Comparing best practices of safety related control system development - CompSoft

VTT Technical Research Centre of Finland

TECHNOLOGY FOR BUSINESS

Introduction / background

It has been detected that 40 % of faults contributing to programmable electronic systems related incidents emerge during the safety requirements specification phase of a system life cycle. Early life cycle phases of programmable electronic systems are sensitive to defects. One third of software related defects are made in the requirements specification phase. Therefore it is important to focus on the early life cycle phases of systems: safety requirements specification and risk assessment.

When analysts make risk assessment they typically get different results depending on the background of analysts. Risk assessment should result in specific PL or SIL demands in order to set requirements for control systems. Too strict requirements lead to expensive systems and too low requirements lead to unsafe systems.

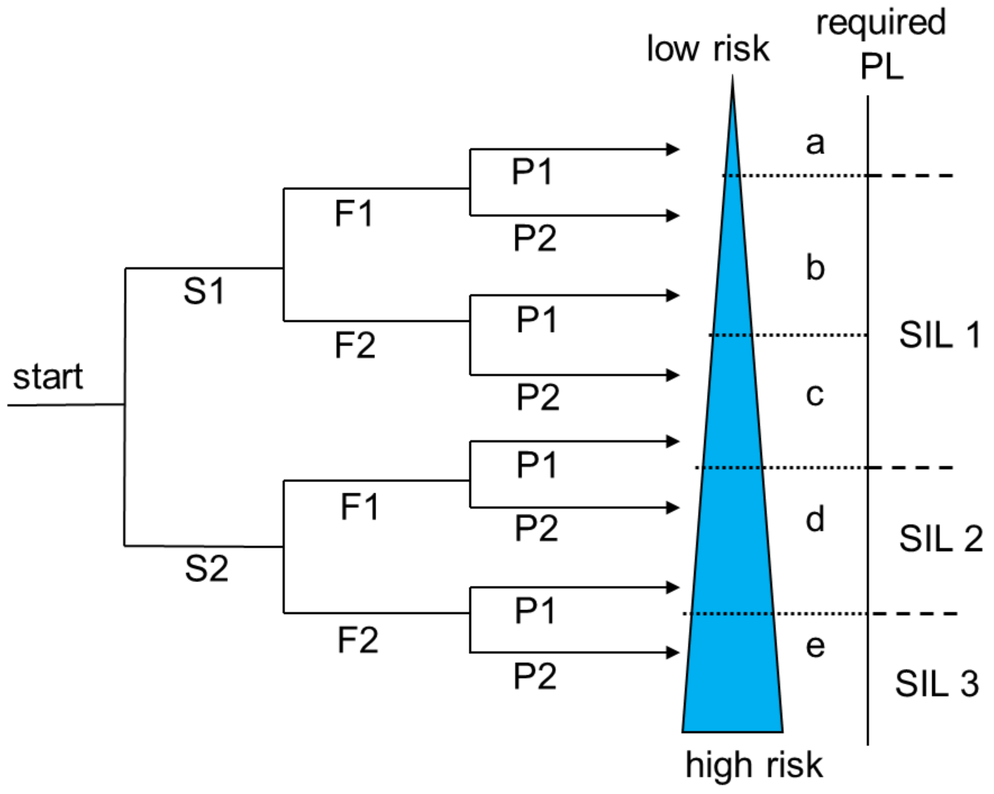

Figure 1. Risk graph of ISO 13849-1.

Objectives

The objective of the project is to develop risk assessment and safety requirements specification phases of safety related control system design by combining well-tried methods, techniques and principles. The aim is to apply methods with good reputation, select a set of best methods and techniques and find ideas to improve or integrate them to support better each other. The impact of the comparative approach of the study is intended to affect performance and safety culture in organisations.

Each participating institute and enterprise will execute a round robin test according to a pre-determined plan. Round robin test is a test including measurement, analysis or conceptual assessment which is evaluated by multiple independent experts applying same methods for the case systems (or products) to compare the methods and the variance of the results (cp. analysis of variance). The objective for the round robin test is

- to find the best practices for safety requirements specification and risk assessment
- to find the criteria for the selection of methods and techniques
- to find the strengths and weaknesses of methods used in the early safety life cycle phases of control system design using a comparative approach
- to find uniform principles, practices and methods used in different institutes.

Tasks

The results from interviews, workshops and round robin test are compared to find most objective (less variation in results), effective (less work done) and feasible methods. The combination of the best features of examined methods is studied to create a demonstration tool for the process from risk assessment to safety requirements. The strategy is to arrange interviews and workshops to select methods for examination and apply round robin test and case studies to assess these methods. The selection criteria for methods, techniques and principles are made to support oil, machine, paper and steel industries and SMEs that design safety related control systems.

Results

The results are disseminated as a form of workshops, open seminars, a report including guidelines and an article. The utilization of results is expected to decrease the number of incidents that may occur due to weaknesses in risk assessment and safety requirements specification phases of safety related control system design process. The results will assist to develop new or improved practices for safety management, and affect the safety culture on design activities for new products and facilities.

Contacts

Marita Hietikko
Tel. +358 20 722 3222
marita.hietikko@vtt.fi

Timo Malm
Tel. +358 20 722 3224
timo.malm@vtt.fi

TECHNOLOGY FOR BUSINESS

Invitation to participate in CompSoft project

where risk assessment and safety requirements specification of safety related control systems are studied

VTT Technical Research Centre of Finland

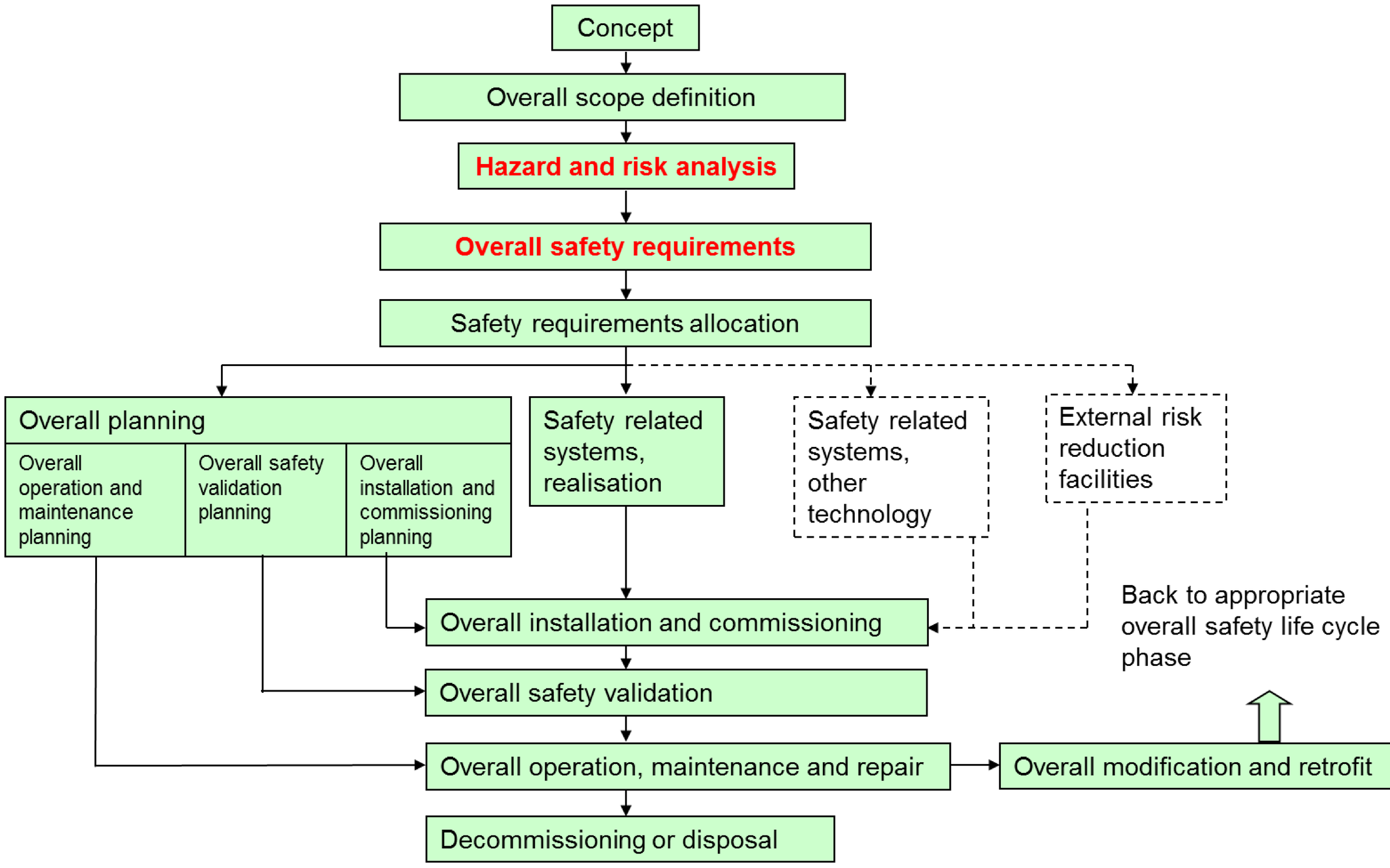

Figure 2. Overall life cycle model of IEC 61508. The project focuses on the red coloured phases of system life cycle.

Cooperation

The research will be carried out in cooperation with NTNU (Norway), SP (Sweden), SINTEF (Norway) and VTT (Finland). The project is financed by the Finnish Work Environment Fund, participating research organisations and enterprises.

How enterprises can participate in the project

- Experts of enterprises will be interviewed and therefore time for these interviews is expected. In this context design engineers' experiences, current practices relating to risk assessment and safety requirements specification of systems and objects for development are discussed.
- The experts and designers of enterprises have possibility to participate in the round robin test, workshops and seminars.
- Enterprises are expected to give financial support for the study.

Time Table

The project started on April 2014 and it will end on December 2015.

Exploitation

- Enterprises can point out challenges relating to their system design.
- A specific topic can be discussed and assessed in the round robin test.
- A special case study can be performed.
- The Excel based risk assessment demonstration tool will have properties stated by enterprises. As a result of the project enterprises will get the demonstration tool and project reports.
- Workshops and seminars will be held for enterprises and their interest groups. Final goal is that the enterprises will gain improvements for their risk assessment and safety requirement specification process.

Contacts

Marita Hietikko
Tel. +358 20 722 3222
marita.hietikko@vtt.fi

Timo Malm
Tel. +358 20 722 3224
timo.malm@vtt.fi