiotietokantaan perustuvaa tietokantatyökalua. Diplomityönä toteutetussa osatehtävässä päädyttiin järjestelmäturvallisuuskonseptin laajuuden vuoksi keskittymään poikkeamatarkastelun menetelmän (ohjausjärjestelmän HAZOP-analyysi) ja siitä toteutettavan tietokannan vaatimusten määrittelemiseen sekä tietokannan toteuttamiseen.

Ongelman laajuuden vuoksi päädyttiin rajaamaan työn kohderyhmäksi ammattilaiset, jotka tekevät poikkeamatarkasteluanalyysejä työssään. Asiakkaille toteutettavan työkalun tulee olla helppokäyttöinen, koska heillä ei ole välttämättä kokemusta eri analyysimenetelmistä. Tämän vuoksi asiakkaille kehitettävän työkalun vaatimukset tulee määrittää erikseen.

Tietokannan toteutuksen osalta kehitystyössä noudatettiin kansainvälistä HAZOP-standardia IEC 61882, jonka avulla pyrittiin saamaan analyysien teosta systemaattisempaa työntekijöiden kesken. Kirjallisuuden avulla tutustuttiin menetelmiin, joita käytettiin tietokannan kehittämisen eri vaiheissa. Tietokannan vaatimukset määriteltiin ”Contextual Design” -menetelmän avulla, jossa tulevat käyttäjät otettiin tiiviisti mukaan tietokannan eri suunnitteluvaiheisiin. Aluksi tietokannasta kehitettiin paperimalleja ja pohdittiin tietokannan toimintoja käyttäjän näkökulmasta. Tämän jälkeen MS Access 2002 -ohjelmiston avulla kehitettiin käyttöliittymästä malleja, joista kaikissa ei ollut vielä toiminnallisuutta. Käytettävyystestaukset toteutettiin Nielsenin kymmenen kohdan heuristiikan mukaisesti. Tämän menetelmän avulla löydettiin ongelmia tietokannan käytettävyydessä. Käytettävyystestit suoritettiin kolmen testihenkilön kanssa. Parannusehdotusten ja kommenttien perusteella tehtiin muutoksia, jotka nämä kolme käyttäjää testasivat vielä uudelleen.

Tulevaisuudessa on tarkoituksena kehittää laajempi tietokanta, jossa olisi useita järjestelmäturvallisuuskonseptiin kuuluvia analyysimenetelmiä linkitettynä toisiinsa. Aikaisempiin työtapoihin verrattuna työssä kehitetyn HAZOP-tietokannan avulla tietoa on entistä helpompi etsiä ja muokata. Lisäksi erilaisten raporttien tuottaminen on nopeampaa ja alusta mahdollistaa työkalun kehittämisen.

Kalmar Industries OyAB:n kanssa tutkittiin järjestelmäturvallisuuskonseptin lähestymistavan ja systematiikan toimivuutta ja testattiin tietokantapohjaisia analyysityökaluja yrityksen uuden nosturiautomaatiosovelluksen kehitystyön yhteydessä.

Preface

This publication presents the results of the research project “From Machines to systems – New challenges for risk management. Case – safety risk management in an automatic container crane system”. The project was conducted by VTT Technical Research Centre of Finland during 2005–2007.

The project manager at VTT was Senior Research Scientist Risto Tiusanen. Project team members at VTT were Research Scientist Jarmo Alanen, Senior Research Scientist Marita Hietikko, Technician Vesa Hämäläinen, Technician Pekka Kivinen and Research Assistant Nina Pátkai.

Members of the project management group were Director Ilkka Tahvanainen from the Finnish Work Environment Fund, Automation R&D Manager Pekka Yli-Paunu from Kalmar Industries and Senior Research Scientist Pasi Valkokari from VTT.

This project was financially supported by the Finnish Work Environment Fund, VTT and Kalmar Industries.

Tampere, February 2008

Authors

Risto Tiusanen, Marita Hietikko, Jarmo Alanen, Nina Pátkai & Outi Venho

Contents

List of abbreviations

CDR	Critical Design Review
E/E/PES	Electrical/Electronic/Programmable Electronic System
EHA	Environmental Hazard Assessment
EUC	Equipment Under Control
FMECA	Failure Modes, Effects and Criticality Analysis
FRR	Functional Requirements Review
FTA	Fault Tree Analysis
MA	Managing Activity
OHA	Operating Hazard Analysis
PDR	Preliminary Design Review
PES	Programmable Electronic System
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
PL	Performance Level
RAC	Risk Assessment Code
RAMS	Reliability, Availability, Maintainability, Safety
SAR	Safety Assessment Report
SCA	Safety Compliance Assessment
SCR	System Concept Review
SE	System Engineering
SIL	Safety Integrity Level
SRP/CS	Safety-Related Part of a Control System
SRS	Safety-Related System
SSHA	SubSystem Hazard Analysis
SSPP	System Safety Program Plan
SSWG	System Safety Working Group

1. Introduction

Tele-operated and autonomously moving machines are no longer stand-alone machines, but are parts of the automated production systems, which are controlled from the control room via a factory-wide communication network. In the mining industry, the biggest open pit mines use unmanned dumpers, and in some of the largest underground mines, loading machines, dumpers, and ore transporting trains are tele-operated via radio and video links. In large container terminals, container handling systems move and stack containers automatically. The control room can be far from the production area. In most advanced systems, mobile machines operate autonomously using their onboard navigation systems, which detects the environment and compares it with pre-programmed routes and maps.

In the most commonly used version of machine remote control, the operator stands beside the machine or at least in the vicinity of the machine. This is called remote control line of sight. The control commands are linked via a cable or radio transmitter. In many cases, the operator's working conditions are improved by moving the location of the remote control to a separate vehicle or building. The distance from the machine can be several hundred metres, and the driving is achieved with a video link.

When the machines are remotely controlled and the machine control is developing towards machine fleet control and management, the focus on machine safety issues changes to system safety issues and the risk management of the whole operational environment.

These changes and development trends provide the machine manufacturers, system designers and end users with difficult challenges in terms of safety issues.

The relation between the risk assessment procedure and the conformity to the essential health and safety requirements is not clear or unambiguous when talking about machine systems. Present machinery safety standards give the basic principles and procedures for the risk assessment of a single machine. They do not, however, supply instructions on how to apply the principles at the machine system level.

Safeguarding principles for large automated material handling systems have been studied at VTT with system suppliers in the late nineties (Malm et al. 1998). The risk assessment approach for mobile mining machinery has been developed and applied in VTT with Sandvik Mining and Construction since 1995. The focus in this development has been on stand-alone manual machinery and their remote control (Tiusanen 2000).

In large-scale machine automation applications, the safety-related remote control functions are complicated and difficult to analyse. They can be compared with automation systems in process industries. Safety-related control functions in highly automated machine systems include multi-dimensional aspects such as the operator's actions, user interface communication protocols and machine level control signals.

There is a need for knowledge about how to specify system safety requirements and system reliability requirements for the unique machine application at different levels. There is also a need for new procedures on how to manage system safety and reliability risks throughout the whole life cycle of the system.

The new idea in the system safety concept presented in this report is to combine different analysis tools to cover the entire machine system: use of the machinery, operators' actions, system level control functions, and machine level safety issues. The automated machine system is divided into sub systems such as the local safeguarding system in the production area, machine level systems, communication system, the production control system and the remote control stations.

The aim of this study has been to develop a generic concept and procedure for the safety risk management of automated working machine systems. The system safety concept and all of the system safety tasks should be understood as an essential part of the ordinary systems engineering work. In this system safety concept and procedure, the human–technology interactions related to remotely controlled machinery will be considered particularly when specifying safety requirements and designing safeguarding principles.

The case system in this project was an automatic crane system in a harbour container terminal. Automatic cranes are used for stacking and in-stack transportation. It leaves and picks up containers from a dedicated area at front-end stacks. A similar dedicated area is used also in the landside end of the stacks. Stacks are located crosswise to the quayside. Manual shuttle carriers, trailers or unmanned AGVs are used to transport the containers from the ship-to-shore crane to the front of the stacks. The automatic stacking cranes are monitored and operated from a control room. Loading and unloading of road trucks is carried out via tele-operation from the control room.

2. Theoretical approach

2.1 Systems engineering

International Council on Systems Engineering (INCOSE) defines systems engineering as follows: *"Systems Engineering is an interdisciplinary approach and means to enable the realization of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, then proceeding with design synthesis and system validation while considering the complete problem:*

- *Operations,*
- *Cost & Schedule,*
- *Performance,*
- *Training & Support,*
- *Test,*
- *Disposal,*
- *Manufacturing.*

Systems Engineering integrates all the disciplines and specialty groups into a team effort forming a structured development process that proceeds from concept to production to operation. Systems Engineering considers both the business and the technical needs of all customers with the goal of providing a quality product that meets the user needs." (INCOSE website.)

The Federal Aviation Administration (FAA) has published a System Engineering Manual (SEM), which describes the proper application of System Engineering (SE) elements within the FAA (FAA 2006).

2.2 System life cycle model

Ulrich and Eppinger have presented an approach to the system life cycle model (Ulrich & Eppinger 2000). Figure 1 describes the different life cycle phases according to this model.

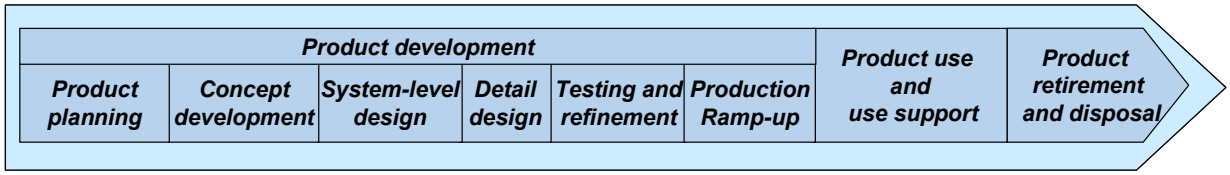

Figure 1. System life cycle model (Ulrich & Eppinger 2000).

The system life cycle is the sequence of phases, each containing tasks. The total system life cycle from initial concept to decommissioning is covered. An approach to how the railway RAMS management is carried out is presented in Figure 2.

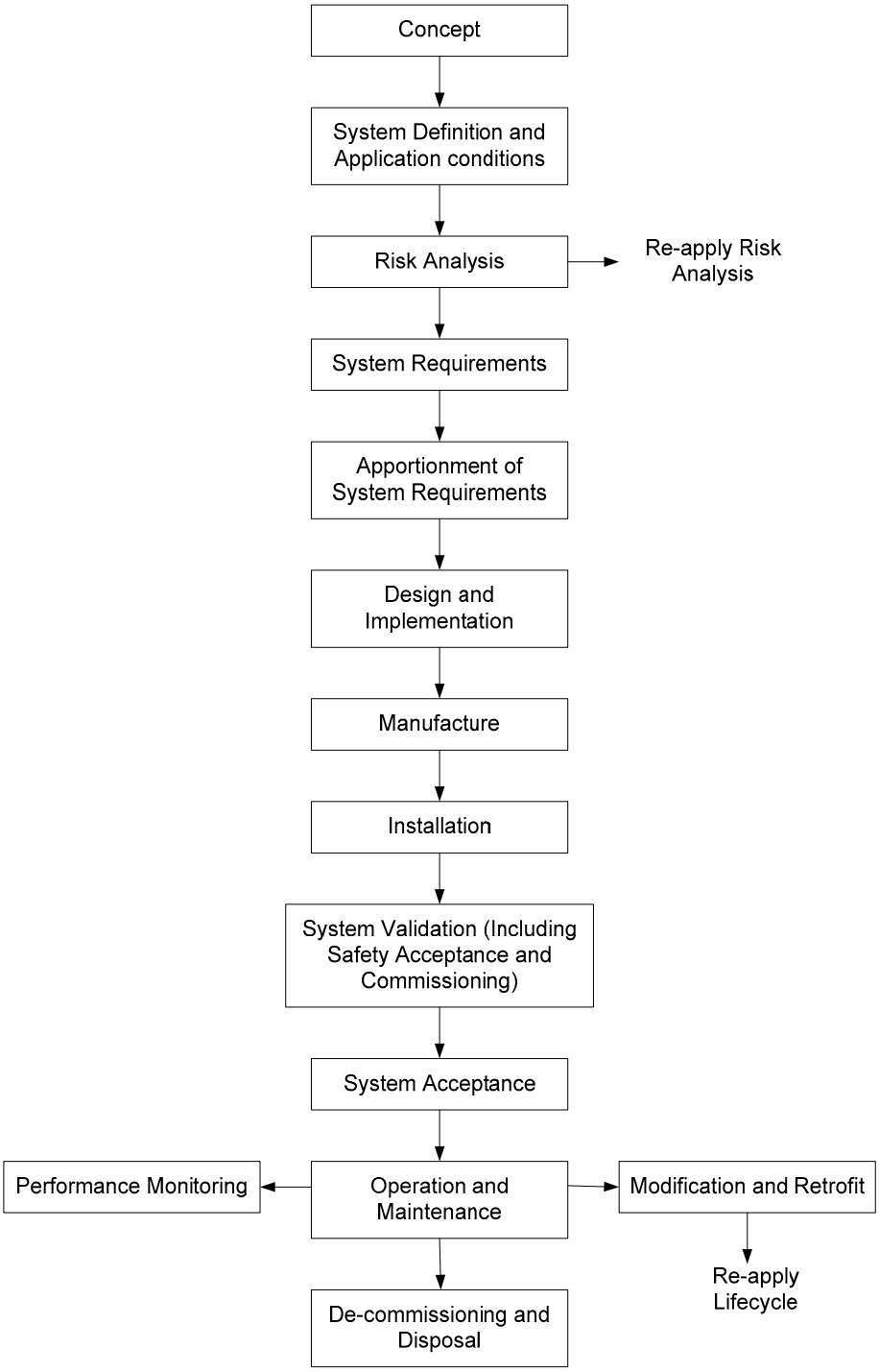

Figure 2. System life cycle (EN 50126 1999).

A concept of safety and reliability information system was developed in co-operation with VTT, MTT Vakola and Finnish machine manufactures in 2003–2004 using conceptual modelling. The initial part of the conceptualisation process involved interviews with industrial partners from Finland. Safety and reliability information management practices were studied in mobile machine manufacturing companies and their subcontracting companies. 26 persons including managing directors, R&D managers and designers were interviewed. The interviews were supported by questionnaires that were delivered to the companies in advance. Each person was interviewed separately and the results were documented (Suutarinen et al. 2005).

Basic RAMS program outlines were developed to cover two application areas. These included a general model for mobile machine manufacturing companies and a model for a company that delivers automated high performance warehousing and distribution systems. The basic RAMS program outlines consist of the descriptions of the appropriate life cycle or project phases, the phase-related RAMS tasks and responsibilities, results and deliverables of each RAMS program phase (Suutarinen et al. 2005).

System life cycle is a sequence of phases covering the total life cycle of a system from initial concept through to decommissioning and disposal. Companies are increasingly using the life cycle concept for their investment projects to provide a structure for planning, managing, controlling and monitoring all aspects of the system, including reliability, availability, maintainability and safety (i.e., RAMS). Special attention is often given to RAMS aspects in order to make sure that the asset shall operate during the life cycle under every circumstance in relation to reliability, availability, maintainability and safety. The supplier is typically obliged to support the RAMS activities during the project phases. In order to be able to do this, the supplier is – according to e.g. the standard EN 50126 (1999) – advised to establish a specific RAMS program for the purposes of the delivery project. This program proceeds iteratively with the project as the system design develops. The RAMS programs of similar projects or system requirements of a supplier may yield a “standard RAMS program” (basic RAMS program) which establishes the RAMS baseline of a company (Tiusanen 2006).

Standard EN 50126 (1999) describes project phase-related tasks for each life cycle phase. These tasks are divided into phase-related general tasks, RAM tasks and safety tasks (Figure 3).

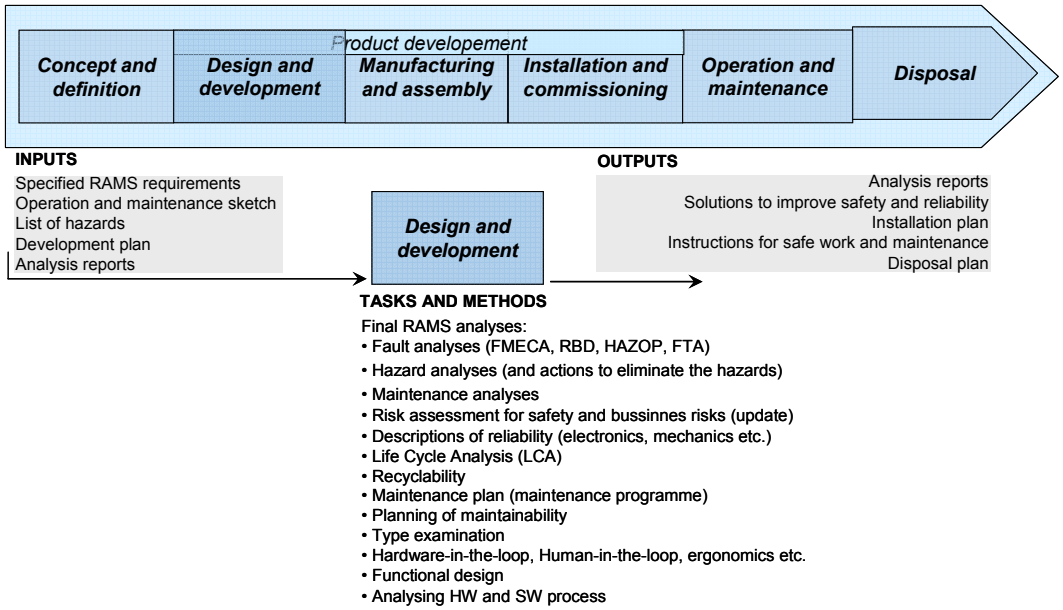

Figure 3. Example of RAMS tasks and method in the design and development phase modified from EN 50126 (1999).

2.3 Risk assessment principles

2.3.1 ISO 14121

Risk assessment is, according to ISO 14121 "Safety of machinery. Principles for risk assessment", a series of logical steps to enable, in a systematic way, the analysis and evaluation of the risks associated with machinery. Risk assessment is followed by risk reduction, if necessary. The iteration of this process might be necessary to eliminate hazards as far as practicable and to adequately reduce risks through the implementation of protective measures (ISO 14121 1999)

Risk assessment includes risk analysis and risk evaluation (Figure 4). Risk analysis includes the determination of the limits of the machinery, hazard identification and risk estimation.

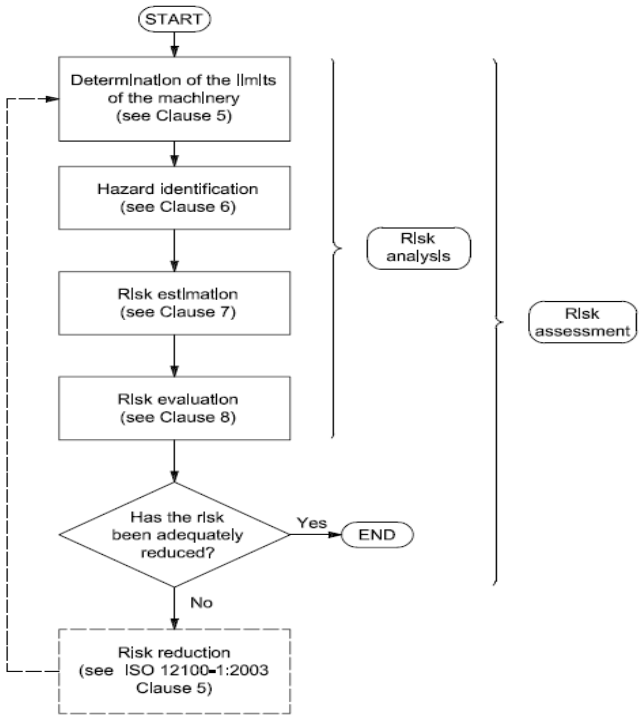

Figure 4. Risk analysis process (ISO 14121 1999).

2.3.2 IEC 60300-3-9

IEC 60300-3-9 (2006) provides guidelines for selecting and implementing risk analysis techniques, particularly for the risk assessment of technological systems. The aim of this standard is to ensure quality and consistency in the planning and implementing of risk analyses and the presentation of results and conclusions.

According to IEC 60300-3-9, risk assessment includes risk analysis (scope definition, hazard identification, risk estimation) and risk evaluation (risk tolerability decisions, analysis of options), whereas risk management also includes risk reduction and control (decision-making, implementation, monitoring).

The standard describes the risk analysis process, providing a guideline for planning, executing and documenting risk analyses (IEC 60300-3-9 2006).

2.4 Functional safety standards

2.4.1 IEC 61508

This international standard set out a generic approach for all safety life cycle activities for systems comprised of electrical/electronic/programmable electronic components that are used to perform safety functions. The standard provides a method for the development of the safety requirement specification necessary to achieve the required functional safety for E/E/PE safety-related systems.

The standard presents safety integrity levels for specifying the target level of safety integrity for the safety functions to be implemented with E/E/PE safety-related systems. It also adopts a broad range of principles, techniques and measures for both HW and SW to achieve functional safety.

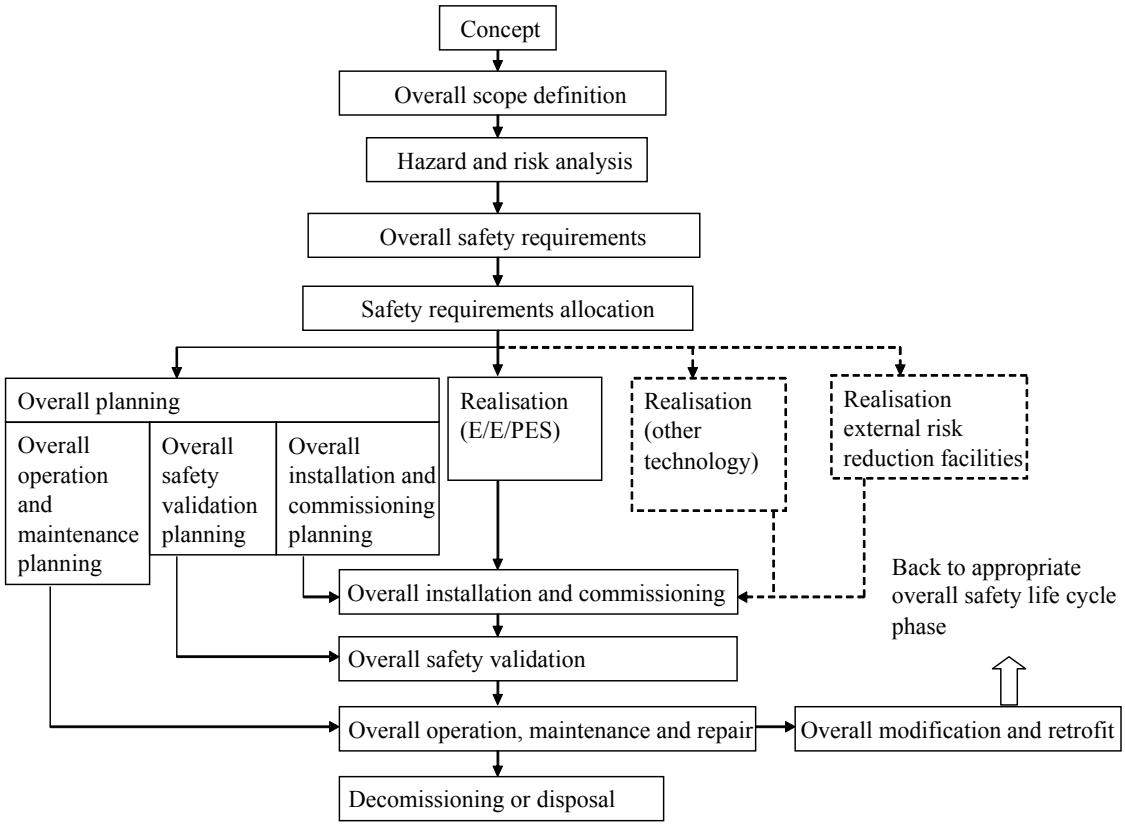

Figure 5. Overall safety life cycle model (IEC 61508-1 1998).

The phases in the overall safety life cycle model (Figure 5) are briefly described in the following sections. The information and results acquired in each phase of the overall safety life cycle model is documented.

In the **concept phase** of the system (EUC), the objective is to develop a level of understanding of the EUC and its environment (physical, legislative, etc.) sufficient to enable the other safety life cycle activities to be satisfactorily carried out. A thorough familiarity is acquired of the EUC, its required control functions and its physical environment. The likely sources of hazards have to be determined. Information about the determined hazards (toxicity, explosive conditions, corrosiveness, reactivity, flammability, etc.) as well as information about the current safety regulations (national and international) is obtained. Hazards due to interaction with other EUCs (installed or to be installed) in the proximity of the EUC are considered.

The objectives of the **overall scope definition phase** are to determine the boundary of the EUC and the EUC control system and to specify the scope of the hazard and risk analysis (for example process hazards, environmental hazards, etc.). The physical equipment, including the EUC and the EUC control system, to be included in the scope of the hazard and risk analysis is specified. In addition, the external events to be taken into account in the hazard and risk analysis, the subsystems that are associated with the hazards, and the type of accident-initiating events that need to be considered (e.g. component failures, procedural faults, human error, dependent failure mechanisms which can cause accident sequences to occur) are specified.

The objectives of **hazard and risk analysis** are to determine the hazards and hazardous events of the EUC and the EUC control system (in all modes of operation) for all reasonably foreseeable circumstances, including fault conditions and misuse, to determine the event sequences leading to the hazardous events and to determine the EUC risks associated with the hazardous events. Consideration has to be given to the elimination of the hazards. The requirements can be met by the application of either qualitative or quantitative risk analysis techniques.

The objective is to develop the specification for the **overall safety requirements**, in terms of the safety functions requirements and safety integrity requirements, for the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities, in order to achieve the required functional safety. The safety functions necessary to ensure the required functional safety for each determined hazard are specified. The necessary risk reduction is determined for each determined hazardous event. It may be determined in a quantitative and/or a qualitative manner. For situations where an application sector international standard exists, which includes the appropriate methods for directly determining the necessary risk reduction, then such standards may be used to meet the requirements.

The **safety functions**, contained in the specification for the overall safety requirements (both the safety functions requirements and the safety integrity requirements), are

allocated to the designated E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities. A safety integrity level is allocated to each safety function. The allocation is iterative, and if it is found that the necessary risk reduction cannot be met, then the architecture has to be modified and the allocation repeated.

A **plan for operating and maintaining** the E/E/PE safety-related systems is developed to ensure that the required functional safety is maintained during operation and maintenance. The plan specifies the routine actions that need to be carried out to maintain the required functional safety of the E/E/PE safety-related systems. The actions and constraints that are necessary (e.g. during start-up, normal operation, routine testing, foreseeable disturbances, faults and shutdown) to prevent an unsafe state, to reduce the demands on the E/E/PE safety-related system, or reduce the consequences of the hazardous events, are included in the plan. It also includes the documentation of hazardous incidents and all incidents with the potential to create a hazardous event, as well as the documentation of functional safety audits and tests. The scope of the maintenance activities, the actions to be taken in the event of hazards occurring and the contents of the chronological documentation of operation and maintenance activities are also specified in the plan. The routine maintenance activities that are carried out to detect unrevealed faults should be determined by systematic analysis.

The overall safety validation plan of the E/E/PE safety-related systems includes details of when the validation will take place and who shall carry out the validation. It includes the specification of the relevant modes of the EUC operation with their relationship to the E/E/PE safety-related system (preparation for use including setting and adjustment, start up, teach, automatic, manual, semi-automatic, steady state of operation, re-setting, shut down, maintenance, and reasonably foreseeable abnormal conditions). It includes specification of the E/E/PE safety-related systems that need to be validated for each mode of EUC operation before commissioning commences. It includes the technical strategy for the validation (e.g. analytical methods, statistical tests, etc.). It includes the measures, techniques and procedures which confirm that the allocation of safety functions has been carried out correctly (each safety function conforms with the specification for the overall safety functions requirements and safety integrity requirements). A specific reference to each element contained in the outputs from safety requirements and their allocation is included. The required environment in which the validation activities are to take place (e.g. for tests this would include calibrated tools and equipment), the pass and fail criteria; as well as the policies and procedures for evaluating the results of the validation, particularly failures, are also included.

A **plan for the installation and commissioning** of the E/E/PE safety-related systems is developed. This plan specifies the installation and commissioning schedule, responsibilities, procedures, sequences, relationships to the validation, etc.

Realisation is carried out according to IEC 61508-2 (2000) (hardware) and IEC 61508-3 (1998) (software). These standards give hardware and software-related life cycle models and statements for their application.

Overall installation and commissioning activities are carried out in accordance with the plans for the installation and commissioning of the E/E/PE safety-related systems. The information recorded during installation includes the documentation of installation activities as well as the resolution of failures and incompatibilities. Respectively, commissioning activities are carried out in accordance with the plan for the commissioning of the E/E/PE safety-related systems. The information recorded during commissioning includes the documentation of commissioning activities, references to failure reports, and the resolution of failures and incompatibilities.

The objective of **overall safety validation** is to ensure that the E/E/PE safety-related systems meet the specification for the overall safety requirements in terms of the overall safety functions requirements and overall safety integrity requirements, taking into account the safety requirements allocation for the E/E/PE safety-related systems. Validation activities are carried out according to the overall safety validation plan for the E/E/PE safety-related systems. All equipment used for quantitative measurements as part of the validation activities have to be calibrated against a specification traceable to a national standard or to the vendor's specification. The information recorded during validation includes documentation of the validation activities in chronological form and the version of the specification for the overall safety requirements being used. It also includes the safety function being validated (by test or by analysis) as well as tools and equipment used, along with calibration data. It includes the results of the validation activities. It also includes configuration identification of the item being tested, the procedures applied and the test environment. Discrepancies between expected and actual results are also included.

The objective of the requirements concerning **overall operation, maintenance and repair** is to operate, maintain and repair the E/E/PE safety-related systems in order that the required functional safety is maintained. The plan for maintaining the E/E/PE safety-related systems, the operation, maintenance and repair procedures for the E/E/PE safety-related systems, and the operation and maintenance procedures for software have to be implemented. The implementation of these items includes the initiation of actions like the implementation of procedures, the following of maintenance schedules, and the maintaining of documentation. It also includes periodical functional safety audits to be

carried out and the documenting of modifications that have been made to the E/E/PE safety-related systems.

Chronological documentation of operation, repair and maintenance of the E/E/PE safety-related systems has to be maintained. This documentation contains information on the results of functional safety audits and tests. The documentation of the time and cause of demands on the E/E/PE safety-related systems (in actual operation), together with the performance of the E/E/PE safety-related systems when subject to those demands, and the faults found during routine maintenance is included. In addition, documentation of modifications that have been made to the EUC, to the EUC control system and to the E/E/PE safety-related systems is included. The exact requirements for chronological documentation can be detailed in the application sector standards.

Overall modification and retrofit can be initiated only by the issue of an authorised request under the procedures for the management of functional safety. This request has to detail the determined hazards that may be affected, the proposed change (both hardware and software), and the reasons for the change. The objective is to ensure that the functional safety for the E/E/PE safety-related systems is appropriate, both during and after the modification and retrofit phase has taken place.

An impact analysis shall be carried out which includes an assessment of the impact of the proposed modification or retrofit activity on the functional safety of any E/E/PE safety-related system. The assessment includes a hazard and risk analysis sufficient to determine the breadth and depth to which subsequent overall, E/E/PES or software safety life cycle phases will need to be undertaken. Authorisation to carry out the required modification or retrofit activity is dependent on the results of the impact analysis. All modifications, which have an impact on the functional safety of any E/E/PE safety-related system, initiate a return to an appropriate phase of the overall, E/E/PES or software safety life cycles. All subsequent phases are then carried out in accordance with the procedures specified for each phase in IEC 61508-1 (1998). Chronological documentation has to be established and maintained, which includes the details of all modifications and retrofits as well as references to the modification or retrofit request, the impact analysis, re-verification and revalidation of data and results, and all documents affected by the modification and retrofit activity.

Decommissioning or disposal is carried out and documented according to the same principles as required for modification and retrofit. For example, impact analysis is required also in this phase.

2.4.2 ISO 13849-1

Part 1 of the ISO 13849 standard provides safety requirements and guidance on the principles for the design and integration of the safety-related parts of control systems (SRP/CS), including the design of software. For these safety-related parts, it specifies characteristics that include the performance level, which is required for carrying out safety functions. It applies to SRP/CS for all kinds of machinery, regardless of the type of technology and energy used. It also provides specific requirements for SRP/CS using programmable electronic system(s). This part of the standard does not specify the safety functions or performance levels that are to be used in a particular case. It does not give specific requirements for the design of products, which are parts of SRP/CS. The given principles such as categories or performance levels can be used (ISO 13849-1 2006).

The standard provides an overview of risk assessment and reduction, which is presented in Figure 6. The strategy for risk reduction at the machine is the same as defined in ISO 12100-1 (ISO 12100-1 2003, ISO 13849-1 2006):

- Hazard elimination or risk reduction by design;
- Risk reduction by safeguarding and possibly complementary protective measures; and
- Risk reduction through the provision of information for use about the residual risk.

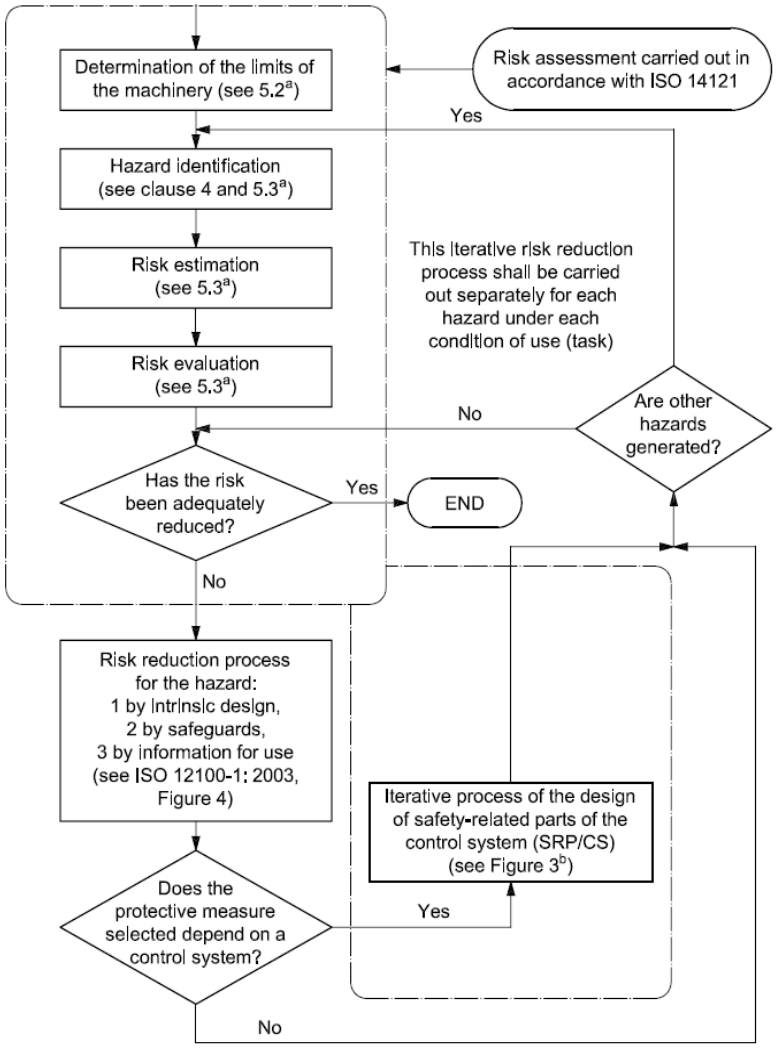

Figure 6. The strategy for risk reduction (ISO 13849-1 2006).

This part of ISO 13849 introduces performance levels. Performance level (PL) is defined as a discrete level used to specify the ability of safety-related parts of control systems to perform a safety function. Five performance levels (a to e) are set out, with defined ranges of probability of a dangerous failure per hour, as presented in Table 1.

Table 1. Performance levels and their correspondence to SIL levels.

PL	Average probability of dangerous failure per hour (1/h)	Corresponding SIL level
a	≥ 10^{-5} to 10^{-4}	no correspondence
b	≥ 3 x 10^{-6} to 10^{-5}	1
c	≥ 10^{-6} to 3 x 10^{-6}	1
d	≥ 10^{-7} to 10^{-6}	2
e	≥ 10^{-8} to 10^{-7}	3

2.4.3 IEC 62061

Standard IEC 62061 specifies requirements and makes recommendations for the design, integration and validation of safety-related electrical, electronic and programmable electronic control systems (SRECS) for machines. It is applicable to control systems used (either singularly or in combination) to carry out safety-related control functions on machines. Groups of machines working together in a co-ordinated manner are also included, whereas machines portable by hand are not included (IEC 62061 2007). Table 2 gives overview and objectives of IEC 62061.

Table 2. Overview and objectives of IEC 62061.

Task	**Objective**
Management of functional safety	Specification of the management and technical activities necessary for the achievement of the required functional safety of the SRECS.
Requirements for the specification of safety-related control functions	Setting out the procedures to specify the requirements for safety-related control functions. These requirements are expressed in terms of functional requirements specification, and safety integrity requirements specification.
Design and integration of the safety-related electrical control system	Specification of the selection criteria and/or the design and implementation methods of the SRECS to meet the functional safety requirements. This includes: – selection of the system architecture; – selection of the safety-related hardware and software; – design of hardware and software; and – verification that the designed hardware and software meets the functional safety requirements.
Information for use of the machine	Specification of the requirements for the information in use of the SRECS, which has to be supplied with the machine. This includes: – provision of the user manual and procedures, – provision of the maintenance manual and procedures.
Validation of the safety-related electrical control system	Specification of the requirements for the validation process to be applied to the SRECS. This includes the inspection and testing of the SRECS to ensure that it achieves the requirements stated in the safety requirements specification.
Modification of the safety-related electrical control system	Specification of the requirements for the modification procedure that has to be applied when modifying the SRECS. This includes: – modifications to any SRECS are properly planned and verified prior to making the change; and – the safety requirements specification of the SRECS is satisfied after any modifications have taken place.

2.5 System safety approach

2.5.1 History of System Safety

Many of the safety techniques and concepts were invented at the end of the Second World War. System Safety was addressed for the first time in a paper called "Engineering for Safety" in 1947 (Moriarty & Roland 1983). The paper stated that safety should be an important part of the design of an aeroplane and safety groups are an essential part of the manufacturer's organisation. An approach called "flyfixfly" is a good example of an ineffective safety program (Moriarty & Roland 1983, Stephenson 1991).

The approach can be described with aircrafts; an aeroplane is built and it works, after a while it gets broken therefore it has to be fixed and then it can be flown again (Moriarty & Roland 1983, Stephenson 1991). This approach was common before the 1940's amongst designers (Stephenson 1991).

The idea of System Safety evolved as missile systems were developed and space travel was researched. The need for safer systems increased in the late 1950s and early 60s. The Minuteman Intercontinental Ballistic Missile (ICBM) program was the first large step for System Safety, because it had a System Safety program (Stephans 2004), (Moriarty & Roland 1983). In 1966, a military specification MILS38130 (Military specification General Requirement for Safety Engineering of Systems and Associated Subsystems and Equipment) was published based on the ballistic system division program. The safety of systems was seriously taken into consideration when later in 1969 the MILSTD882 (System Safety Program for Systems and Associated Subsystems and Equipment: Requirements for) became mandatory for System Safety programs (Moriarty & Roland 1983).

2.5.2 MIL-STD 882C

MIL-STD 882C defines **System Safety** as follows: *"The application of engineering and management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle."* (MIL-STD 882C 1993.)

System safety engineering is defined in the MIL-STD 882C standard as follows: *"An engineering discipline requiring specialized professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify and eliminate hazards, in order to reduce the associated risk."*

System safety program plan (SSPP) is a description of the planned tasks and activities that are planned to be used by the contractor for implementing the required system safety program. This description includes organisational responsibilities, resources, methods of accomplishment, milestones, depth of effort, and integration with other program engineering and management activities and related systems.

"SSPP shall describe, in detail, tasks and activities of system safety management and system safety engineering that are required to identify, evaluate, and eliminate/control hazards, or reduce the associated risk to an acceptable level to the MA throughout the system life cycle. The approved plan provides a formal basis of understanding between the contractor and MA on how the system safety program will be executed to meet contractual requirements, including general and specific provisions." (MIL-STD 882C 1993.)

The contractor shall develop a SSPP to provide a basis of understanding between the contractor and the MA as to how the system safety program will be accomplished to meet contractual safety requirements included in the general and special provisions of the contract. The approved plan shall, on an item-by-item basis, account for all contractually required tasks and responsibilities, including those in the Statement of Work (SOW). The SSPP shall include the following:

- Program scope and objectives;
- System safety organisation;
- System safety program milestones;
- General system safety requirements and criteria;
- Hazard analysis;
- System safety data;
- Safety verification;
- Audit program;
- Training;
- Incident reporting; and
- System safety interfaces.

SSPP can be an annex to a project and quality plan. The preliminary SSPP may be presented together with the offer. SSPP defines the contractual obligations of system safety, the selected procedures and the distribution of liabilities, limitations and restrictions. SSPP covers the design, development, testing, use, support, and changes/modifications.

The safety analysis methods (e.g. FMECA, PHL, PHA, FTA, etc.) and the purpose of using them are described briefly in SSPP. One approach is described in Figure 7. In this approach, FMECA is used in the identification of risks and protective measures. PHL

gives data for PHA, which produces data of identified hazards, related hazard events, situations and mitigations to Hazard Log. Hazard Log is a collection of all risks with, among other things, descriptions, status information, pre and post ratings and hazard reduction principles. PHA also gives information for FTA, by means of which the hazard frequency is estimated. In addition, PHA gives information to the Safety Assessment Report (SAR), which summarises all the safety data produced for the system. SAR produces a summary of all the safety measures and the results of analyses used during the system safety work. Operating & Support Hazard Analysis (OHA) and Environmental Hazard Assessment (EHA) also produce information for Hazard Log (Liukkonen 2006).

Safety Compliance Assessment (SCA) is the declaration from the supplier that system safety is at an acceptable level. SAR and SCA will be supplied together with the system delivery.

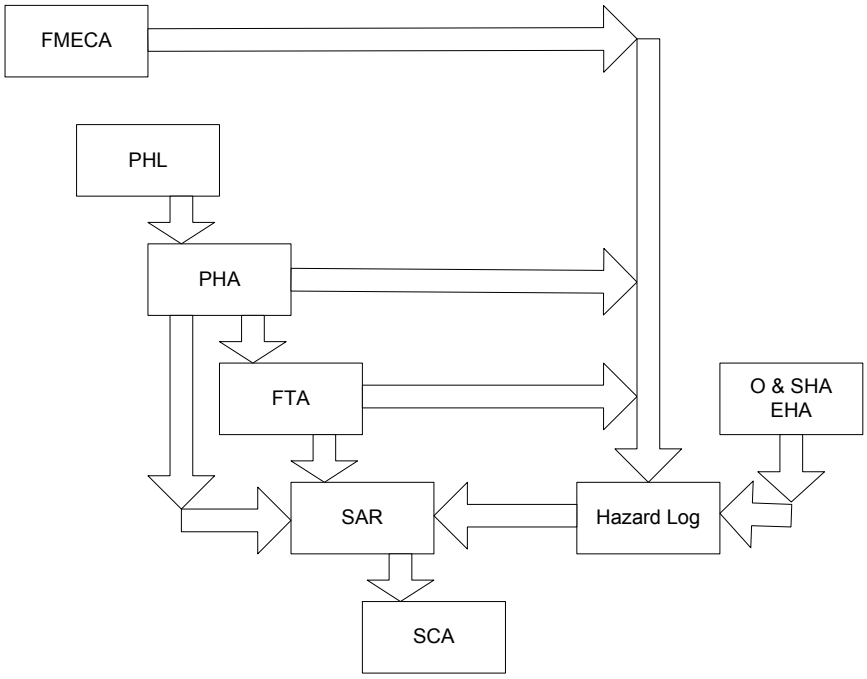

Figure 7. System safety flow (Liukkonen 2006).

Risk estimation is carried out in terms of risk severity and risk probability as follows:

- risk severity (catastrophic, critical, marginal, remote)
  - definitions for personnel, system/property and environment
- risk probability (frequent, probable, occasional, remote, improbable, incredible)

=> risk classification / risk matrix.

Figure 8 shows an example of a risk matrix (Liukkonen 2006).

		Consequence			
		1	2	3	4
Frequence	a	A	A	A	B
	b	A	A	B	C
	c	A	B	C	C
	d	B	C	C	D
	e	C	C	D	D
	f	C	D	D	D

Figure 8. Example of a risk matrix (Liukkonen 2006).

In Figure 8, the classification of risks is defined as follows: Class A means intolerable risk, Class B means undesirable risk, Class C means limited tolerable risk, and Class D means tolerable risk.

Sub System Hazard Analysis (SSHA) is a document, the purpose of which is *"to verify subsystem compliance with safety requirements contained in subsystem specifications and other applicable documents; identify previously unidentified hazards associated with the design of subsystems including component failure modes, critical human error inputs, and hazards resulting from functional relationships between components and equipment comprising each subsystem; recommend actions necessary to eliminate identified hazards or control their associated risk to acceptable levels."* (MIL-STD 882C 1993.)

According to MIL-STD 882C, *"the contractor shall perform and document a subsystem hazard analysis to identify all components and equipment that could result in a hazard or whose design does not satisfy contractual safety requirements. This will include government furnished equipment, nondevelopmental items, and software. Areas to consider are performance, performance degradation, functional failures, timing errors, design errors or defects, or inadvertent functioning. The human shall be considered a component within a subsystem, receiving both inputs and initiating outputs, during the conduct of this analysis."*

According to MIL-STD 882C, the contractor has to participate as an active member of the System Safety Working Group (SSWG). Such participation shall include activities specified by the Managing Activity (MA) such as:

- Presenting the contractor safety program status, including the results of design or operational risk assessments;

- Summarising hazard analyses including identification of problems, status of resolution, and residual risk;
- Presenting incident assessment (particularly mishaps and malfunctions of the system occurring) results including recommendations and action taken to prevent recurrences;
- Responding to action items assigned by the chairman of the SSWG;
- Developing and validating system safety requirements and criteria applicable to the program;
- Identifying safety deficiencies of the program and providing recommendations for corrective actions or preventions of reoccurrence;
- Planning and coordinating support for a required certification process; and
- Documenting and distributing meeting agendas and minutes.

2.6 Life cycle of a system

The main stages in the life cycle of a system are concept, definition, development, production and system operation (Stephans 2004). Different analyses methods are performed in certain phases of the life cycle. The first stage in the life cycle is the system concept phase, during which the basis of the system is built by using previously gathered data and studying technical developments (Stephenson 1991). A Preliminary Hazard Analysis (PHA) is performed during the concept stage, in which the attempt is to find the hazards in a certain concept. Also a System Safety Program Plan (SSPP) is carried out, starting from the concept phase until the development stage of the life cycle (Moriarty & Roland 1983). It is important to start the SSPP at the concept phase, in order to make sure that safety issues are examined in a systematic way during the whole process (Stephenson 1991).

The SSPP is continued during the definition stage of the life cycle. The subsystems, assemblies and subassemblies are defined to verify the preliminary design. This is done with the Subsystem Hazard Analysis (SSHA) and later with a System Hazard Analysis (SHA) (Moriarty & Roland 1983). The preliminary design is reviewed during the definition stage, in which the design should fulfil the criteria set for it during the concept phase. As a result of the definition stage, the general design is described for the next phase, which is the development phase (Figure 9).

The third stage is the development of the system, in which the design is approved for production. Operating Hazard Analysis (OHA) examines the human-machine hazards in the system, which will continue to be examined until the production stage (Stephenson

1991). The design is approved for release in the production stage, after which the safety operations are controlled and maintained in the deployment stage. The operations phase identifies new hazards, which is the final stage in the life cycle (Stephans 2004). The hazards in the operations phase are found by inspections and audits. Conducting different analysis methods at certain stages of the life cycle can help to design a safer product, which is safe to maintain and operate.

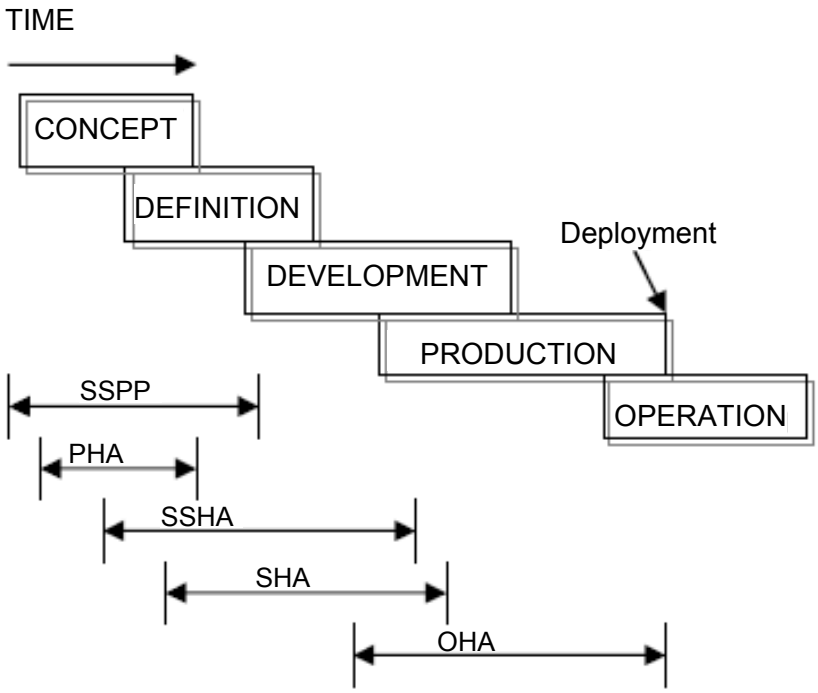

Figure 9. System Safety tasks during the life cycle of a system based on Stephans (2004).

3. System Safety concept for machine systems

The System Safety concept means the effort to make things as safe as possible in the early stages of the system's life cycle by using engineering and management tools (Stephenson 1991). It involves well planned, systematic safety analysis processes.

Safety analysis means the recognition and improvement of dangerous features in a system (Bahr 1997). Hazards in a system should be identified and controlled before losses occur, with different analysis methods, at different stages of its life cycle (Moriarty & Roland 1983).

Safety is often taken into account after an accident occurs and then corrections are performed to prevent similar accidents. This approach is expensive and time consuming, also very inefficient, dangerous and often inhumane. The System Safety method addresses the hazards before losses occur, making the system safe to operate and maintain. Through analysis, design and management actions, the hazards are identified, evaluated, eliminated and controlled in order to make the system safer (Leveson 2005). The main objective of System Safety is to make conditions as safe as possible for the workers and others who are using the system (Moriarty & Roland 1983). Due to the increasing complexity of industrial systems, the System Safety principles are applied by various fields in industry.

3.1 Development work in mining automation sector

The National Institute for Occupational Safety and Health and the Mine Safety and Health Administration have been developing recommendations addressing the functional safety of processor-controlled mining equipment (Figure 10). It is part of a risk-based system safety process encompassing hardware, software, humans, and the operating environment for the equipment's life cycle. Figure 10 shows a safety framework containing these recommendations. A series of reports have been published and some of them are still being worked upon. The idea is to address the various life cycle stages of inception, design, approval and certification, commissioning, operation, maintenance, and decommissioning. The recommendations are intended for use by mining companies, original equipment manufacturers, and aftermarket suppliers to these mining companies. (Sammarco et al. 2001.)

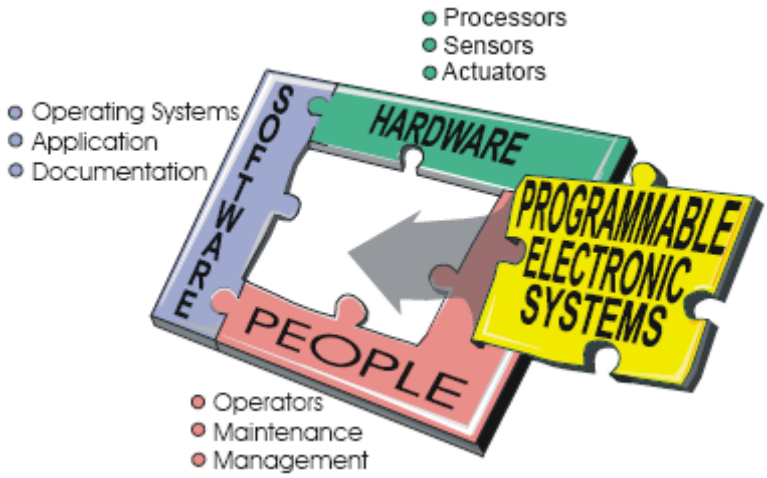

Figure 10. A basic programmable electronic mining system (Sammarco et al. 2001).

• **1.0 Safety Introduction.** – This is an introductory report for the general mining industry. It provides basic system/software safety concepts, discusses the need for mining to address the functional safety of programmable electronics, and includes the benefits of implementing a system/software safety program.

• **2.1 System Safety and 2.2 Software Safety. –** These reports draw heavily from International Electrotechnical Commission (IEC) standard 61508 and other recognised standards. System safety seeks to design safety into all phases of the entire system. Software is a subsystem; thus, software safety is a part of the system's safety.

• **3.0 Safety File. –** This report contains the documentation that demonstrates the level of safety built into the system and identifies limitations for the system's use and operation. In essence, it is a "proof of safety" that the system and its operation meet the appropriate level of safety for the intended application. It starts from the beginning of the design, is maintained during the full life cycle of the system, and provides administrative support for the safety program of the full system.

• **4.0 Safety Assessment.** – The independent assessment of the Safety File is addressed. It establishes consistent methods to determine the completeness and suitability of safety evidence and justifications. This assessment could be done by an independent third party.

• **5.0 Safety Framework Guidance. –** It is intended to supplement the safety framework reports with guidance that provides users with additional information. The purpose is to help users in applying the concepts presented. In other words, the safety framework is what needs to be done and the guidance is how it can be done (Figure 11). The guidance information reinforces the concepts, describes various methodologies that

can be used, and gives examples and references. It also gives information on the benefits and drawbacks of various methodologies. The guidance reports are not intended to promote a single methodology or to be an exhaustive treaty of the subject material. They provide information and references so that the user can more intelligently choose and implement the appropriate methodologies given the user's application and capabilities (Sammarco et al. 2001).

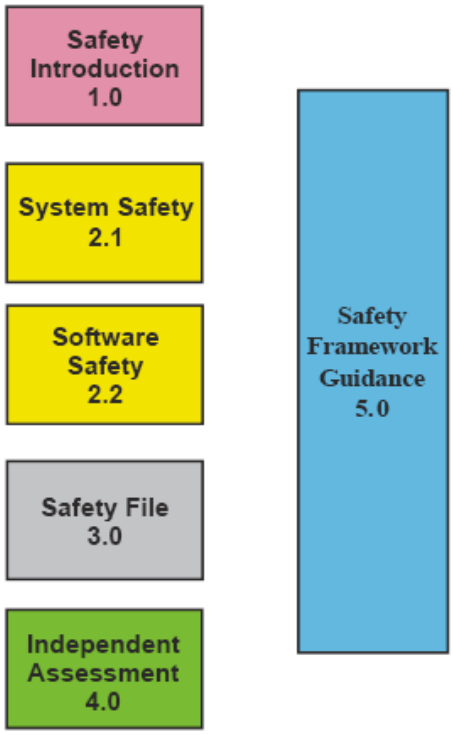

Figure 11. The safety framework and associated guidance (Sammarco et al. 2001).

3.2 Development work at VTT

Methodology for safety design and risk assessment for automatic robot systems has been studied at VTT for several years. The risk assessment approach for single manual mobile machinery has been developed and applied by VTT with mobile machine manufacturers since 1995. The focus in this development has been on stand-alone manual machinery and their remote control (Tiusanen 2000).

Safety engineering standards e.g. ISO 14121 (ISO 14121 1999) and IEC 60300-3-9 (IEC 60300-3-9 2006) provide the basic principles and procedures for the risk assessment of a single machine. They do not, however, supply instructions on how to apply the principles at the machine system level. These standards do not link the risk analysis to the machine or machine system's life cycle stages.

The system safety concept is designed to affect the total life cycle of a product or system. The system safety program's intention is to activate the performance of system safety tasks over the lifetime of the system. The focus in system safety is on hazards from the system's beginning through the evaluation and control of the hazards. System safety principles and concepts have been around since 1960 and beginning with the military and aviation systems (Moriarty & Roland 1983).

A system safety approach for automated mining machine systems has been developed in co-operation with mining machine manufacturer Sandvik Tamrock Corp, mining companies LKAB (Sweden) and DeBeers (South Africa) and their subcontractors. System safety management principles commonly used in the process industry were applied to mobile machine system (Figure 12). The approach includes three different analysis methods that are used at different stages of the system's life cycle. The methods are Potential Hazard Analysis (PHA), Operating Hazard Analysis (OHA) and subsystem Hazard and Operability Analysis (HAZOP) (Tiusanen 2004).

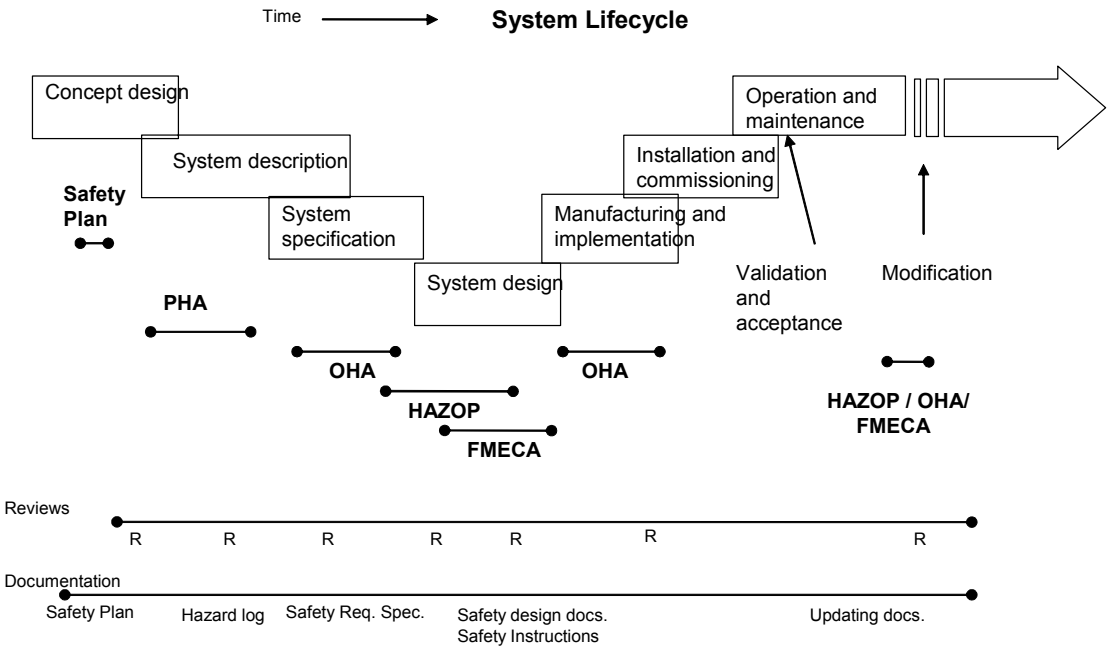

Figure 12. System safety tasks integrated into the system life cycle phases (Tiusanen 2004).

In complex machinery systems, the risk assessment must be performed at several levels to be able to cover the entire machine system. One must consider the use of the machinery, operators' actions, system level control functions and machine level safety issues. The automated machine system must be divided into sub systems such as the local safeguarding system in the production area, machine level systems, factory-wide communication system, the production control system and the remote control stations. This means more co-operation between machine manufactures, their subcontractors and the end users.

This clause describes the procedure and gives instructions and tools for the overall control of safety risks during the life cycle of the machine system beginning from the feasibility studies and ending up at the commissioning of a system. The safety risk management process description consists of safety tasks, information, resources and documents.

3.3 Safety plan

At the beginning of the project it is important that the possible safety implications are raised as soon as possible when discussing the customer needs, production concepts, operating principles and the environment of the application.

The input information for safety planning is e.g.:

- Process Description;
- Other relevant customer documents that are available;
- Information about requirements, hazards and the performance of previous applications;
- Information about the customer's safety policy and targets; and
- Information about safety legislation and approval procedures.

System safety work in a system development project or in a customer project includes management tasks, analysis tasks, review tasks and documentation and file maintenance tasks.

1. System Safety team establishment and team work management
2. Review of project documentation and existing safety data
3. Risk analysis and risk assessment tasks
    - Application level Preliminary Hazard Analysis (PHA)
    - Operation Hazard analysis (OHA)
    - Sub system Hazard and Operability analyses (HAZOP)
4. Safety verification and validation
    - Design and manufacture reviews
    - Installation and commissioning reviews.

3.4 System Safety team management

System safety work is intensive co-operation between all partners. Project management has the overall responsibility for ensuring that system safety work is established, resources are allocated, training is conducted for all personnel associated with the system safety work and safety concerns are identified and communicated.

The roles and responsibilities in safety issues must be defined in the project plan and resources for system safety tasks must be allocated for all partners. At the working level, system safety tasks are normally performed by a system safety working group (Figure 13).

The system safety team is organised and practical things like co-operation principles, meeting and review practices, team members, documentation, reporting, document and file maintenance and distribution, etc., are agreed in a kick-off meeting (Figure 14).

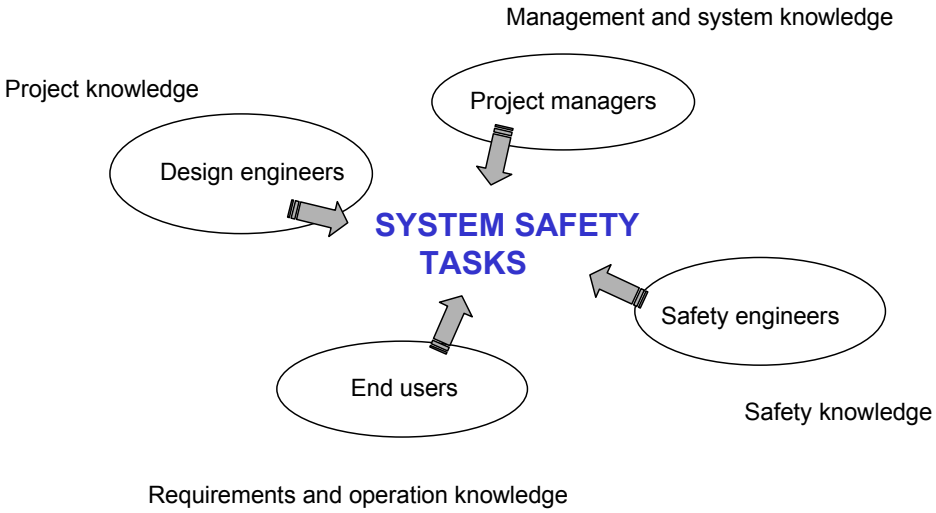

Figure 13. Partners in a system safety team.

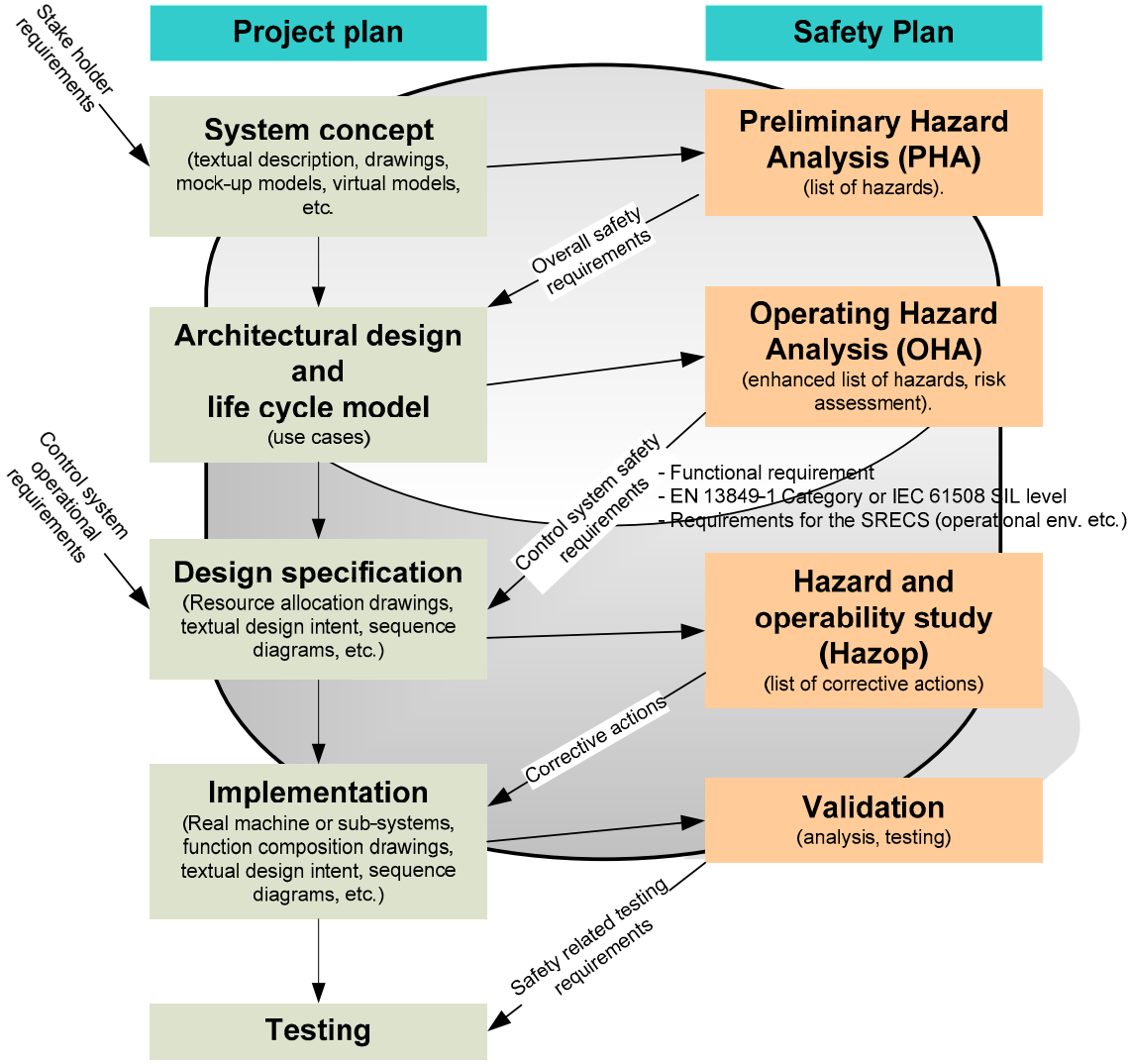

Figure 14. Safety risk management process synchronisation with the development process.

3.4.1 Preliminary Hazard Analysis (PHA)

PHA is used to identify the essential safety risks and potentially hazardous situations related to the use and maintenance of machines or processes. Special attention is paid to the interfaces and application conditions, as well as interactions with other systems and operations effecting the application.

The input information needed for machine system PHA is:

- Process Description;
- System specification;
- Relevant functional specifications and design documents; and
- Previous risk analysis.

Analysis starts with brainstorming sessions and continues for selected life cycle stages and issues. The output of PHA is a preliminary Hazard Log. This log forms the basis for the system level safety documentation.

Typically, VTT prepares the guidelines and material for PHA and sends it to the system safety team for comments. Analyses will be carried out in half or full day meetings. The results of PHA are documented in an application specific Hazard Log. This log forms the basis for the system level safety documentation.

Risk assessment is very important in each step of the risk management process. The severity of consequences and probability of the events related to each hazard is defined and the magnitude of the risk is assessed. At this stage, one should determine and classify the acceptability of the risk associated with each identified hazard, having considered the risk in terms of conflicts with availability and life cycle costs. The risk assessment procedure follows the procedure described in ISO 14121 (1999) and IEC 60300-3-9 (2006). The output of risk assessment is updated Hazard Log.

PHA and risk assessment requires teamwork between all partners.

The Hazard Log should include the following items (EN 50126 1999):

- *Aim and purpose of the Hazard Log;*
- *Each hazardous event and contributing technical and human factor;*
- *Likely consequences and frequencies of sequence of events associated with hazards;*
- *Risk of each hazard;*
- *Risk tolerability criteria for the application;*
- *Measures taken to reduce risks to a tolerable level;*
- *Limits of any analysis carried out;*
- *Any assumptions made during analysis;*
- *Any confidence limits applying to data used within the analysis;*
- *Methods, tools and techniques used;*
- *Personnel and their competencies involved in the process;*
- *Process to review risk tolerability;*
- *Process to review the effectiveness of risk reduction measures;*
- *Process for on-going risk and accident reporting; and*
- *Process for management of the Hazard Log.*

3.4.2 Operating Hazard Analysis (OHA)

One major type of system safety analysis is the operating (and support) hazard analysis.

The purpose of OHA is to perform a detailed safety risk assessment of the system's operational and support procedures. OHA integrates the people and the procedures into the system. OHA can be performed when the operating and support procedures have been defined at such level that they can be analysed as work tasks (Figure 15).

Hazards identified earlier in PHA are updated and supplemented, causes and consequences of possible new hazards are analysed and the possibilities of prevention are assessed. PHA and HAZOP typically focus on technical safety issues.

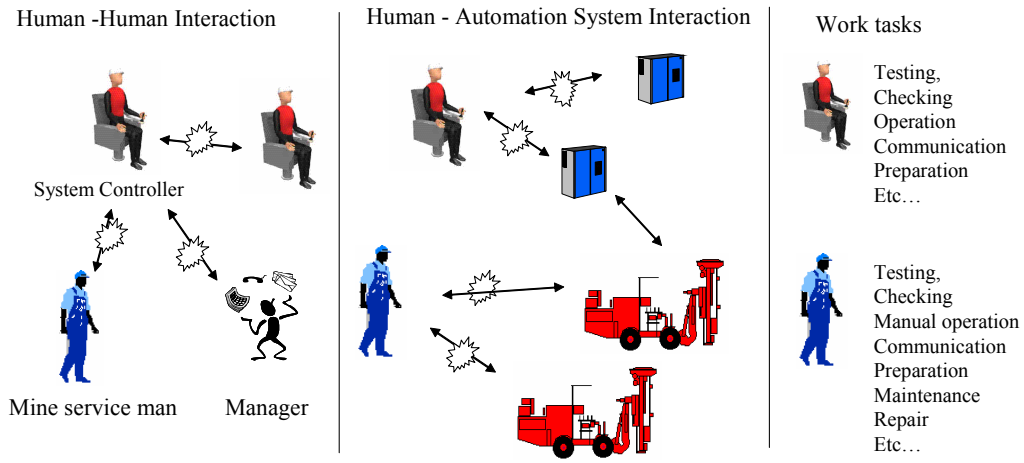

Figure 15. Human–technology interaction. Three perspectives in OHA.

OHA considers human factors and critical human errors, normal and emergency operations and support tasks.

OHA, also called Operating and support hazard analysis (O&SHA), focuses on hazards resulting from tasks, activities, or operating system functions that occur as the system is used. The hazard is not necessary the result of a failure of a component or human operator's error. However, the focus is on the operational event or activity that may be an indirect cause of the mishap. More than likely, the operational event merely allows the subsequent sequence of events to cause the undesired occurrence. The specific goals for OHA were stated as follows (Moriarty & Roland 1983, Stephenson 1991, Stephans 2004):

- Evaluate operating and support procedures for a given system;
- Identify hazards associated with those procedures and assess the safety risks;
- Consider human factors and critical human errors;
- Identify existing controls; and
- Develop alternative controls and/or procedures to eliminate or control the hazards.

The OHA in a mobile machine system can be divided into the following phases: daily routines carried out at the beginning of a work shift, daily work with machinery, and daily maintenance and repair work. All of the main work tasks in production areas and in the control room will be analysed. These tasks include e.g. area preparation, marking and teaching the routes for the automated machines, testing the control functions, operation (manual drive, tele-operation, automated drive), maintenance, troubleshooting, repair, works, etc.

Input information needed for machine system OHA is:

- Operation system concept and preliminary Support concept;
- System Controller's operating tasks, automation-related maintenance tasks; and
- Hazard Log.

Part of the analyses is conducted in traditional project team work meetings. Another way of working is to have a combination of safety expert working in the office and reviewing meetings with the project team.

Typically, VTT prepares the guidelines and material for PHA and sends it to the system safety team for comments. Analyses will be carried out in half or full day meetings. The analysis results are documented in specific analysis worksheets.

The results are presented in an OHA report and the Hazard Log will be updated with these results. OHA also provides input for safety instructions and system safety training materials.

3.4.3 System level Hazard and Operability analysis (HAZOP)

As the project develops and more detailed design data is available, HAZOP studies should be conducted to provide more detailed, in-depth risk assessment information.

The goal of HAZOP is to determine the effects of possible functional and operational deviations and failures to the intended subsystem's operation and functions.

In HAZOP studies, the deviations of the functional quantities are identified systematically, and their consequences are analysed. The analysis technique uses keywords "no, less, more, as well as, other than, part of, reverse". Time dependence is also critical in system level functions, and keywords such as "before, after, early, and late" are used. All existing failure detection and failure protection measures are identified and recorded. HAZOP results are documented in the Hazard Log.

The input information needed for system level HAZOP studies is:

- Operation system concept and preliminary Support concept;
- System Requirement Specification and operating system concept;
- PHA and OHA reports, Hazard Log; and
- Relevant design documents and safety design standards.

The safety-related functions are first specified according to the results of the earlier PHA and OHA. The selected safety-related system functions are then analysed following the Hazard and Operability analysis HAZOP standard IEC 61882 and its application guide (IEC 61882 1999, IEC 61882 2001). In this approach, the safety-related control functions were determined so that they included the operator's actions, control equipment, the communication system between the machine and external IT-systems, and the machine level control system. The analysis of control functions can be carried out at three different levels.

System level functions included e.g. communication control, traffic control, route control, tele-operation, and production area safeguarding.

Machine level functions included e.g. navigation, automatic functions, and condition monitoring.

Signals included e.g. emergency stop, normal stop, driving, steering, braking, mode selection, status, position, ID, monitoring, warning and alarm.

The system level analysis highlights the effects of failures and disturbances to the control functions and machine operation. The hardware installation and connections, as well as procedures for maintenance and modification are analysed to discover possible safety critical failures and deviations at different stages of the system's life cycle. Analysis can reveal new potential hazards that have not been identified earlier in PHA and OHA.

Analysis meetings will be carried out in co-operation with the machine manufacturer's system designers and subcontractors' specialists. After HAZOP studies, the "System level safety requirements" will be specified for the application together with system designers.

Typically, VTT prepares the analysis sessions, leads the analysis sessions and documents the results. Analyses will be carried out in half or full day meetings. The analysis results are documented in specific analysis worksheets and reported in a HAZOP report.

Application specific safety requirements are specified on the basis of the safety analysis and risk assessment taking into account the local safety legislation in force and the customer's safety policy and targets.

Application specific safety requirement specification should include the following items (EN 50126 1999):

- *Occupational health requirements;*
- *Machinery safety requirements;*
- *Environmental safety requirements;*
- *Functional safety requirements for operations and function interfacing application to customers systems;*
- *Safety integrity requirements for each safety-related function; and*
- *External measures necessary to achieve the safety requirements.*

3.5 Design and Implementation

System safety management means a lot of different reviews as part of other project reviews or as separate safety reviews. System safety requirements including safety instructions are verified in design, manufacturing and assembly reviews and during tests.

All possible safety-related modifications and deviations from the requirements are handled and accepted following the safety management procedures.

In the system design and manufacture phase, the preparation of the application specific **Safety Case** can be started. The purpose of the Safety Case is to justify that the design of the application and its realisation, including installation and test phases, meet the system safety requirements and all safety regulations in force.

Safety Case is a set of documents that should include the following (EN 50126 1999):

- *An overview of the application;*
- *Summary or reference to the safety requirements including a consideration of the safety integrity level (SIL) justification for safety functions;*
- *Summary of the quality and safety management controls adopted within the life cycle;*

- *Summary of safety assessment and safety audit tasks;*
- *Summary of safety analysis tasks;*
- *An overview of the safety engineering techniques employed within the system;*
- *Verification of the manufacturing process;*
- *Adequacy of compliance with safety requirements, including any SIL requirements;*
- *Summary of any limitations and constraints applying to the system;*
- *Any special exemptions imposed and justified by the contract;*
- *Any additional information necessary to justify system safety for the application; and*
- *Any limitations or constraints relevant to the application.*

The input information needed for a Safety Case is:

- System safety requirement Specification;
- Hazard Log;
- PHA, OHA and HAZOP reports;
- Relevant safety design documents and standards; and
- Verification and validation reports.

Application Safety Case refers to the "System's Technical Construction File" required in the machine directive (98/37/EC) in Europe.

4. Database tool to support the system safety concept

Safety analysis tools provide the basis for conducting safety analysis efficiently. The problem behind this research was that Safety Analysts were not satisfied with their current analysis tools, which were considered time consuming and inefficient. Safety Analysts often use word processing tools for conducting safety analyses during the life cycle of a system. This proved to be a problem not only for the analysts but also for the customers. It was decided that the problem could be solved by developing a better tool for carrying out safety analyses. Therefore, the goal of the research was to develop a data management tool from the viewpoint of the System Safety concept. It was decided to concentrate on the Hazard and Operability (HAZOP) analysis, since it is a commonly used safety analysis method. This clause is based on the Nina Pátkai's diploma thesis (Pátkai 2006).

During this research, various versions of the database were implemented on the MS Access 2002 platform. After constructing the database according to the requirements, which were collected with the Contextual Design method, and modifying it several times, a fully functional database was completed. The usability tests of the database were carried out according to Nielsen's 10 step usability heuristics. Three evaluators tested the tool, during and after which the results were received verbally by the observer. The database was modified according to the evaluators' comments and again tested with three users once it was finished.

Both customers and safety professionals benefit from the tool by saving time and expenses. The developed data management tool improves analysis data management by enabling Safety Analysts to conduct hazard and operability analyses efficiently and to produce reports rapidly. Data is more structured in the database and the platform opens up new possibilities for additional development.

The presented problem can be solved by developing an improved tool for carrying out safety analysis. Consequently, the goal of this research is to develop a data management tool from the viewpoint of System Safety. The concept of System Safety means the effort to control, analyse and identify hazards by using engineering and management tools (Stephans 2004). Because the System Safety concept is so extensive, it was decided to concentrate on the Hazard and Operability analysis method. Therefore, the aim is to develop a data management tool for conducting HAZOP studies.

Commercial analyses tools are available on the market for performing HAZOP and other System Safety analyses. PHAPro 7 software from Dyadem enables users to perform PHA and HAZOP analyses (PHAPro 7). PHAPro offers a knowledge base,

which makes it possible for the users to utilise previous studies in the analysis and provides access to professional libraries (PHAPro 7). Various knowledge based HAZOP tools have been developed to automate the HAZOP procedure. These tools contain predefined information which can be used during the study (Khan & Abbasi 2000). YetPole developed a computer aided hazard analysis system called CASEHAT in 1993, which was developed for the semiconductor manufacturing industry. The CASEHAT system was developed using Microsoft Access and the Visual Basic programming language (YetPole 2003). Khan and Abbasi developed TOPHAZOP, a knowledgebased software tool, in 1997 (Khan & Abbasi 1997b). They discovered that the amount of time spent in conducting the HAZOP analysis in the traditional way, versus utilising the knowledge-based software, was substantially reduced (Khan & Abbasi 1997b). Another tool, also developed by Khan and Abbasi, called OptHAZOP, utilises an information base (Khan & Abbasi 1997a).

It is valuable to get all of the information needed for a product from the same place. Product Data Management (PDM) systems are relational database systems, which manage attribute and documentary data of the products. In addition to the drawings of parts and assemblies, the database can hold information for instance on the weight and location of the product. Different parts and assemblies are called items in product data management. Similar information can be grouped together in the database, which makes it easier to find necessary information rapidly.

The benefits of a PDM system are that it makes it faster to find data and it updates the versions of the documents, so up-to-date data can be found easily. In an ideal case, the found hazards could be linked together with the customer's product data of the elements, to provide up-to-date information in one location. To do this the HAZOP analysis should be performed systematically. The field descriptions would have to be accurate, in order to be able to link hazards with the existing items.

Numerous tools have been developed for analysing process hazards. However, many of the developed HAZOP tools do not apply to all situations in hand. The reason for this is that the use of HAZOP analysis is popular in various areas, not merely in the process industry. Therefore, a variety of safety analysis tools have been developed for different circumstances. Perhaps this is one of the reasons why so many different types of tools, for conducting Hazard and Operability analysis, have been developed during the last decades. In his journal, McKelvey discussed "How to Improve the Effectiveness of Hazard and Operability Analysis" of the limitations of HAZOP analysis. His opinion was that in order to conduct the HAZOP process successfully, there must be experienced professionals performing the study; it is not enough to have a HAZOP expert system (McKelvey 1988). However, computer-aided HAZOP tools provide assistance for executing analyses.

Several researchers have developed various applications for conducting HAZOP analyses, e.g. knowledge-based tools. Time consumed in a HAZOP analysis can be reduced by the use of computer-aided tools. The development of such a tool requires the experts' knowledge of the safety issues and programming knowledge. However, in the end it pays off by considerably reducing the amount of time spent in analysis sessions. Such a tool would be valuable for the professionals conducting safety analyses in their work and it would also benefit the customers.

The major difference between word processing tools and an MS Access relational database is that information can be easily and quickly retrieved from the MS Access application. Various reports can be easily printed from the database and high risks can be found easily from the reports by the Safety Analysts and customers, who both benefit from the results. One limitation of MS Access is that merely one person can utilise the database at a time. The user interface to HAZOP analysis work sheet is shown in Figure 16.

The developed HAZOP data management tool improves analysis data management when comparing it to traditional word processing tools, e.g. the platform provides possibilities for further development and data is more structured. The benefits of the tool compared to other HAZOP tools are that it is tailored to fit the users' needs and it is cheaper than buying a commercial tool. The limitations of the tool are that e.g. the target group is narrowed down and the tool can only be utilised by one person at a time.

The requirements of the system were gathered by using the Contextual Design method, in which the users were an essential part of the data management tool design. The Contextual Design method proved to be a very good choice in the end, since it gave a good understanding of the users' needs. The usability of the database was tested according to Nielsen's 10 step usability heuristics, after which modifications were made to the database. The usability of the tool increased after the modifications were implemented in the database.

The safety experts can utilise the tool for Hazard and Operability analysis data management. The practical meaning of this work is that the developed data management tool increases the efficiency of conducting HAZOP studies. The tool allows users to search important data from the analysis, in addition to modifying and copying input data.

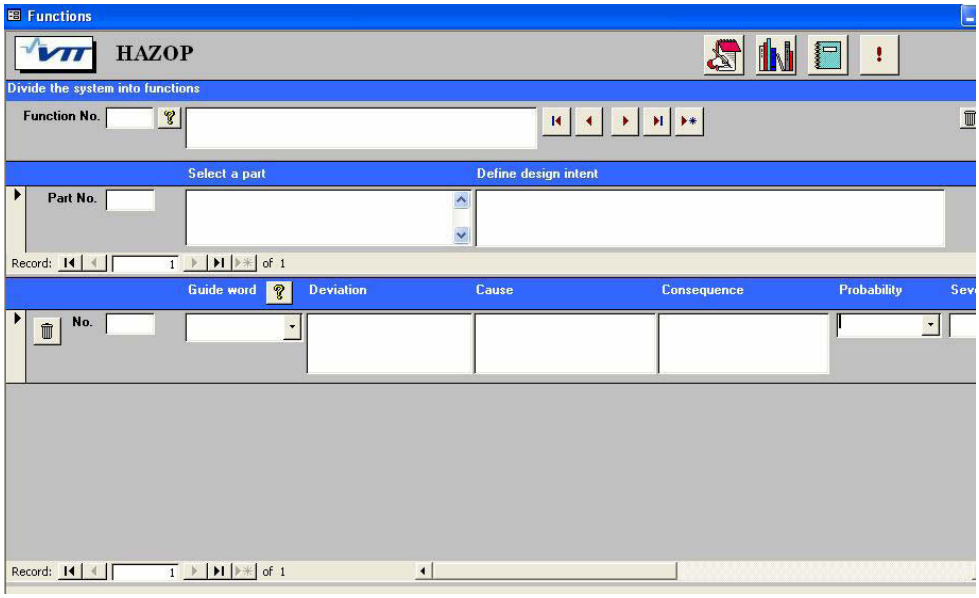

Figure 16. The user interface of the MS Access database tool (Pátkai 2006).

As part of the concept development at VTT, a new function level drawing technique has been developed. So-called resource allocation drawings integrate information from design documents like system (architectural) description, list of control and safety functions, design intent descriptions, module and I/O-lists and communication message specifications. These drawings depict the resources (sensors, actuators controllers, I/O-signals and communication signals) needed to perform the control functions (Figure 17) (Tiusanen 2007).

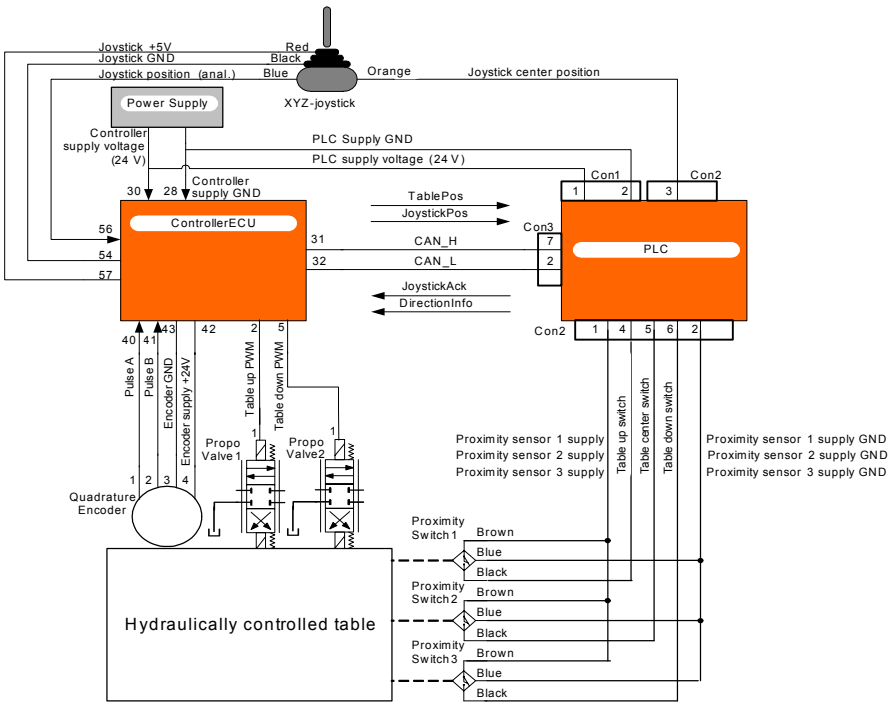

Figure 17. Resource allocation drawing is a partial view of the programmable electrical/electronic control system (Tiusanen 2007).

5. Conclusions

In complex machinery systems, risk analysis must be performed at several levels to be able cover the entire machine system. One must consider the use of the machinery, operators' actions, system level control functions, and machine level safety issues. The automated machine system must be divided into sub systems such as the local safeguarding system in the production area, machine level systems, factory-wide communication system, the production control system and the remote control stations. This means more co-operation between machine manufactures, their subcontractors and the end users.

In large-scale machine automation applications, the safety-related remote control functions are complicated and difficult to analyse. They can be compared with automation systems in the process industries. Safety-related control functions in highly automated machine systems include multi-dimensional aspects such as the operator's actions, user interface communication protocols and machine level control signals. In such a context, safety aspects must be understood to be an important part of systems engineering. The system operation and maintenance work tasks must be specified and designed taking into account the new automation-related hazards and potential safety risks.

The risk analysis of machinery typically results in proposals for technical improvements to the machinery and instructions for use and maintenance. The applied system level approach forced the consideration of new issues related to the work process such as production planning, maintenance planning, and work management. It additionally introduced new safety-related aspects for co-operation inside the company between production and maintenance people and co-operation with machine suppliers and other subcontractors working in the automated production areas, topics that are not normally discussed when the safety analysis is conducted only at the machine level.

When implementing new technology, it is essential that operators and maintenance people understand how the system works, what are the key elements to achieve the required operational efficiency and how safety is build into the system and its operating procedures.

In the future, it seems to be important to be able to identify hazards and assess risks related to the installation, integration and commission phases. Typically, hazards are identified and risks are assessed during the production phase and maintenance situations. In large machinery systems' commissioning phase, all of the safety systems and safety solutions for production are not in use and safety must be ensured using changing temporary arrangements and instructions (Tiusanen 2007).

A new safety engineering approach has been developed. This approach combines the base line hazard identification, task-based hazard identification, system level HAZOP studies and risk assessment principles into a system safety concept. System safety work is becoming a more and more important part of the systems engineering activities in companies developing and manufacturing highly automated machinery systems in global markets.

One of the most important results in system safety teams has been the understanding of subsystem's functionalities and particularly the interaction between subsystems. This is a clear result of the systematic analysis and open communication in the team. Systematic analyses at different levels and at different stages of the project work out well also alongside other important issues that are not related to safety. A systematic approach and the right timing makes it possible to utilise the higher level analysis results as measurable safety requirements, design principles or proposals for solutions to the next project phase. This procedure ensures that specified safety requirements and safety solutions are based on the actual risks in the real operating environment of the machine system.

Practical experience has shown that rough risk estimation with three severity categories and three probability categories is enough for the Preliminary Hazard Analysis at the conceptual design phase. During use case specification phase when conducting Operating Hazard Analysis, a 5 x 5 risk matrix with clearly specified categories is needed to see the real implications of the severity and probability in those specific use case situations.

Comments from our partners encourage us to continue development work on this system safety concept and supporting methods and tools (Tiusanen 2007):

> "Following the system safety concept, the analyses are conducted at the right time. The new machinery system is under definition or the development phase or the customer project is under the specification and design phases".
>
> "The analysis results can directly be taken into use and, if necessary, the specifications and design details can be changed".
>
> "The best way to estimate risks analyse deviations is team work with all of the partners involved in the project. It requires resources, but it is an excellent way of sharing information and solving difficult design problems".

References

98/37/EC. 1998. Machinery Directive. Official Journal of the European Communities L 207/1.

Bahr, J. N. 1997. System Safety Engineering and Risk Assessment: A Practical Approach. New York: Taylor & Francis Group.

EN 50126. 1999. Railway applications. The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS). 76 p.

FAA. 2006. National Airspace System. System Engineering Manual. Federal Aviation Administration, ATO Operations planning. Version 3.1. 6.6.2006. http://www.faa.gov/asd/SystemEngineering/.

IEC 60300-3-9 Ed. 2.0. 2006. Dependability management – Part 3-9: Application guide – Risk analysis of technological systems. Document: 56/1172/CD. 14 December 2006.

IEC 61508-1. 1998. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 1: General requirements.

IEC 61508-2. 2000. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 2: Requirements for electrical/electronic/ programmable electronic safety related systems.

IEC 61508-3. 1998. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 3: Software requirements.

IEC 61882. 1999. Hazard and operability (HAZOP) studies – Guide word approach.

IEC 61882. 2001. Hazard and operability studies. (HAZOP studies) – Application guide. 122 p.

IEC 62061. 2007. Safety of machinery – Functional safety of safety-related electrical, electric and programmable electronic control systems.

INCOSE website. 2008. http://www.incose.org/practice/whatissystemseng.aspx.

ISO 12100-1. 2003. Safety of machinery. Basic Concepts, general principles for design. Part 1: Basic terminology, methodology.

ISO 13849-1. 2006. Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design. 85 p.

ISO 14121. 1999. Safety of machinery – Principles of risk assessment.

Khan, F. I. & Abbasi, S. A. 1997a. OptHAZOP – an effective and optimum approach for HAZOP study. Journal of Loss Prevention in the Process Industries, Vol. 10, No. 3, pp. 191–204.

Khan, F. I. & Abbasi, S. A. 1997b. TOPHAZOP: a knowledge-based software tool for conducting HAZOP in a rapid, efficient yet inexpensive manner. Journal of Loss Prevention in the Process Industries, Vol. 10, No. 5–6, pp. 333–343.

Khan, F. I. & Abbasi, S. A. 2000. Towards automation of HAZOP with a new tool EXPERTOP. Environmental Modelling and Software, Vol. 15, No. 1, pp. 67–77.

Leveson, N. G. 2005. Safety in Integrated Systems Health Engineering and Management. NASA Ames Integrated System Health Engineering and Management Forum, Napa, November 2005. Aeronautics and Astronautics. Engineering Systems MIT.

Liukkonen, R. 2006. Case Patria Vehicles. Tehokkuutta turvallisuus- ja käyttövarmuustiedon hallintaan -seminaari 28.11.2006. Teknologiakeskus Hermia Oy. (In Finnish.)

Malm, T., Kivipuro, M. & Tiusanen, R. 1998. Safety of large automation systems. VTT Research Notes 1938. Espoo: VTT. 72 p. (In Finnish.)
http://www.vtt.fi/inf/pdf/tiedotteet/1998/T1938.pdf.

McKelvey, C. 1988. How to improve the effectiveness of hazard and operability analysis. IEEE Transaction on Reliability, Vol. 37, No. 2, pp. 167–170.

MIL-STD 882C 1993. System Safety Program Requirements. 19 January 1993.

Moriarty, B. & Roland, H. 1983. System Safety engineering and management. New York: John Wiley & Sons. 384 p.

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. 72 p. + app. 6 p.

Sammarco, J. J., Fisher, T. J., Welsh, J. H. & Pazuchanics, M. J. 2001. Programmable Electronic Mining Systems: Best Practice Recommendations (in Nine Parts). NIOSH-Publications, IC 9456. Pittsburgh: National Institute for Occupational Safety and Health.

Stephans, R. A. 2004. System Safety for the 21st Century. New Jersey: John Wiley & Sons, Inc. 385 p.

Stephenson, J. 1991. System Safety 2000: a practical guide for planning, managing, and conducting System Safety programs. New York: John Wiley & Sons, Inc. 336 p.

Suutarinen, J., Kämäräinen, P., Tiusanen, R. & Reunanen, M. 2005. General model to manage safety and reliability information in working machine systems. Helsinki: Teknologiateollisuus ry. ISBN 951-817-890-9. (In Finnish.)

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. Krakow: Jagiellonian University. Pp. 333–336.

Tiusanen, R. 2004. From manual working machines to remotely controlled machinery systems – new challenges for safety risk management. Proceedings of ORP 2004, 3rd International Conference on Occupational Risk Prevention. Santiago de Compostela, Spain, June 2nd to 4th 2004. ISBN 84-933328-2-8.

Tiusanen, R. 2006. Management of safety and reliability through the use of context dependent safety and reliability information. In: Rouhiainen, Veikko (ed.) Safety and reliability. Technology theme – Final report. VTT Publications 592. Espoo: VTT. Pp. 44–52. http://www.vtt.fi/inf/pdf/publications/2006/P592.pdf.

Tiusanen, R. 2007. System Safety Concept for Remotely Controlled Mobile Machine Systems. Proceedings of the 5th International Conference on Safety of Industrial Automated Systems. Academy Common of Meiji University, Tokio.

Ulrich, K. T. & Eppinger, S. D. 2000. Product Design and Development. New York: MacGraw-Hill. ISBN 007-123273-7. 366 p.

YetPole. 2003 Yet-Pole I. Development and applications of CASEHAT – a multipurpose computer aided hazard analysis automation system used in semiconductor manufacturing industry. Journal of Loss Prevention in the Process Industries, Vol. 16, No. 4, pp. 271–279.

Series title, number and
report code of publication

VTT Research Notes 2437
VTT-TIED-2437

Author(s)
Tiusanen, Risto, Hietikko, Marita, Alanen, Jarmo, Pátkai, Nina & Venho, Outi

Title

System Safety Concept for Machinery Systems

Abstract

There are several new trends for moving machines that will affect also on the requirements for the safety and reliability of machines. Working machines will become more and more evidently a part of the production process. When the machines are remotely controlled and the machine control is developing towards machine fleet control and management, the focus on machine safety issues changes to system safety issues and the risk management of the whole operational environment. In future, automated, remote controlled and autonomously moving machines will no longer be stand-alone machines but rather are parts of the automated production systems and when developing those, the whole production process and operation environment have to be considered. There is a need for knowledge about how to specify system safety requirements and system reliability requirements for the unique machine application at different levels. There is also a need for new procedures on how to manage system safety and reliability risks through the whole life cycle of the system.

The scope of this study has been to develop a generic concept and procedure for the safety risk management of automated working machine systems, which tends to take into account interactions between human, technology and environment when specifying safety requirements to the system and designing, implementing and maintaining safety solutions. Special attention has been paid to describing the risk management process, the needed methods and tools and information management.

The developed “System Safety Concept” and safety requirement management is related to Systems engineering and the concept follows the System life cycle model and Risk assessment principles (IEC 60300-3-9, ISO 14121). The control and automation system parts comply with IEC 61508, ISO 13849 and IEC 62061 principles. As a result of this research, a data management tool for conducting HAZOP studies on the MS Access 2002 platform was developed from the viewpoint of the System Safety concept.

ISBN
978-951-38-7214-4 (soft back ed.)
978-951-38-7215-1 (URL: http://www.vtt.fi/publications/index.jsp)

Series title and ISSN	Project number
VTT Tiedotteita – Research Notes 1235-0605 (soft back ed.) 1455-0865 (URL: http://www.vtt.fi/publications/index.jsp)	774

Date	Language	Pages
June 2008	English, Finnish extended abstr.	53 p.

Name of project	Commissioned by
From Machines to systems – New challenges for risk management. Case – safety risk management in an automatic container crane system	Finnish Work Environment Fund, Kalmar Industries, VTT Technical Research Centre of Finland

Keywords	Publisher
system safety, risk management, machinery systems, working machine, HAZOP	VTT Technical Research Centre of Finland P.O. Box 1000, FI-02044 VTT, Finland Phone internat. +358 20 722 4520 Fax +358 20 722 4374

Automated, remote controlled and autonomously moving machines are no longer stand-alone machines but rather are parts of the automated production systems. When the machines are remotely controlled and the machine control is developing towards machine fleet control and management, the focus on machine safety issues changes to system safety issues and the risk management of the whole operation environment.

This publication deals with the concept and procedure for the safety risk management of automated working machine systems, which tends to take into account interactions between human, technology and environment when specifying safety requirements to the system and designing, implementing and maintaining safety solutions. Special attention has been paid to describing the risk management process, the needed methods and tools and information management. A data management tool for conducting Hazard and Operability study (HAZOP) was developed and tested within this study.

Julkaisu on saatavana
VTT
PL 1000
02044 VTT
Puh. 020 722 4520
http://www.vtt.fi

Publikationen distribueras av
VTT
PB 1000
02044 VTT
Tel. 020 722 4520
http://www.vtt.fi

This publication is available from
VTT
P.O. Box 1000
FI-02044 VTT, Finland
Phone internat. + 358 20 722 4520
http://www.vtt.fi

ISBN 978-951-38-7214-4 (soft back ed.)
ISSN 1235-0605 (soft back ed.)

ISBN 978-951-38-7215-1 (URL: http://www.vtt.fi/publications/index.jsp)
ISSN 1455-0865 (URL: http://www.vtt.fi/publications/index.jsp)