NTNU – Trondheim
Norwegian University of
Science and Technology

Safety of machinery

Integrity assessment of safety-related
control systems

Peter Joos Louwe
Kooijmans

Reliability, Availability, Maintainability and Safety (RAMS)
Submission date: June 2015
Supervisor: Anne Barros, IPK
Co-supervisor: Marvin Rausand, IPK

Norwegian University of Science and Technology
Department of Production and Quality Engineering

RAMS
Reliability, Availability,
Maintainability, and Safety

Safety of machinery: Integrity assessment of safety-related control systems

P.J. Louwe Kooijmans

June 2015

MASTER THESIS

Department of Production and Quality Engineering

Norwegian University of Science and Technology

Supervisor 1: Professor Anne Barros

Supervisor 2: Professor Marvin Rausand

Preface

This report is the final product of my master's thesis in RAMS-engineering at the NTNU. The thesis-project started January 2015 and was finalised June 2015.

The thesis-project started as a collaborative project between a private owned Norwegian company and me. Due to organisational and communication issues, I decided to discontinue the collaboration. This decision was made after consulting my supervisor, professor Marvin Rausand. This meant I was forced to re-define my scope of work midway my thesis period. As a result, this report presents a more theoretical contemplation of the topic than initially planned for.

The report is written for readers that have interest in how European legislation regarding essential healthy and safety requirements is structured and how a manufacturer of machinery can meet these requirements. Special attention is given to safety integrity requirements for control systems, how these requirements can be systematically used in the design process for machines, and how integrity of the control system can be assessed. This approach towards safety integrity for control systems might be of special interest for readers that are known with general concepts of safety integrity presented in standards such as the IEC61508, but are new to machinery sector's specific standards.

It is assumed that the reader is known with the standard IEC61508, and has background knowledge of reliability theory equivalent to that presented by Rausand and Høyland (2004).

Trondheim, 26-6-2015

Peter Joos Louwe Kooijmans

Acknowledgment

First of all I would like to thank professor Marvin Rausand for his guidance during the first stages of my thesis project. He helped me to define my research topic and guided me through European legislation and standards. I also would like to thank professor Anne Barros for her supervision. Her consultation was of great help when I needed to redefine my scope.

Last but not least I would like to thank my fellow students of the RAMS program. They were always willing to help me during my thesis period, and made my time at the NTNU an enjoyable experience.

P. J. Louwe Kooijmans

Summary and Conclusions

This project had two phases. The first phase was of an exploring nature and had as main objectives to (1) give an introduction to the machinery directive, its structure, and main safety requirements with special focus on requirements regarding safety-related control systems, to (2) give an introduction to functional safety, to (3) present the two competing standards IEC 62061 and ISO 13849, highlighting their similarities and differences, and to (4) present current issues within the design of reliable and safe control system for machinery. The second phase focused on current issues within the design of reliable and safe control systems for machinery. It had as main objectives to (1) give an in-depth analysis of the issue regarding safety-functions that operate in continuous mode and to (2) present concepts and solutions that might be used to resolve the issues regarding safety-functions that operate in continuous mode.

Phase one

The Machinery Directive 2006/42/EC is European legislation that promotes free movement of machinery within the EU and guarantees a high level of protection of the EU workers and citizens. It does this by dictating essential health and safety requirements relating to the design and construction of machinery. It is the manufacturer's responsibility to assess if the machinery meets the requirements from the Machinery Directive. Guidance on how to meet the requirements from the Machinery Directive is provided by harmonized standards. During the project, the standards have been analysed. It is concluded that at the core of achieving safety of machinery lies a risk based approach. This risk based approach is described in the standard ISO 12100:2010; *"Safety of machinery - General principles for design - Risk assessment and risk reduction"*. It specifies principles of risk assessment and risk reduction. The part of machine safety which depends on the correct functioning of active control and safety systems is called functional safety. Control systems that contribute to functional safety are in general referred to as safety-related control systems. These systems provide the required risk reduction and are an integral subset of the machine. The Machinery Directive imposes requirements regarding the safety and reliability of control systems. ISO 13849-1: *"Safety of machinery - Safety-related parts of control systems"* and IEC 62061: *"Safety of machinery- Functional safety of safety-related*

electrical, electronic and programmable electronic control systems", specify requirements for the design and implementation of safety-related control systems. ISO 13849-1 introduces the concept of Performance levels (PL) and the IEC 62061 adopts the concept of Safety Integrity Levels (SIL). Both concepts are studied and it shows that both concepts use methods and tools to establish the risk that needs to be reduced, and give guidance and requirements on designing systems that shall reduce the risk. Some oddities within the standards are researched and explored. It is concluded that, although the standards might show guidance, the designer of the control system needs to assess whether they are applicable on the system at hand. Throughout the first phase of the project it became clear that in both standards the phenomenon of basic control systems that conduct safety-related control functions that operate in continuous mode (SRCF$_{\text{cont.}}$) is underexposed. SRCF$_{\text{cont.}}$ means that the function is continuously controlling the machinery. Their failure results in a hazardous event that may lead to harm.

Phase two

To reduce risk of a certain hazardous event, it is common practice to add safety barriers (safety functions) to machinery. Throughout the second phase of the project it became apparent that incremental adding of safety barriers as promoted in the ISO 12100, ISO 13849-1 and IEC 62061, leads to inaccurate safety integrity assessments of safety barrier sequences that consist out of at least one SRCF$_{\text{cont.}}$. This may lead to inaccurate reliability requirements for barriers during the design of such barrier sequences.

To develop a method that results in a more accurate safety integrity assessment of such systems, this thesis proposes an integral approach. Instead of assessing the safety integrity of each individual safety barrier in the sequence, the safety integrity of the full barrier sequence is assessed. The approach is based on modelling the full barrier sequence and establishing the value of the risk metric "Hazardous event frequency" (HEF). Once the HEF is found, this can be evaluated if this HEF is deemed to be acceptable or not.

During the project a model of such a system is constructed. It does not yet include common cause failures nor is it checked. The model is therefore not completed nor validated. Still, initial simulation shows plausible results and it is a promising start for further research into completing the integral method.

Contents

Chapter 1

Introduction

When designing a system, it is important that it fulfils all requirements from relevant laws and regulations. These requirements are mainly related to health and safety aspects of the system. The basic safety requirements for systems that are placed on the EU market are described in the EU Directives. An EU Directive is legislation that is binding for the member states of the EU.

The Machinery Directive 2006/42/EC applies to new machinery products that are placed on the EU market. This directive has as objectives to promote free movement of machinery within the EU and guarantee a high level of protection of the EU workers and citizens.

Product safety requirements, in the directives, do not only apply to the final product. They are related to the whole life cycle of the product, from early conception until disposal. It is the manufacturer's responsibility to document the activities taken to ensure that the safety is adequate and show that his product meets all relevant requirements. Detailed risk analyses of the product in the various life phases are sometimes required, and the risk analysis reports may have to be part of the product documentation. To help manufactures comply with these requirements, a comprehensive framework of harmonised standards is available.

As a result of automation, demand for increased production and reduced operator physical effort, safety-related control systems of machines play an increasing role in the achievement of overall machine safety by reducing the risk of hazardous events. The machinery directive imposes general requirements regarding the safety and reliability of control systems. In line with these general requirements, both the standards ISO 13849-1 and IEC 62061 specify requirements for the design and implementation of safety-related control systems. The methods developed in both of these standard differ, but when correctly applied, can achieve a comparable level of risk reduction. Both standards adopt the strategy for risk reduction presented in ISO 12100. A guideline for how to conduct a risk assessment is presented in the technical report ISO/TR 14121-2.

Meeting the safety requirements regarding the control system by applying one of the competing standards, ISO 13849-1 or IEC 62061, will present some challenges for manufactures of machinery. These challenges lay in conducting a fitting risk assessment to determine the appropriate risk reduction a control system needs to deliver, and a correct interpretation of the architectural and reliability requirements stated in the standards. This requires a good understanding of the machinery under control, knowledge of the hazardous events that may occur, possible safety functions that may be applied, architectural constrains, reliability calculations and how to interpret component reliability data.

A fair amount of literature and guidelines is available that offer tools and methods to design control systems that meet the safety requirements. The European Union has published a guideline on how The Machinery Directive 2006/42/EC should be interpreted and what specific standards can be applied to meet the basic safety requirements. This guideline is available on the website of the European Union `http://ec.europa.eu`. Technical report ISO/TR 18569; *"Safety of Machinery - Guidelines for the understanding and use of safety of machinery standards"*, shows how harmonised standards that are part of the supporting standard framework can be applied. Authors such as Rausand (2011) present methods and guidance on how to conduct risk assessments that are in-line with the ISO12100. Specific literature on functional safety show how from a risk assessment the required integrity/performance of a control system can be established. Examples are Rausand (2014) and Rockwell (2011). Besides this, the IEC has published the technical report IEC/TR 62061-1:*"Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery"*, that gives a short introduction and brief comparison of the competing standards.

1.1 Objectives

To demonstrate the challenges a manufacturer might meet during the design of a machine, the project is divided into two parts. The first part of the report is of an exploring nature. Its main goal is to show the relation between the applicable legislation, requirements and standards. It introduces the concept of functional safety and a general description of modern control systems. It highlights current issues within the field of safety integrity of control systems. The second part will elaborate on the described issues and suggest how these issues might be resolved.

Part one

The objectives of part one are to:

1. Give an introduction to the machinery directive, its structure, and main safety requirements. Special focus shall be given to requirements to safety-related control systems.
2. Give an introduction to functional safety.
3. Present the two competing standards IEC 62061 and ISO 13849 and highlight similarities and differences between these two standards.
4. Present current issues within the design of reliable and safe control systems for machinery.

Part two

With the objectives of the first part met, the second part of the project has the objectives to:

1. Give an in-depth analysis of the issue regarding safety-functions that operate in continues mode.
2. Present concepts and solutions that might be used to resolve the issue regarding safety-functions that operate in continues mode.

1.2 Limitations

- When referring to the requirements that originate from european legislation, only those from the Machinery Directive 2006/42/EC are listed. It might well be that other requirements from other EU directives apply to control systems of machinery as well.

- Description and explanation of methods, concepts and procedures that are given in standards, is limited. When possible, reference to specific chapter, clauses and appendices to standards are made. If the author believes there are points of interest within the standards, these will be discussed.

- As it is assumed that the reader is familiar with the IEC 61508, the report will not explain the methods and concepts that are described in this standard in detail. When possible, the differences between the machinery sector specific standards and the IEC 61508 are highlighted.

- Examples of systems used in the report are based on generic equipment. The data in this report are taken from accredited databases.

- When failure rates are used, they are assumed to be constant. If otherwise, the failure distribution is given

- When calculating the reliability of systems that are presented in examples, only the failure probability contribution from random hardware failure is considered. The contribution of systematic failures, human factors and alternative testing mechanisms are not considered.

- When calculating the reliability of systems that are presented in examples, the β-factor model for contribution of common cause failure is adopted.

1.3 Approach

The thesis project is structured and conducted by the following activities:

1. Literature research: To understand the machinery directive, its structure and main requirements, a literature research into legislation is conducted. This research is the basis for further understanding of the framework of standards that support the directive. More literature is read and analyzed on the topics;

    - standards ISO 13849-1 and IEC 62061,
    - system analysis,
    - modern control systems,
    - risk assessment,
    - and functional safety.

2. Familiarisation with current issues in the field of safety integrity of control systems: With the knowledge gained from the literature research, problem areas are explored. Fitting examples and cases are described that highlight the problems at hand.

1.4 Structure of the Report

The rest of the report is organised as follows. Part one of the report starts at chapter two. Chapter two introduces the machinery directive, its structure and the main safety requirements. It describes the relation between the directive and the supporting harmonised standards, the requirements for the technical file and the CE-marking. It ends with illustrating the process of compliance.

Chapter three elaborates on the harmonised standards. It explains how they are organised and shows how systematic risk reduction is established by applying the processes described in the harmonised standards.

With the introduction to relevant legislation and standards in place, chapter four focuses on specific requirements regarding the control system. It introduces the term functional safety and relevant concepts. Standards ISO 13849-1 and IEC 62061 are discussed and compared.

Part two of the report starts of with a short conclusion of part one, highlighting the problem areas and issues regarding assessing the safety integrity of control systems within the machinery sector. Chapter five expands on the issue of safety-related control functions that operate in continuous mode. It shows the problem at hand by giving examples of problems that may arise when designing such control functions.

Based on the problems described in chapter five, chapter six introduces a solution to the problem that is sketched in chapter five. It gives a modelling solution.

Chapter seven presents the results, recommendation, the conclusion and recommendation for further work.

Part I

The Machinery Directive & safety and reliability of control systems.

Chapter 2

Legislation and Requirements

The Machinery Directive 2006/42/EC promotes free movement of machinery within the EU and guarantees a high level of protection of the EU workers and citizens. Free movement of machinery that complies with the Machinery Directive is guaranteed by article 6 of the directive. This article forbids member states to prohibit, restrict or impede the placing of machinery that comply with the directive on their markets. The high level of protection of the EU workers and citizens is ensured by the dictated essential health and safety requirements relating to the design and construction of machinery. Which products are considered as machinery and are part of the Machinery Directive's scope, is described in Article 1 of the directive. All these products need to meet the essential health and safety requirements relating to the design and construction of machinery that are listed in Annex I of the Machinery Directive. The requirements are listed as followed;

1. General remarks,
2. control systems,
3. protection against mechanical hazards,
4. required characteristics of guards and protective devices,
5. risk due other hazards,
6. maintenance,

7. information.

Some supplementary requirements are listed for specific product groups such as foodstuffs machinery and machinery for cosmetics or pharmaceutical products.

2.1 Compliance

It is the manufacturer's responsibility to assess if the machinery meets the requirements from the Machinery Directive. Guidance on how to meet the requirements from the Machinery Directive is provided by harmonized standards. Machinery manufactured in conformity with a harmonised standard, shall be presumed to comply with the essential health and safety requirements covered by such a harmonised standard.

The procedure for assessment of conformity varies with product categories. For non-dangerous machines the conformity assessment is done with internal checks. The general requirements for this assessment are described in Annex VIII of the Machinery Directive. These are;

1. For each type of the series of machinery, the manufacturer shall draw up a technical file,

2. The manufacturer must take all measures necessary in order that the manufacturing process ensures compliance of the manufactured machinery with the technical file and with the requirements of this Directive.

Dangerous machines

The Machinery Directive lists dangerous machines in Annex IV. For these machines a different conformity procedure is required. Within these procedures an important task lies with Notified Bodies. These are bodies notified by EU member states and carry out the assessment of conformity of dangerous machines. This is done by conducting the EC type-examination procedure, as described in Annex IX of the Machinery Directive, or indirectly by a full quality assurance procedure that is certified by a notified body. This procedure is described in Annex X of the directive.

Where the machinery is listed and manufactured in accordance with the harmonised standards, and provided that those standard cover all of the relevant essential health and safety requirements, the manufacturer shall apply one of the following procedures:

1. the procedure for assessment of conformity with internal checks on the manufacture of machinery, provided for in Annex VIII;
2. the EC type-examination procedure provided for in Annex IX, plus the internal checks on the manufacture of machinery provided for in Annex VIII;
3. the full quality assurance procedure provided for in Annex X. This Annex describes the conformity assessment of machinery referred to in Annex IV, manufactured using a full quality assurance system, and the procedure whereby a notified body assesses and approves the quality system and monitors its application.

Where the machinery is referred to in Annex IV and has **not** been manufactured in accordance with the harmonised standards, or only partly in accordance with such standards, or if the harmonised standards do not cover all the relevant essential health and safety requirements or if no harmonised standards exist for the machinery in question, the manufacturer shall apply one of the following procedures:

1. the EC type-examination procedure provided for in Annex IX, plus the internal checks on the manufacture of machinery provided for in Annex VIII, point 3;
2. the full quality assurance procedure provided for in Annex X.

Partly Completed Machinery

In case of partly completed machinery, the manufacturer of partly completed machinery shall ensure that:

- the relevant technical documentation is prepared;
- assembly instructions are prepared;
- a declaration of incorporation shall been drawn up.

The assembly instructions and the declaration of incorporation shall accompany the partly completed machinery until it is incorporated into the final machinery and shall then form part of the technical file for that machinery.

2.2 Technical file

To demonstrate that the machinery complies with the requirements the manufacturer shall compile a technical file.

1. A technical file shall comprise:

    - a construction file including:

        - a general description of the machinery,
        - the overall drawing of the machinery and drawings of the control circuits, as well as the pertinent descriptions and explanations necessary for understanding the operation of the machinery,
        - full detailed drawings, accompanied by any calculation notes, test results, certificates, etc., required to check the conformity of the machinery with the essential health and safety requirements,
        - the documentation on risk assessment demonstrating the procedure followed,
        - the standards and other technical specifications used, indicating the essential health and safety requirements covered by these standards,
        - any technical report giving the results of the tests carried out either by the manufacturer or by a body chosen by the manufacturer or his authorized representative,
        - a copy of the instructions for the machinery,
        - where appropriate, the declaration of incorporation for included partly completed machinery and the relevant assembly instructions for such machinery,
        - where appropriate, copies of the EC declaration of conformity of machinery or other products incorporated into the machinery,

    - a copy of the EC declaration of conformity;

  - The manufacturer must carry out necessary research and tests on components, fittings or the completed machinery to determine whether by its design or construction it is capable of being assembled and put into service safely. The relevant reports and results shall be included in the technical file.

2. The technical file referred to in point 1 must be made available to the competent authorities of the Member States for at least 10 years following the date of manufacture of the machinery or, in the case of series manufacture, of the last unit produced.

   The technical file does not have to be located in the territory of the Community, nor does it have to be permanently available in material form. However, it must be capable of being assembled and made available within a period of time commensurate with its complexity by the person designated in the EC declaration of conformity.

   The technical file does not have to include detailed plans or any other specific information as regards the subassemblies used for the manufacture of the machinery unless a knowledge of them is essential for verification of conformity with the essential health and safety requirements.

For partly completed machinery, documentation must show which requirements of this Directive are applied and fulfilled. It must cover the design, manufacture and operation of the partly completed machinery to the extent necessary for the assessment of conformity with the essential health and safety requirements applied. The documentation shall comprise out of:

- a construction file including:
  - the overall drawing of the partly completed machinery and drawings of the control circuits,
  - full detailed drawings, accompanied by any calculation notes, test results, certificates, etc., required to check the conformity of the partly completed machinery with the applied essential health and safety requirements,
  - the risk assessment documentation showing the procedure followed, including:

  - a list of the essential health and safety requirements applied and fulfilled,
  - the description of the protective measures implemented to eliminate identified hazards or to reduce risks and, where appropriate, the indication of the residual risks,
  - the standards and other technical specifications used, indicating the essential health and safety requirements covered by these standards,
  - any technical report giving the results of the tests carried out either by the manufacturer or by a body chosen by the manufacturer or his authorised representative,
  - a copy of the assembly instructions for the partly completed machinery;

- a copy of a Declaration of Incorporation of Partly Completed Machinery.

2.2.1 Manual

All machinery must be accompanied by instructions in the official Community language or languages of the Member State in which it is placed on the market and/or put into service. Section 1.7.4 of Annex I describes the requirements the instructions should meet. An important subsection is 1.7.4.2. This subsections dictates what should be included in the instructions.

2.2.2 Risk reports

To demonstrate that a risk assessment is conducted, a risk report shall be compiled. When conducting a risk assessment conform the ISO 12100. Guidance on how to conduct a risk assessment and structure the documentations is described in ISO/TR 14121-2.

2.2.3 Declarations

The manufacturer must draw up and sign an EU Declaration of Conformity (DOC) as part of all the conformity assessment procedure provided by the Machinery Directive.The EU DOC is the document that states that that the product satisfies the essential requirements of the applicable legislation. By drawing up and signing the DOC, the manufacturer assumes responsibility for the compliance of the product. Just as it is the case for the technical documentation, the EU Declaration of Conformity must be kept for ten years from the date of placing the product on the market. This is the responsibility of the manufacturer or the authorised representative established within the EU. What the DOC needs to contain is described in Annex II of the Directive. A copy of the DOC has to be included into the instruction manual of the machinery. An example of a DOC is shown in Figure 2.2. The manufacturer of machinery or his authorised representative is obligated to keep the original DOC for a period of at least 10 years from the last date of manufacture of the machinery.

Declaration of Incorporation of Partly Completed Machinery

In case of partly completed machinery, defined as an assembly which is almost machinery but which cannot in itself perform a specific application, not a DOC has to be drafted but a Declaration of Incorporation of Partly Completed Machinery. What the Declaration of Incorporation of Partly Completed Machinery needs to contain is shown in Annex II of the Directive. An example of a DOC is shown in Figure 2.3

2.3 CE Marking

The CE mark, shown in figure2.1, is a mandatory safety mark on many product that are placed on the market in the European Economic Area (EEA). This mark is a sign of conformity with product safety requirements set out in the EU Machinery Directives. To permit the use of a CE mark on a product, proof that the item meets the relevant requirements must be documented. By affixing the CE marking on a product, a manufacturer is declaring, on his sole responsibility (and irrespectively of whether a third-party has been involved in the conformity assessment process), conformity with all of the legal requirements to achieve CE marking.

2.4 Process

The process of complying with the Machinery Directive is shown in the flowchart presented in Figure 2.4. The figure shows two different paths. One path for Machinery and one path for partly completed machinery, defined as an assembly which is almost machinery but which cannot in itself perform a specific application.

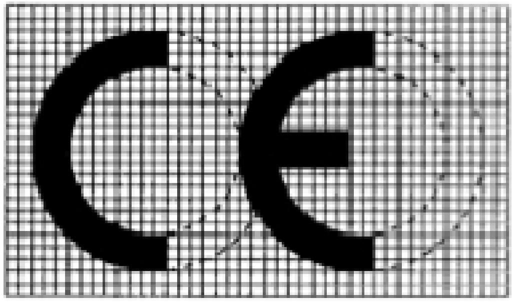
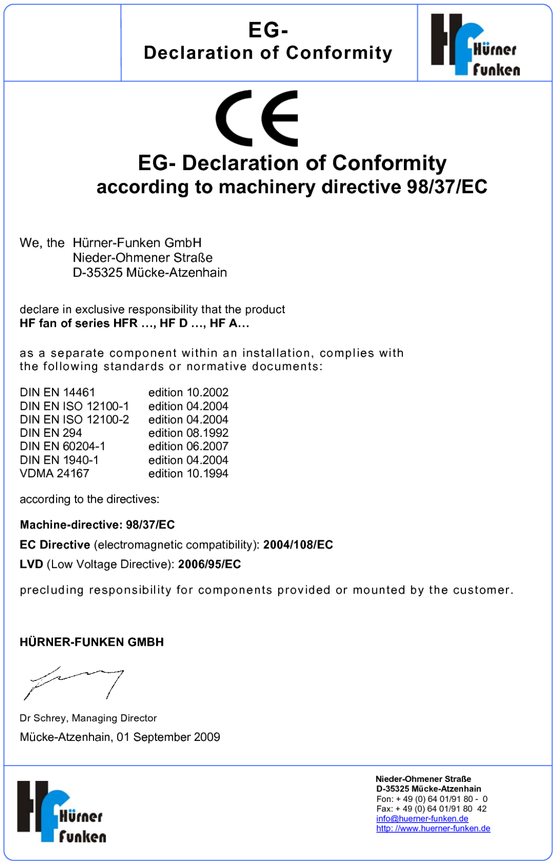


Figure 2.1: The symbol of CE marking



EG-
Declaration of Conformity

EG- Declaration of Conformity
according to machinery directive 98/37/EC

We, the Hürner-Funken GmbH
Nieder-Ohmener Straße
D-35325 Mücke-Atzenhain

declare in exclusive responsibility that the product
HF fan of series HFR …, HF D …, HF A…

as a separate component within an installation, complies with the following standards or normative documents:

DIN EN 14461	edition 10.2002
DIN EN ISO 12100-1	edition 04.2004
DIN EN ISO 12100-2	edition 04.2004
DIN EN 294	edition 08.1992
DIN EN 60204-1	edition 06.2007
DIN EN 1940-1	edition 04.2004
VDMA 24167	edition 10.1994

according to the directives:

Machine-directive: 98/37/EC

EC Directive (electromagnetic compatibility): **2004/108/EC**

LVD (Low Voltage Directive): **2006/95/EC**

precluding responsibility for components provided or mounted by the customer.

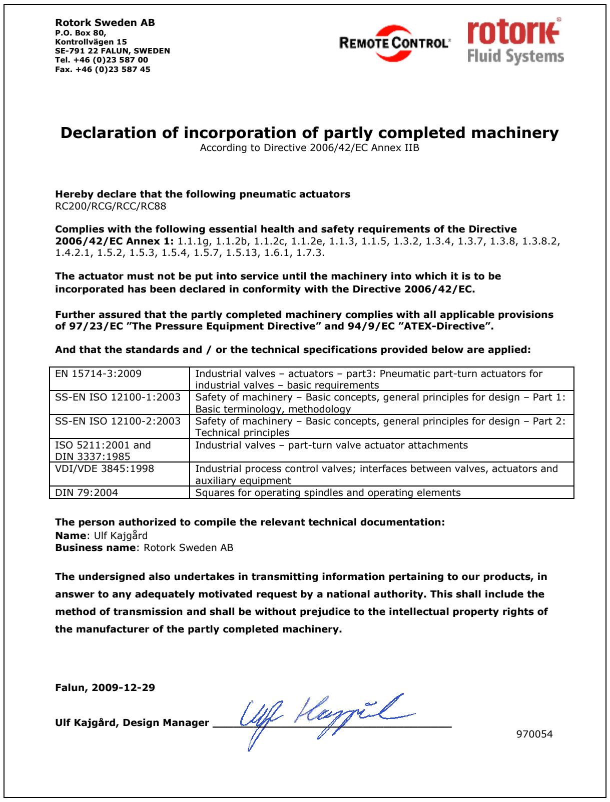
HÜRNER-FUNKEN GMBH

Dr Schrey, Managing Director

Mücke-Atzenhain, 01 September 2009

Nieder-Ohmener Straße
D-35325 Mücke-Atzenhain
Fon: + 49 (0) 64 01/91 80 - 0
Fax: + 49 (0) 64 01/91 80 42
info@huerner-funken.de
http: //www.huerner-funken.de

Figure 2.2: Example of a DOC



Rotork Sweden AB
P.O. Box 80,
Kontrollvägen 15
SE-791 22 FALUN, SWEDEN
Tel. +46 (0)23 587 00
Fax. +46 (0)23 587 45

Declaration of incorporation of partly completed machinery
According to Directive 2006/42/EC Annex IIB

Hereby declare that the following pneumatic actuators
RC200/RCG/RCC/RC88

Complies with the following essential health and safety requirements of the Directive 2006/42/EC Annex 1: 1.1.1g, 1.1.2b, 1.1.2c, 1.1.2e, 1.1.3, 1.1.5, 1.3.2, 1.3.4, 1.3.7, 1.3.8, 1.3.8.2, 1.4.2.1, 1.5.2, 1.5.3, 1.5.4, 1.5.7, 1.5.13, 1.6.1, 1.7.3.

The actuator must not be put into service until the machinery into which it is to be incorporated has been declared in conformity with the Directive 2006/42/EC.

Further assured that the partly completed machinery complies with all applicable provisions of 97/23/EC ”The Pressure Equipment Directive” and 94/9/EC ”ATEX-Directive”.

And that the standards and / or the technical specifications provided below are applied:

EN 15714-3:2009	Industrial valves – actuators – part3: Pneumatic part-turn actuators for industrial valves – basic requirements
SS-EN ISO 12100-1:2003	Safety of machinery – Basic concepts, general principles for design – Part 1: Basic terminology, methodology
SS-EN ISO 12100-2:2003	Safety of machinery – Basic concepts, general principles for design – Part 2: Technical principles
ISO 5211:2001 and DIN 3337:1985	Industrial valves – part-turn valve actuator attachments
VDI/VDE 3845:1998	Industrial process control valves; interfaces between valves, actuators and auxiliary equipment
DIN 79:2004	Squares for operating spindles and operating elements

The person authorized to compile the relevant technical documentation:
Name: Ulf Kajgård
Business name: Rotork Sweden AB

The undersigned also undertakes in transmitting information pertaining to our products, in answer to any adequately motivated request by a national authority. This shall include the method of transmission and shall be without prejudice to the intellectual property rights of the manufacturer of the partly completed machinery.

Falun, 2009-12-29

Ulf Kajgård, Design Manager ______________________

970054

Figure 2.3: Example of a DOC

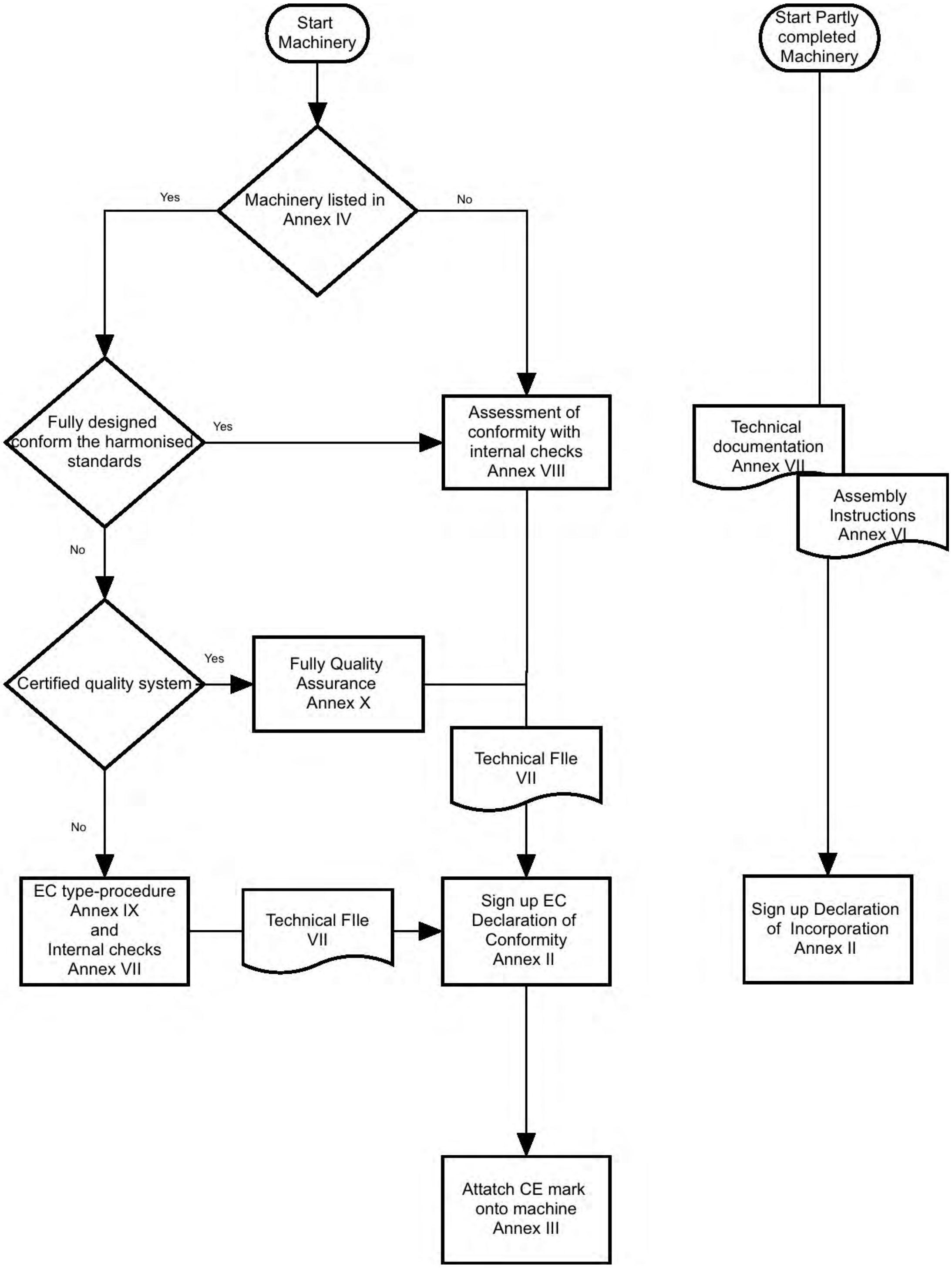

Start Machinery
Machinery listed in Annex IV
Yes
No
Fully designed conform the harmonised standards
Yes
Assessment of conformity with internal checks Annex VIII
No
Certified quality system
Yes
Fully Quality Assurance Annex X
Technical FIle VII
No
EC type-procedure Annex IX and Internal checks Annex VII
Technical FIle VII
Sign up EC Declaration of Conformity Annex II
Attatch CE mark onto machine Annex III
Start Partly completed Machinery
Technical documentation Annex VII
Assembly Instructions Annex VI
Sign up Declaration of Incorporation Annex II

Figure 2.4: Flowchart of depicting the process of compliance

Chapter 3

Harmonised standards

Harmonised standards support European legislation. They (1) have been mandated by the European Commission, (2) have been developed by one of the European standard bodies, (3) address essential requirements of directives and (4) notification of their development has been published on the Official Journal of the European Communities.

As explained by the European Commission, the standards supporting the Machinery Directive are classified into three categories:

- A-type standards: These standards specify basic concepts, terminology and design principles applicable to all categories of machinery. Application of such standards alone, although providing an essential framework for the correct application of the Machinery Directive, is not sufficient to ensure conformity with the relevant essential health and safety requirements of the Directive and therefore does not give a full presumption of conformity.

- B-type standards: These standards deal with specific aspects of machinery safety or specific types of safeguard that can be used across a wide range of categories of machinery. Application of the specifications of B-type standards confers a presumption of conformity with the essential health and safety requirements of the Machinery Directive that they cover when a C-type standard or the manufacturer's risk assessment shows that a technical solution specified by the B-type standard is adequate for the particular category or model of machinery concerned. Application of B-type standards that give specifications for safety components that are independently placed on the market confers a presumption of conformity for the safety components concerned and for the essential health and safety requirements covered by the standards.

- C-type standards: These provide specifications for a given category of machinery. The different types of machinery belonging to the category covered by a C-type standard have a similar intended use and present similar hazards. C-type standards may refer to A or B-type standards, indicating which of the specifications of the A or B-type standard are applicable to the category of machinery concerned. When, for a given aspect of machinery safety, a C-type standard deviates from the specifications of an A or B-type standard, the specifications of the C-type standard take precedence over the specifications of the A or B-type standard. Application of the specifications of a C-type standard on the basis of the manufacturer's risk assessment confers a presumption of conformity with the essential health and safety requirements of the Machinery Directive covered by the standard. Certain C-type standards are organised as a series of several parts, Part 1 of the standard giving general specifications applicable to a family of machinery and other parts of the standard giving specifications for specific categories of machinery belonging to the family, supplementing or modifying the general specifications of Part 1. For C-type standards organised in this way, the presumption of conformity with the essential health and safety requirements of the Machinery Directive is conferred by application of the general Part 1 of the standard together with the relevant specific part of the standard.

A list of the standards that support the Machinery Directive are published and regularly updated on the website of the European Union.

3.1 A risk based approach

At the core of achieving safety of machinery lies a risk based approach. The main concept of this approach is described in the A-standard ISO 12100:2010; *"Safety of machinery - General principles for design - Risk assessment and risk reduction."* It specifies principles of risk assessment and risk reduction. Technical report ISO/TR 14121-2:2012; *"Safety of machinery - Risk assessment - Part 2: Practical guidance and examples of methods"*, provides practical guidance on conducting risk assessments for machinery in accordance with ISO 12100 and describes various methods and tools for each step in the process. The overall process of conducting a risk assessment and reducing risk is shown in Figure 3.1. For a detail description on how to conduct a risk assessment, Rausand (2011) presents different methods, tools and theoretical backgrounds.

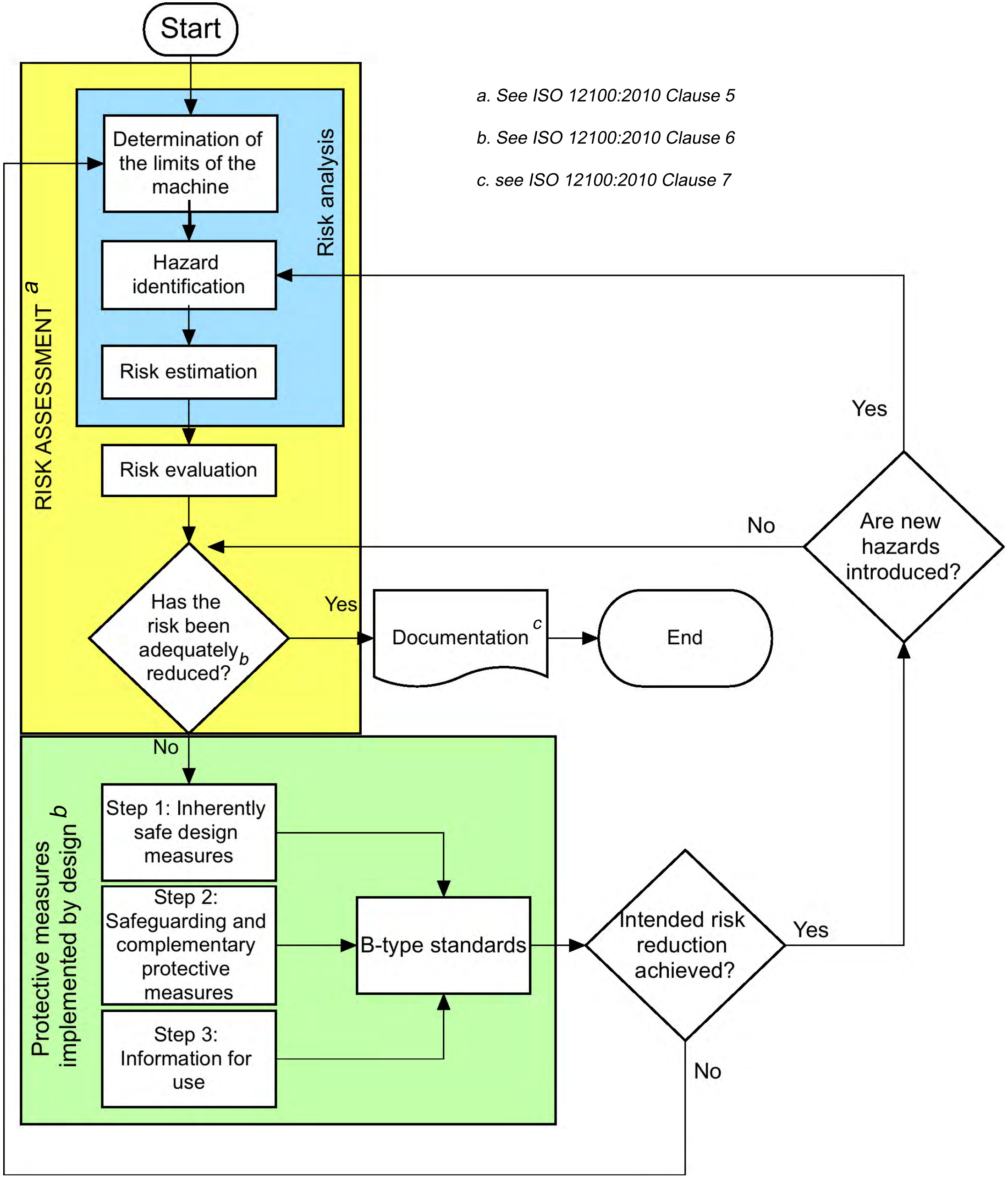

Start
RISK ASSESSMENT a
Risk analysis
Determination of the limits of the machine
Hazard identification
Risk estimation
Risk evaluation
Has the risk been adequately b reduced?
Yes
No
Documentation c
End
a. See ISO 12100:2010 Clause 5
b. See ISO 12100:2010 Clause 6
c. see ISO 12100:2010 Clause 7
Are new hazards introduced?
Yes
No
Protective measures implemented by design b
Step 1: Inherently safe design measures
Step 2: Safeguarding and complementary protective measures
Step 3: Information for use
B-type standards
Intended risk reduction achieved?
Yes
No

Figure 3.1: Flowchart risk assessment process. (adapted from ISO/TR18569 (2004) and ISO-12100:2010 (2010))

Risk reduction

Once a risk assessment is conducted and it has been judged that the risk for an identified hazard has not been adequately reduced, the ISO 12100:2010 promotes a hierarchal implementation of protective measures. The order of implementation is as follows:

1. Inherently safe design measures: When reducing risk, these measures are to be implemented first. These measures eliminate hazards or reduce the associated risks by a suitable choice of design features of the machine itself. Requirements are described in clause 6.2 of the ISO 12100. An example of an inherently safe design measure is a safety function conducted by a control system. Clause 6.2.11 of the ISO 12100:2010 refers to the B-standard ISO 13849 and the C-standard IEC 62061.

2. Safeguarding and complementary protective measures: When it is not practicable to reduce risk by use of inherently safe design measures, safeguarding and complementary protective measures can be used to reduce the risk to an acceptable level. Requirements are described in clause 6.3 of the ISO 12100:2010. Examples of these measures are emergency stop equipment and fixed or interlocking movable guards. Specific B standards for each measure is available.

3. Information for use: When risk remains, despite the application of the safe design measures and the safeguarding, the residual risks shall be identified in the information for use. Requirements are described in clause 6.4 of the ISO 12100. The standard IEC 62079 gives requirement and guidance for structuring and presentation of information for use.

Chapter 4

Safety and reliability of control systems

The Machinery Directive imposes requirements regarding the safety and reliability of control systems. These are stated in Annex I, section 1.2 Control systems, clause 1.2.1 'Safety and reliability of control systems". Control systems must be designed and constructed to prevent hazardous situations from arising. They must be designed and constructed in such a way that:

- they can withstand the intended operating stresses and external influences,
- a fault in the hardware or the software of the control system does not lead to hazardous situations,
- errors in the control system logic do not lead to hazardous situations,
- reasonably foreseeable human error during operation does not lead to hazardous situations.

Particular attention must be given to the following points:

- the machinery must not start unexpectedly,
- the parameters of the machinery must not change in an uncontrolled way, where such change may lead to hazardous situations,
- the machinery must not be prevented from stopping if the stop command has already been given,

- no moving part of the machinery or piece held by the machinery must fall or be ejected,
- automatic or manual stopping of the moving parts, whatever they may be, must be unimpeded,
- the protective devices must remain fully effective or give a stop command,
- the safety-related parts of the control system must apply in a coherent way to the whole of an assembly of machinery and/or partly completed machinery.

The first paragraph of section 1.2.1 and its 4 indents set out the basic requirements for the reliability and safety of control systems. The second paragraph of section 1.2.1 and its 7 indents describe the main hazardous events and situations that must be avoided.

The ISO 12100 defines safety functions conducted by control systems as part of the inherently safe design of machinery. It imposes requirements the control systems need to meet in clause 6.2.11. This clause refers to the standards ISO 13849-1 and IEC 62061.

4.1 Standards ISO 13849-1 and IEC 62061

Both ISO 13849-1: *"Safety of machinery - Safety-related parts of control systems"* and IEC 62061: *"Safety of machinery- Functional safety of safety-related electrical, electronic and programmable electronic control systems"*, specify requirements for the design and implementation of safety-related control systems. They have been adopted by the European standardisation bodies CENELEC and CEN and have been published with the status of transposed harmonised standards under the Machinery Directive.

The ISO 13849-1 is a type B standard and gives guidance on the design of machinery control systems in order to comply with the safety requirements of the Machinery Directive. It is applicable on control systems based on electrical, hydraulic, pneumatic and mechanical technologies. It presents strategies and methods that are proven to design systems that avoid, detect and/or tolerate failures in order to reduce hazardous and dangerous situations. The ISO 13849-1 is aimed at traditional electrical technology and with the introduction of more complex electrical and programmable control systems, there is need for a more specific standard that uses the concept of functional safety and safety integrity.

The concept of functional safety and safety integrity is introduces and described in the standard IEC 61508: *"Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related systems"*. The IEC 62061 is the machinery sector specific standard within the IEC 61508 framework. Just as the ISO 13849, it is intended to be used within the framework of systematic risk reduction described in ISO 12100:2010. The standard gives methods and requirements to:

- assign the required measure of risk reduction for each safety-related control function to be implemented by safety-related control systems;
- enable the design of the control system appropriate to the assigned safety- related control functions;
- integrate safety-related subsystems designed in accordance with ISO 13849;
- validate the safety-related control systems.

4.2 Functional safety

As a result of automation, demand for increased production and reduced operator physical effort, control systems of machines play an increasing role in the achievement of overall machine safety. The part of machine safety which depends on the correct functioning of active control and safety systems is called functional safety. Control systems that contribute to functional safety are in general referred to as safety-related control systems. These systems provide the required risk reduction and are an integral subset of the machine. Figure 4.1 illustrates how a safety-related control system might contribute to reducing risk for a specific hazardous situation.

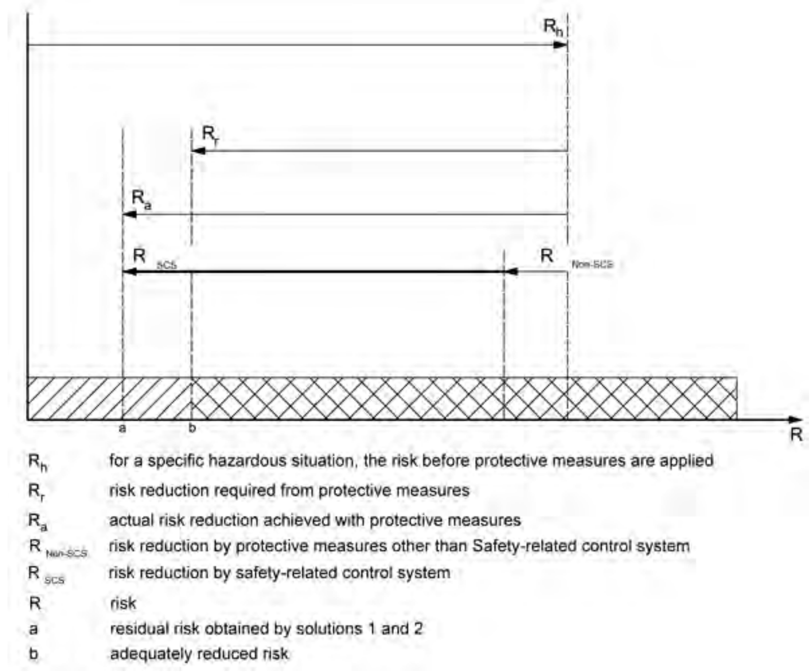

Rh
Rr
Ra
R SCS
R Non-SCS
a
b
R
Rh for a specific hazardous situation, the risk before protective measures are applied
Rr risk reduction required from protective measures
Ra actual risk reduction achieved with protective measures
R Non-SCS risk reduction by protective measures other than Safety-related control system
R SCS risk reduction by safety-related control system
R risk
a residual risk obtained by solutions 1 and 2
b adequately reduced risk

Figure 4.1: Risk reduction by different measures (adapted from EN-ISO13849-1 (2006))

Control systems that are safety-related conduct safety functions. ISO 12100 defines safety functions. Both the ISO 13849 and IEC 62061 adopt this definition.

☞ **Safety function** 'function of the machine whose failure can result in an immediate increase of the risk.

Rausand (2011) distinguishes two categories of safety functions. These are:

- Safety control functions. A safety function that is a normal part of the operation of the machinery and/or integrated into the machinery control system.

- Safety protective function. A dedicated safety function that is separate from the control system and is only activated when the safety function is demanded. Examples are Emergency Shutdown systems (ESD).

Within the ISO 12100, safety functions conducted by control systems are part of the inherently safe design of the machine. This implies that risk reduction achieved by the control system has precedence over safeguards, complementary productive measures and information for use.

4.3 Safety-related control systems

The term control system is well defined. Most standards adopt a definition that is the same or similar to the one given in ISO 13849-1:2006.

☞ **Control system** "system which responds to input signals from parts of machine elements, operators, external control equipment or any combination of these and generates output signals causing the machine to behave in the intended manner." (EN-ISO13849-1, 2006)

The control systems that realises functional safety by conducting safety control functions, consist out of at least three subsystems. These are:

1. Sensor subsystem. This subsystem detects potential danger and produces an electrical signal that is sent to a logic solver.

2. Logic solver subsystem. Detects the electrical signal exceeding a set threshold and sends a signal to the final elements.

3. Final element subsystems. Performs the safety function.

The definitions of a safety-related control system or safety-related part of a control system is less unambiguous. The previous mentioned ISO 13849-1:2006 does not define safety-related control systems, but only mentions safety-related part of a control system (SRP/CS).

☞ **Safety-Related Part of a Control System** "part of a control system that responds to safety-related input signals and generates safety-related output signals." (EN-ISO13849-1, 2006)

This definition seems to exclude parts of the control system that conducts control functions that contribute to risk reduction but do not respond on safety related input, such as operational functions (e.g. starting, normal stopping). These control functions do not respond to safety-related input as such, but are part of the inherent safety design of the machine. ISO 13849-1:2006 states that *"SRP/CS may also provide an operational function"*, but the standard does not specify if the safety function and the operational function can be identical.

The standard IEC 62061 defines Safety-Related Electrical Control Systems (SRECS).

☞ **Safety-Related Electrical Control Systems** "electrical control system of a machine whose failure can result in an immediate increase of the risk." NOTE: A SRECS includes all parts of an electrical control system whose failure may result in a reduction or loss of functional safety and this can comprise both electrical power circuits and control circuits. (IEC-62061, 2006)

As opposed to the definitions of SRP/CS, this definition does imply that a control system that conducts any function, including the operational functions of the control system, that when fails leads to increased risk, are subsumed under SRECS and can be interpreted as a safety function. These functions conducted by the SRECS, that are intended to maintain the safe condition of the machine or prevent an immediate increase of the risk, are defined as Safety-Related Control Function (SRCF).

☞ **Safety-Related Control Function** "control function implemented by a SRECS with a specified integrity level that is intended to maintain the safe condition of the machine or prevent an immediate increase of the risk(s)". (IEC-62061, 2006)

4.3.1 Continuous demand

The duality in function, being a process and safety function, means that the demand rate of the safety function and the process control function is equal. When the demand for the process control function is continuous, the demand rate for the safety function is continuous as well. Although this train of thought is derived from the definitions given in the IEC 62061, nothing in the ISO 13849 seems to contradict this line of thinking.

Within the IEC 61508 framework, the continuous demand for the safety function is defined as the continuous mode. A safety function operates in a continuous mode when the the safety function retains the machine in a safe state as part of normal operation. The fact that a control function can be regarded as safety critical and might be defined as such, has implications for defining integrity requirements for the control function. An in-depth discussion on these implications is presented in Part two of this report.

4.4 Risk estimation, tolerable risk, and required risk reduction

The ISO 13849-1 and the IEC 62061 adopt the strategy for risk reduction at the machine that is presented in ISO 12100-1:2003. The risk estimation has to be conducted conform clause 5.5 of the ISO 12100-1:2010 as described in chapter 3. When the risk of a certain hazardous situations is known, it needs to be established if the risk is tolerable or should be reduced. To establish what risk is tolerable and what risk is not, nor the ISO 12100 or the ISO 14121 mentions specific methods or tools. The ISO 12100 gives very general requirements to evaluate if the risk is tolerable and if it needs to be reduced. The approach described in clause 5.6.3: Comparison of risk, stating; *'As part of the process of risk evaluation, the risks associated with the machinery or parts of machinery can be compared with those of similar machinery or parts of the machinery'.* This can be interpreted as the "Globalement au moins aussi bon" (GAMAB) principle. The IEC 61508 recommends the "as low as reasonable practicable" (ALARP) principle to establish what risk tolerable.

When the risk associated with an identified hazardous event is known, and the tolerable risk is defined, the difference between the two is equal to the required risk reduction. If it is decided that the required risk reduction has to be delivered by a safety function conducted by a control system, or a hazard is introduced by the possible failure of the control system, the measure of required risk reduction needs to be quantified. ISO 13849-1 and IEC 62061 introduce two different concepts to categorize the measure of risk reduction a safety function needs to deliver. Respectively the concept of Performance Levels (PL) and the concept of Safety Integrity Levels (SIL).

4.5 Performance Level

ISO 13849 uses the concept of the performance of safety functions. It consists out of the required Performance Level (PL_r) and the Performance Level (PL). PL_r is the performance that needs to be met by the SRP/CS that conducts the safety functions to achieve the required risk reduction. The PL is the discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions. The standard defines five different PL_r and PL's, ranging from a to e. Once it is established that risk needs to be reduced with a certain

PL_r, a safety function needs to be designed that meets the corresponding PL.

Determining the PL_r

Establishing PL_r results from a risk assessment. The risk assessment assumes a situation prior to provision of the intended safety function. Determination of the PL_r is done by conducting a risk graph. This method is presented in Annex A of the ISO 13849-1 and is discussed by authors such as Baybutt (2007) and Nait-Said et al. (2008)

Safety function design and PL evaluation

Once the PL_r for each hazardous event is established, the safety function(s) that will reduce the risk needs to be designed. The PL of a safety function is determined by its quantifiable aspects and its non-quantifiable, qualitative aspects. The quantifiable aspects are the aspects of the SRP/CS that can be related to the hardware random failures of the system. ISO 13849 states that the probability of these hardware random failures of the system occurring, referred to as the reliability of the system, are determined by the following characteristics of the system:

- the Mean Time To dangerous Failure($MTTF_d$) value for a single component,
- the Diagnostic coverage(DC),
- the Common Caused Failures, and
- the structure of the system.

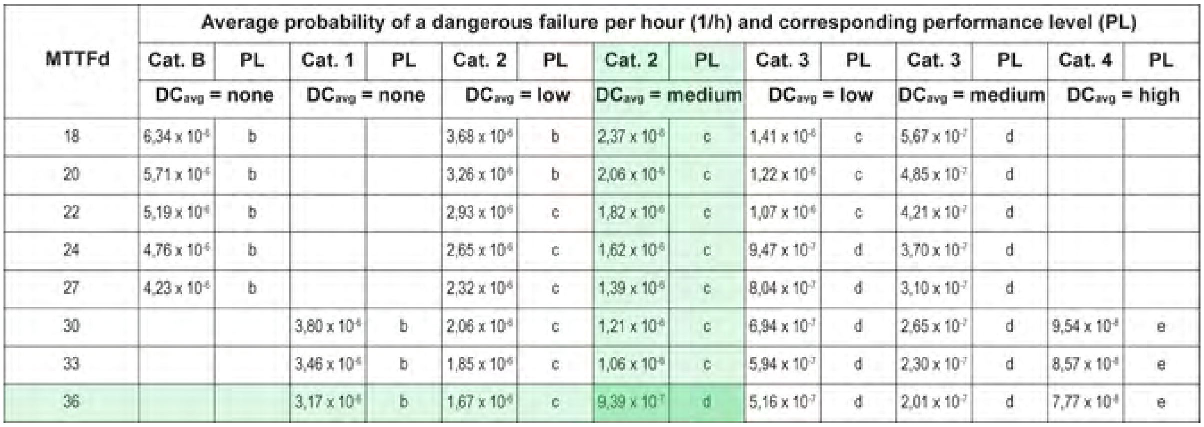
The system has to be designed in such a way that the SRP/CS meets the reliability requirements that are set for each of the PL. As mentioned, the PL's range from a to e. For each PL, ISO 13849 has defined the reliability requirement in terms of average probability of dangerous failure per hour (PFH). They are shown in Table 4.1. In this case a dangerous failure is defined as:

☞ **dangerous failure** "a failure which has the potential to put the SRP/CS in a hazardous or fail-to-function state." (EN-ISO13849-1, 2006). It has to be noted that this definition is adapted from IEC 61508-4:1998.

Table 4.1: Performance levels

PL	Avg. Pr. of dangerous failure/hour (PFH)
a	≥ 10¯5 to < 10¯4
b	≥ 3 ∗ 10¯6 to < 10¯5
c	≥ 10¯6 to < 3 ∗ 10¯6
d	≥ 10¯7 to < 10¯6
e	≥ 10¯8 to < 10¯7

The qualitative aspects of the SRP/CS are characteristics such as the behavior of the safety function under fault conditions, safety-related software, systematic failure and environmental conditions. The relation between the characteristics of the system and the reliability of the system are explained in the standard. It describes a simplified procedure for estimating the PL of a system in clause 4.5.4. Once it is established how the subsystem is structured (category B, 1, 2, 3 or 4), the the diagnostic coverage is established (low, medium, or high) and the $\mathrm{MTTF_d}$ is established, the achieved PL can be found. This is presented in Figure 4.5.



MTTFd	Average probability of a dangerous failure per hour (1/h) and corresponding performance level (PL)													
	Cat. B	PL	Cat. 1	PL	Cat. 2	PL	Cat. 2	PL	Cat. 3	PL	Cat. 3	PL	Cat. 4	PL
	DC_{avg} = none		DC_{avg} = none		DC_{avg} = low		DC_{avg} = medium		DC_{avg} = low		DC_{avg} = medium		DC_{avg} = high	
18	$6,34 \times 10^{-6}$	b			$3,68 \times 10^{-6}$	b	$2,37 \times 10^{-6}$	c	$1,41 \times 10^{-6}$	c	$5,67 \times 10^{-7}$	d		
20	$5,71 \times 10^{-6}$	b			$3,26 \times 10^{-6}$	b	$2,06 \times 10^{-6}$	c	$1,22 \times 10^{-6}$	c	$4,85 \times 10^{-7}$	d		
22	$5,19 \times 10^{-6}$	b			$2,93 \times 10^{-6}$	c	$1,82 \times 10^{-6}$	c	$1,07 \times 10^{-6}$	c	$4,21 \times 10^{-7}$	d		
24	$4,76 \times 10^{-6}$	b			$2,65 \times 10^{-6}$	c	$1,62 \times 10^{-6}$	c	$9,47 \times 10^{-7}$	d	$3,70 \times 10^{-7}$	d		
27	$4,23 \times 10^{-6}$	b			$2,32 \times 10^{-6}$	c	$1,39 \times 10^{-6}$	c	$8,04 \times 10^{-7}$	d	$3,10 \times 10^{-7}$	d		
30			$3,80 \times 10^{-6}$	b	$2,06 \times 10^{-6}$	c	$1,21 \times 10^{-6}$	c	$6,94 \times 10^{-7}$	d	$2,65 \times 10^{-7}$	d	$9,54 \times 10^{-8}$	e
33			$3,46 \times 10^{-6}$	b	$1,85 \times 10^{-6}$	c	$1,06 \times 10^{-6}$	c	$5,94 \times 10^{-7}$	d	$2,30 \times 10^{-7}$	d	$8,57 \times 10^{-8}$	e
36			$3,17 \times 10^{-6}$	b	$1,67 \times 10^{-6}$	c	$9,39 \times 10^{-7}$	d	$5,16 \times 10^{-7}$	d	$2,01 \times 10^{-7}$	d	$7,77 \times 10^{-8}$	e

Figure 4.2: With a $\mathrm{MTTF_d}$ of 36 years, a structure conform cat.2 and a medium DC, the system will meet PL d with an average probability of dangerous failure per hour of $9,39E-7$. Adapted from EN-ISO13849-1 (2006)

4.5.1 Points of interest in ISO 13849

Using $\mathrm{MTTF_d}$ to determine reliability of safety function

ISO 13849 states that one of the characteristics of the system that has influence on the reliability of the safety function is the $\mathrm{MTTF_d}$ for the components that conduct the function. The ISO 13849 shows and presents a simplified method on how the PL of a safety function can be assessed. Part of this method is to calculate the $\mathrm{MTTF_d}$ values for single components. This is explained in Annex C of ISO 13849. All the $\mathrm{MTTF_d}$ of the components that conduct the safety function are then summed. This is shown in Annex D and Annex I. The $\mathrm{MTTF_d}$ is then interpreted as the inverse failure rate of the exponential distribution. Meaning, that from the $\mathrm{MTTF_d}$ it is possible to retain the overall failure rate of the safety function and calculate the average probability of dangerous failure per hour. Thus, estimate if a function meets the required PFH for the corresponding PL's, as shown in Table 4.1. Although this method is common practice, there are some drawbacks. One of them lays in the assumption that the failure of components is distributed exponential over time. $(F(t) = 1 - \exp(-\lambda dt)$. It is known that pneumatic and electromechanical components are more likely to show a Weibull failure distribution. This is of major influence on the evaluation of the $\mathrm{MTTF_d}$ and therefore reliability assessment of the safety function. This is made clear in example 4.1

Example 4.1 Manufactures of components often only give the mean number of cycles until 10% of the components fail dangerously ($\mathrm{B_{10d}}$). In Annex C, the ISO 13849 introduces a pneumatic valve with a mean value of 60 million cycles as $\mathrm{B_{10d}}$. Assuming the valve shows an exponential distribution, the $\mathrm{MTTF_d}$ of the valve is calculated to be $\approx 6 * 10^8$ cycles.

It is known that pneumatic components are more likely to show a Weibull distribution. With some simple calculations this example shows the impact a false assumption of failure distributions can have on the calculation of the expected $\mathrm{MTTF_d}$.

For Weibull the probability that an item fails within the time interval(0,t] is given as:

$$F(t) = 1 - \exp -(\lambda * t)^{\alpha} \tag{4.1}$$

In which λ is the scale parameter, and α the aging parameter. The MTTF for weibull can be calculated as:

$$\frac{1}{\lambda}\Gamma(\frac{1}{\alpha}+1) \tag{4.2}$$

Using the same valve with $B_{10d} = 6 * 10^8$ cycles, and a realistic α=1.2, we solve (4.1) for λ. This gives $\lambda = 2,55513 * 10^-9$. Applying (4.2), with $\Gamma(\frac{1}{\alpha}+1) = 0.93969$, results in a $MTTF_d$ of $3.6 * 10^8$ cycles.

Example 4.1 shows it is essential to understand the failure mechanisms and failure characteristics of components used in safety-related control systems. Although the standard provides guidance, the designer of the control system needs to asses if it is applicable on the system at hand. When it is known a system component does not show exponential failure distribution, the simplified method presented in the ISO 13849 should not be applied.

Measures against CCF

The estimation of common cause failure (CCF) is a well discussed topic. Authors such as Hauge et al. (2013) and Rausand (2011) discuss methods on how to incorporate them in reliability studies of systems. Both ISO 13849 and IEC 62061 adopt the β-factor method. Estimation of the β-factor for the CCF's requires detail knowledge of the system at hand. A proven method to estimate the β-factor, is the use of checklists. These checklists quantify the effect of measures against CCF. By establishing if these measures are absent or present in the system design, the β-factor is estimated. Examples of these checklists can be found in IEC 61508 and IEC 62061.

As mentioned, these checklist will give a certain β-factor that can be used in the reliability calculations. ISO 13849 presents a check list but instead of using it to determine the β-factor, its result is used to determine if additional measures are to be implemented into the system design to avoid CCFs. The CCF checklist of both ISO 13849 and IEC 62061 are less extensive than the one presented in part six of IEC 61508, but are therefore deemed more practical and of better use for machinery design. Both checklist acknowledge that the following factors have effect on the CCF's of machinery:

1. Separation/Segregation

2. Diversity
3. Design/applications/experience
4. Assessment/analysis
5. Competence/training
6. Environmental control

Each factor is accompanied with questions, that when answered get a score. IEC 62061 connects these score to a certain value of the β-factor. See Table 4.2. ISO 13849 uses its score to determine if more measures should be implemented to avoid CCF's. A score of 65 and more, according to ISO 13849's checklist, means no other measures need to be implemented. A score less than 65 means additional measures need to be implemented. ISO 13849 also notes that it is assumed that for redundant systems a β-factor should be less than, or equal to 2%. Table 4.2 shows that a score of 65, according to IEC 62061's checklist, results in a β-factor of 2%. A score of 65 for both checklists seem to result in a β-factor of 2%.

As both the checklists are different in their way of questioning and in their way of scoring the contribution to CFF's of the different factors, the assimilation of a score of 65 from ISO 13849 checklist, to that of a score of 65 from the IEC 62061, without any motivation or reasoning seems to be inaccurate and arbitrary.

Table 4.2: Score and β-factor from EN-ISO13849-1 (2006)

Overall score	Common cause failure factor
<35	10%
36 to 65	5%
65 to 85	2%
85 to 100	1%

4.6 Safety integrity level

The concept of SIL is introduced in IEC 61508 and adopted by IEC 62061. A SIL is the level of integrity a safety function, conducted by a control system, needs to meet to achieve the required risk reduction. IEC 61508 defines 4 levels. SIL1 is the lowest level of safety integrity and SIL4 is the highest level. The IEC 62061 has only adopted the SIL 1,2 and 3. Each SIL has specific requirements that are related to the reliability of the safety function and the structure of the system that conduct the safety function. These are respectively defined as the quantitative reliability requirements and the architectural constrains.

Determining the SIL a safety function needs to meet

The IEC 62061 suggests several methods to determine which SIL a safety functions a needs to meet to gain sufficient risk reduction. It has adopted the SIL assignment matrix in its Annex A, but refers to the IEC 61508-5 for other methods. Methods presented in the IEC 61508-5 are:

- A quantitative method
- Risk graph methods
- Semi-quantitative method using layer of protection analysis (LOPA)

Quantitative reliability requirements

The IEC 61508 introduces two different reliability measures. The probability of failure on demand (PFD) and the probability of dangerous failure per hour (PFH). The IEC 62061 only adopts the PFH as a reliability measure and defines it as:

☞ **probability of dangerous failure per hour** "the average probability of a dangerous failure per hour of a safety-related system/subsystem to perform the specified safety function over a given period of time." (IEC-62061, 2006)

In which a dangerous failure is defined as:

☞ **dangerous failure** "failure of a SRECS, a subsystem, or a subsystem element that has the potential to cause a hazard or non-functional state."(IEC-62061, 2006)

The reader known with the IEC 61508 notices that dangerous failures are defined differently in the IEC 61508. This is related to the fact that the IEC 62061 only considers SRCF's that operate in continuous mode or act on high demand. The second part of this report discusses this topic in further detail.

Architectural constrains

As explained, a SRECS consists at least out of three subsystems. To ensure that the system is robust enough, IEC 62061 formulates architectural restrains. These constraints specify the redundancy level, of each subsystem, to claim compliance with the SIL's. Establishing the required level of redundancy is based on the SIL the subsystem needs to meet, and the safe failure fraction (SFF) of each element within the subsystems. Although originating from IEC 61508, the architectural constrains presented in IEC 62061 are different. The redundancy level is referred to as the hardware fault tolerance (HFT). A HFT of N means that N+1 faults in a subsystem can cause a loss of the SRCF. What HFT is allowed in a subsystem configuration is made depended on the SFF of each element within the subsystem and the SIL the subsystem needs to meet. Table 4.3 shows the the architectural constraints on subsystems. Readers familiar with IEC 61508 might notice that IEC 62061, unlike IEC 61508, does not differentiate between the type and complexity of each element of the SRECS. It also does not allow for a SIL4 to be met by any technical solution.

As expressed by Rausand (2011), the SFF is a measure of the inherent tendency of an element to fail towards a safe state. The SFF is calculated as

$$\text{SFF} = \frac{\text{The sum of the rate of safe and DD failures of the element}}{\text{The sum of the rate of safe and dangerous failure of the element}}$$

The question is if this way of calculating the SFF still holds in case of continuous demand, as a dangerous detected or a dangerous undetected failure might have the same effect. The second

Table 4.3: Architectural constraints on subsystems: maximum SIL that can be claimed

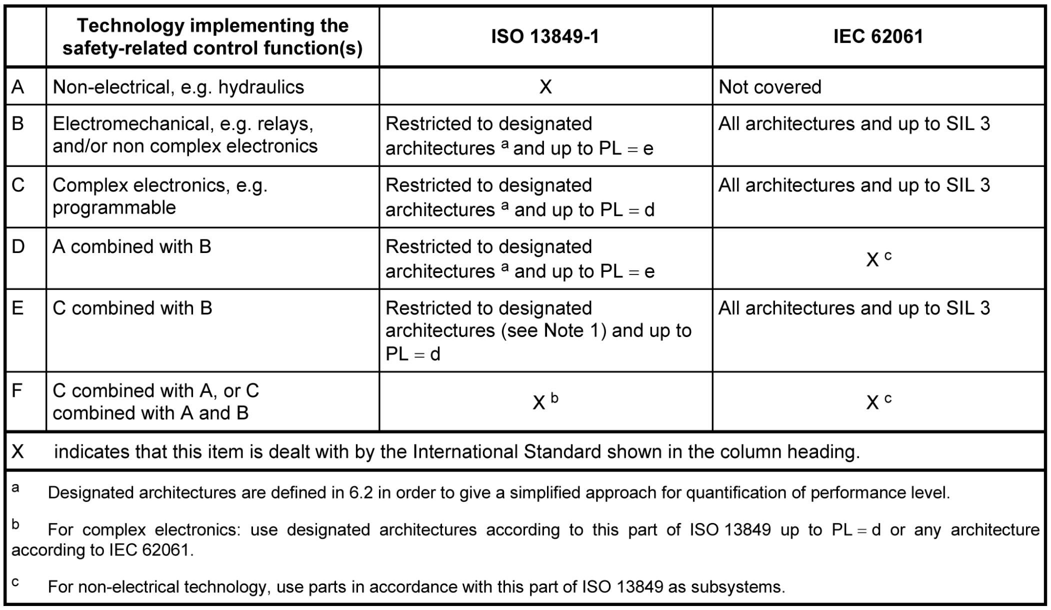
Safe Failure Fraction	Hardware Fault Tolerance		
	0	1	2
<60%	Not allowed	SIL 1	SIL 2
60% to <90%	SIL 1	SIL 2	SIL 3
90% to <99%	SIL 2	SIL 3	SIL 3
>99%	SIL 3	SIL 3	SIL 3

part of this report discusses this topic in further detail.

4.7 Comparison and selecting standard to use

Both standards present methods based on dependability studies to design control systems that comply with the essential health and safety requirements. They both introduce concepts and methods that establish the risk that needs to be reduced, and give guidance and requirements on designing systems that shall reduce the risk. Selecting the standard to apply on the control system is a choice made by the manufacturer. Both the ISO 13849-1 and the IEC 62061 present table 4.4 in their introduction to show which systems are within the scope of each standard.

Table 4.4: Recommended application ofIEC 62061 and ISO 13849-1 from EN-ISO13849-1 (2006)



	Technology implementing the safety-related control function(s)	ISO 13849-1	IEC 62061
A	Non-electrical, e.g. hydraulics	X	Not covered
B	Electromechanical, e.g. relays, and/or non complex electronics	Restricted to designated architectures [a] and up to PL = e	All architectures and up to SIL 3
C	Complex electronics, e.g. programmable	Restricted to designated architectures [a] and up to PL = d	All architectures and up to SIL 3
D	A combined with B	Restricted to designated architectures [a] and up to PL = e	X [c]
E	C combined with B	Restricted to designated architectures (see Note 1) and up to PL = d	All architectures and up to SIL 3
F	C combined with A, or C combined with A and B	X [b]	X [c]

X indicates that this item is dealt with by the International Standard shown in the column heading.

[a] Designated architectures are defined in 6.2 in order to give a simplified approach for quantification of performance level.

[b] For complex electronics: use designated architectures according to this part of ISO 13849 up to PL = d or any architecture according to IEC 62061.

[c] For non-electrical technology, use parts in accordance with this part of ISO 13849 as subsystems.

The technical report IEC/TR 62061-1: "Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery" describes the following examples of selection criteria:

- previous knowledge and experience in the design of machinery safety-related systems based upon one of the standards;
- safety-related control systems based upon media other than electrical can mean that the use of ISO 13849-1 is more appropriate;
- customer requirements to demonstrate the safety integrity of a machine safety-related control system in terms of a SIL can mean that the use of IEC 62061 is more appropriate;
- safety-related control systems of machinery used in, for example, the process industries, where other safety-related systems are characterized in terms of SILs, can mean that the use of IEC 62061 is more appropriate.

It is recommended to select the standard based on the scope description of both standards. If the system that is to be designed fits both standards, the practical selection criteria such as presented in IEC/TR 62061-1 can be decisive.

Part II

Continuous Mode

Chapter 5

Continuous mode

The first part of this report has shown how the machinery directive is structured and how the harmonised standards on functional safety introduce concepts for systematic risk reduction by the use of control systems in machinery. It has become apparent that the phenomenon of safety-related control functions that operate in continuous mode ($\text{SRCF}_{\text{cont.}}$) are underexposed. This leads to some points of interest for engineers that are familiar with methods and concepts presented in the IEC 61508. The introduction of a process control function, conducted by the basic control system of machinery, that can be regarded as safety critical and can be defined as such has implications for defining integrity requirements for the control function and the overall design of control systems. The duality in function, being a process and safety function, means that the demand rate of the safety function and the process control function is equal. When the demand for the process control function is continuous, the demand rate for the safety function is continuous as well. Within the IEC 61508 framework the continuous mode is defined as follows

☞ **Continues mode** "where the safety function retains the equipment under control (EUC) in a safe state as part of normal operation." (IEC-61508, 2010)

The IEC 62061 adds to this definition the note that continuous mode means that a safety-related control function is performed perpetually, i.e. the SRECS is continuously controlling the machine and a failure of its function results in a hazardous event. This implies that there is a direct causal relation between the failure of the $\text{SRCF}_{\text{cont.}}$ and the probability of a hazardous event occurring. This makes that there is a significant difference between the SRCF$_{\text{cont.}}$ and the safety functions that act on a demand such as discussed in the IEC 61508

Protection layers and the ISO 12100:2010 framework

Chapter 3 explains that the ISO 12100:2010 promotes a specific order of protection layers to reduce the machine risk to an acceptable level. During design of the machinery, risk reduction by inherently safe design measures has precedence over all other measures. The basic control system design is seen as an inherently safe design measure. The IEC 62061 introduced the SRECS that may conduct a SRCF$_{\text{cont.}}$ as part of the basic control system. These SRCF will have to meet the integrity requirements and the architectural constrains stated in the standard. Once it is not practicable to reduce risk by use of these SRCFs, a Safety-instrumented system (SIS) might be designed. A SIS is then seen as a safeguarding and complementary protective measure. These SISs only act upon the failure of preceding safety layers, such as the SRCF. Therefore they act on demand. When the demand occurs, the SIS brings the machinery, referred to as the equipment under control (EUC), into a safe state. A safety function conducted by a SIS that is assigned a SIL is called a safety instrumented function (SIF). The design choice of adding a SIS to the machine does not mean that the SRCF no longer needs to meet the requirements set in the IEC 62061. Adding safety layers such as a SIS is a proven concept of reducing risk related to the EUC. This concept is often referred to as the onion model and is illustrated in Figure 5.2. Each layer reduced the risk concerning the EUC. It illustrates the sequences of protection layers. The sequence starts from the center and proceeds outwards. Safety layers that act on demands, failure of previous safety layer, can be interpreted as a safety barrier that by conducting its function, prevents a hazardous event of happening. As Rausand (2014) explains: *"The interpretation of hazardous event related to a safety function operating in demanded mode is illustrated in Figure 5.1 where two safety barriers that perform safety functions are installed against a certain type of demands."*

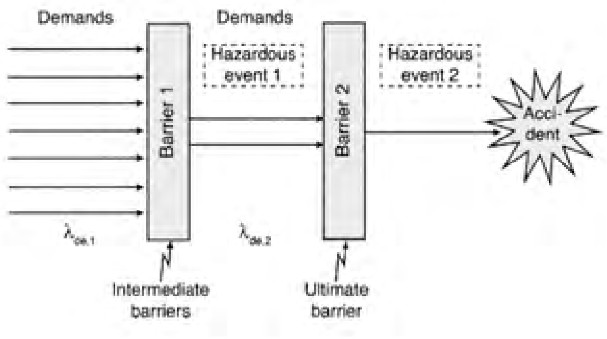


Figure 5.1: The interpretation of a hazardous event to a safety function operated in demanded mode. From Rausand (2014)

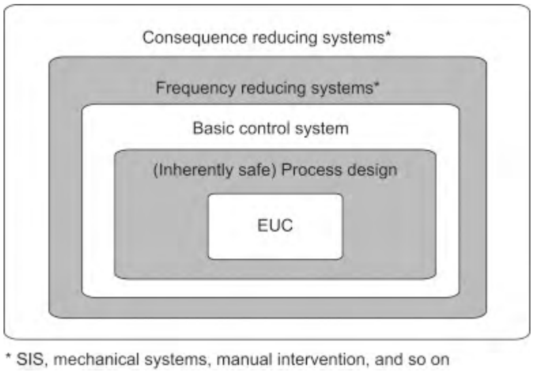

Consequence reducing systems*
Frequency reducing systems*
Basic control system
(Inherently safe) Process design
EUC
* SIS, mechanical systems, manual intervention, and so on

Figure 5.2: The onion model from Rausand et al. (2010)

Issues

This chapter will explore points of interest for designers of control systems that conduct $\text{SRCF}_{\text{cont.}}$ The following issues will be discussed:

1. Design of a $\text{SRCF}_{\text{cont.}}$ and establish its safety integrity, and

2. the combination of a SRECS that conducts a SRCF in continuous mode and a SIS that conducts a SIF on demand to achieve sufficient risk reduction.

5.1 PFH of $\text{SRCF}_{\text{cont.}}$

The reliability measure used in the IEC 62061 for SRCF that need to meet a certain SIL is expressed in PFH. PFH is defined as the probability of a dangerous failure per hour of a safety-related system/subsystem to perform the specified safety function over a given period of time. To calculate the PFH we therefore need to know the two factors:

1. The probability of dangerous failures, and

2. the period of time.

Dangerous failures

In case of a safety function that acts on demand, a dangerous failure is a safety function failure that can lead to a hazardous event in the machine that is protected by the safety function, if a demand for the safety function should occur. As the demand for the function is not always present, a dangerous failure within the safety function can occur and only show when the demand presents itself. This type of failure is called dangerous undetected failure (DU). A failure that can be observed before the function is demanded, is called a dangerous detected failure (DD).

With the introduction of the SRECS that may conduct a $\text{SRCF}_{\text{cont.}}$ as part of the basic control system, this definition of a dangerous failure does not hold. In case of continues mode, the demand for the SRCF can be interpreted as equal to one. It is always present. Any failure of the SRCF, at any time during operation, leads to a hazardous event. Therefore, a dangerous failure is a failure that terminates the ability of the SRECS to conduct its SRCF.

If we assume that a hazardous event occurs more or less immediately when a dangerous failure occurs, the distinction between a dangerous detected (DD) and a dangerous undetected (DU) failure is of no meaning.

Period of time

When calculating the PFH and the item is neither proof-tested, nor overhauled, the IEC 61508 states that a life time of twenty years should be used in the calculation of the PFH. This period of time is denoted as τ

Equations

As explained in section 4.3 of part one, control systems that conducts a safety function, consist out of at least three subsystems. These are:

1. Sensor subsystem (S).

2. Logic solver subsystem (LG).

3. Final element subsystems (FE).

The three subsystems are configured as a series system. It is assumed that the three subsystems are independent and have high reliability. The probability that two or three subsystems fail at the same time is negligible, such that the PFH_{system} can be expressed as:

$$PFH_{\text{system}} = PFH_{\text{S}} + PFH_{\text{LG}} + PFH_{\text{FE}} \tag{5.1}$$

For each subsystem the PFH is:

$$PFH_{\text{G}}(0,\tau) = \frac{\text{Mean number of dangerous group failures in } (0,\tau)}{\tau} \tag{5.2}$$

The average PFH over the test interval is also the long term average and is given by:

$$PFH_{\text{G}}(0,\tau) = \frac{1}{\tau}\int_0^{\tau} PFH_{\text{G}}(t)\,dt \tag{5.3}$$

In this chapter examples of safety systems are introduced and used for demonstrating how the reliability can be calculated. In these examples, calculations are done by the Markov method. For an introduction into using the Markov to calculate the PFH see Rausand (2014) and Rausand and Høyland (2004). As the Markov method is used, 5.3 can be expressed as:

$$PFH_{\text{G}}(0,\tau) = \frac{1}{\tau}\sum_{i\in M_{\text{C}}} \Lambda_{\text{i}} \int_0^{\tau} P_{\text{i}}(t) \tag{5.4}$$

$$PFH_{\text{G}}(0,\tau) = \sum_{i\in M_{\text{C}}} \Lambda_{\text{i}} P_{\text{i}}[0,\tau] \tag{5.5}$$

Where M_{c} denotes the set of critical working states, Λ_{i} the sum of the failure rates removing the critical working state i and finishing in the failed state. $P_{\text{i}}[0,\tau]$ denotes the average probability of being in the critical working state, per unit of time.

5.2 Architectural constraints in continuous mode

Architectural constraints are introduced in Part one, chapter 4 of this report. It describes that the IEC 62061 adopts a slightly modified HFT method from the IEC 61508. The required redundancy in the subsystems is established by the SFF of components and the SIL that needs to be met by the SRCF. Authors such as Lundteigen and Rausand (2009) discuss if the use of HFT is an appropriate method to introduce robustness into the system. Still, as the standards adopt the HFT requirement it is of interest to discuss the topic and assess if the introduction of continuous mode has influence on the structural requirements for SRECS's.

The SIL a SRCF needs to perform is independent of its operation mode. Continuous, high or low demand, the SIL is set during the risk assessment with knowledge of the mode of operation. The SFF on the other hand might be different in continuous mode or demand mode. As expressed by Rausand (2011), the SFF is a measure of the inherent tendency of an element to fail towards a safe state. The SFF is calculated as

$$\text{SFF} = \frac{\text{The sum of the rate of safe and DD failures of the element}}{\text{The sum of the rate of safe and dangerous failure of the element}} \tag{5.6}$$

Lundteigen and Rausand (2009) interprets this as:

$$SFF = P(\text{The failure is "safe"} \mid \text{A component failure occurs}) \tag{5.7}$$

The reason the safe and DD failures are summed in (5.6) is because it is assumed that when the DD occurs a repair action can be conducted before the component is to conduct its function. In case of continuous mode this reasoning does not longer hold. This would mean that in case of continuous mode:

$$\text{SFF} = \frac{\text{The rate of safe failures of the element}}{\text{The sum of the rate of safe and dangerous failure of the element}} \tag{5.8}$$

This has enormous effect on how a system should be structured if the architectural constraints are to met. This is shown in example 5.1

Example 5.1 For this example we take the data for a generic pressure transmitter presented in Annex Data. If we assume that the functions act in demand mode, the SSF is calculated with the Equation (5.6), this gives:

$$\text{SFF} = \frac{\text{The sum of the rate of safe and DD failures of the element}}{\text{The sum of the rate of safe and dangerous failure of the element}} \tag{5.9}$$

$$\mathrm{SFF} = \frac{\lambda_{\mathrm{S}} + \lambda_{\mathrm{DD}}}{\lambda_{\mathrm{S}} + \lambda_{\mathrm{D}}} \tag{5.10}$$

$$\mathrm{SFF} = \frac{5E-7+5E-7}{5E-7+8E-7} \tag{5.11}$$

$$\mathrm{SFF} = 77\% \tag{5.12}$$

Using Table 4.3 we establish that if we want to meet the requirements for SIL2, the HFT should be 1. Meaning that a subsystem consisting out of this transmitter can be structured as 1oo2. In case of a safety function that operates in continuous mode, we use (5.8). This gives:

$$\mathrm{SFF} = \frac{\text{The rate of safe failures of the element}}{\text{The sum of the rate of safe and dangerous failure of the element}} \tag{5.13}$$

$$\mathrm{SFF} = \frac{\lambda_{\mathrm{S}}}{\lambda_{\mathrm{S}} + \lambda_{\mathrm{D}}} \tag{5.14}$$

$$\mathrm{SFF} = \frac{5E-7}{5E-7+8E-7} \tag{5.15}$$

$$\mathrm{SFF} = 38\% \tag{5.16}$$

Using Table 4.3 we establish that if we want to meet the requirements for SIL2, the HFT should be 2. Meaning that a subsystem consisting out of this transmitter can be structured as 1oo3

This would lead to a bigger amount of redundancy that might lead to a less safe system, as discussed by Lundteigen and Rausand (2009)

5.3 The SRCF is the ultimate barrier

If we assume that the SRCF is the ultimate safety barrier before assets are harmed, repairing the barrier is not an option. Simply because no other measure will bring the machinery into a safe state, when the SRCF fails. In this case the PFH should be calculated from its unreliability $F(T) = 1 - R(t)$. As discussed there is no need to split the dangerous failure rate into DD and

DU. System one is used to show how structuring a SRCF and calculating the PFH of the system is done.

System one A SCRF that operates in continuous mode, is conducted by a SRCS that consists out of three subsystems. It is an ultimate barrier. The first subsystem consists out of sensors that measure pressure, the second subsystem consist out of a logic solver and the third subsystem consists out of solenoid valves. With the data presented in the Appendix 'Data', the structure of the function is designed to meet SIL2. Note that due to operation in continuous mode, and the system being an ultimate barrier, the SFF excluding the DD as safe is used to establish the HFT.

- The sensor has a SFF of 38%. The required HFT = 2. The subsystem is voted 1oo3.
- The standard industrial PLC has a SFF of 50%. The required HFT = 2. The subsystem is voted 1oo3.
- The solenoid valve has a SFF of 63%. The required HFT = 1. The subsystem is voted 1oo2.

The system is shown as a Reliability Block diagram in Figure 5.3

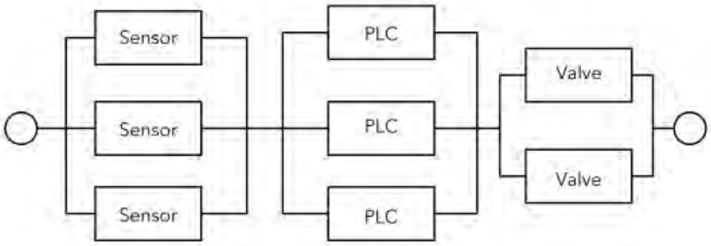


Figure 5.3: RBD system one

5.3.1 Markov modelling

The markov models for each subsystem of **System one** are shown in the Appendix 'Calculations". As we assume the complete SRCS is an ultimate barrier, the models do not include repair rates, nor does it distinguish between DD's and DU's. With the results shown in Tables C.1, C.2

and C.4 of Appendix 'Calculations and results' the PFH_{system} =

$$PFH_{\text{system}} = PFH_{\text{S}} + PFH_{\text{LG}} + PFH_{\text{FE}} \tag{5.17}$$

$$PFH_{\text{system}} = 6.35E-08+1.31E-06+3.65E-07 \tag{5.18}$$

$$PFH_{\text{system}} = 1.7E-06 \tag{5.19}$$

Although system one meets the architectural requirements, the required PFH for a SIL2 is not met. See Table 5.1

Table 5.1: SIL for high demand and continuous safety functions

SIL	PFH
SIL 4	10¯9 to 10¯8
SIL 3	10¯8 to 10¯7
SIL 2	10¯7 to 10¯6
SIL 1	10¯6 to 10¯5

5.4 The SRCF is not the ultimate barrier

If we assume that the SRCF is **not** the ultimate safety barrier, repair of the safety barrier might be possible as the second barrier will bring the machinery into a safe state with a certain probability. In this case the PFH should be calculated from its unavailability $U(t)$. For that same reason, the architectural requirements can be met by using the SFF that includes the DD as safe. This is done for system two.

System two A barrier sequence consists out of SRCF$_{\text{cont.}}$ that is followed by a SIF that acts on demand. The SRCF$_{\text{cont.}}$ is conducted by a SRCS that consists out of three subsystems. The first subsystem consists out of sensors that measure pressure, the second subsystem consist out of a logic solver and the third subsystem consists out of solenoid valves. With the data presented in the Appendix 'Data', the structure of the function is designed to meet SIL2. Note that due to the fact the SRCF$_{\text{cont.}}$ is not the ultimate safety barrier, the SFF that includes the DD as safe, is used to establish the HFT.

- The sensor has a SFF of 77%. The required HFT = 1. The subsystem is voted 1oo2.
- The standard industrial PLC has a SFF of 80%. The required HFT = 1. The subsystem is voted 1oo2.
- The solenoid valve has a SFF of 73%. The required HFT = 1. The subsystem is voted 1oo2.

The system is shown as a Reliability Block diagram in Figure 5.4

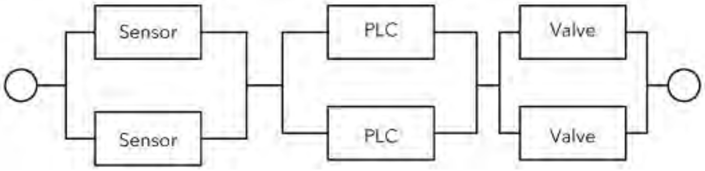


Figure 5.4: RBD system one

Some contemplation

The statement that the repair of the safety barrier might be possible as the second barrier will bring the machinery into a safe state with a certain probability and that for this reason the PFH should be calculated from its unavailability $U(t)$, introduces some food for thought. This statement introduced a certain 'operational' dependency within the barriers. The repair action can only be conducted when the second barrier puts the system into a safe state. As this is not a certain outcome, but a probability, the repair actions can only be conducted with a certain probability. This is expressed in Equation (5.20)

$$\begin{gathered} P(\text{repairing the first barrier when it has failed}) = \\ P(\text{the second barrier does not fail} \mid \text{the first barrier has failed.}) \end{gathered} \tag{5.20}$$

A Markov of the sensor subsystem of system two is shown in Figure 5.5. The markov shows that reaching the safe state (state 6), that allows repair of the system ($\mu_{\text{Repair system}}$), is dependent on the success rate ($\lambda_{\text{Success 2nd}}$) of the succeeding barrier. Although the model visualises the dependency between reaching the safe state and the the possibility of a repair action, the model cannot be used to calculated the PFH. This is due to the fact the process does not qualify as a Markov process. As Rausand and Høyland (2004) explains, a process qualifies as a Markov process if the amount of time it spends in each state, before going to the next state, is exponentially distributed. There is no reason to assume that $\lambda_{\text{Success 2nd}}$ is exponential distributed.

It is clear that configurations such as system two introduce challenges in modelling the reliability of such systems. The 'operational' dependency within the barriers does not only introduce challenges in modelling, it also conflicts with the design method promoted in the ISO12100 framework. The next paragraph will elaborate on this.

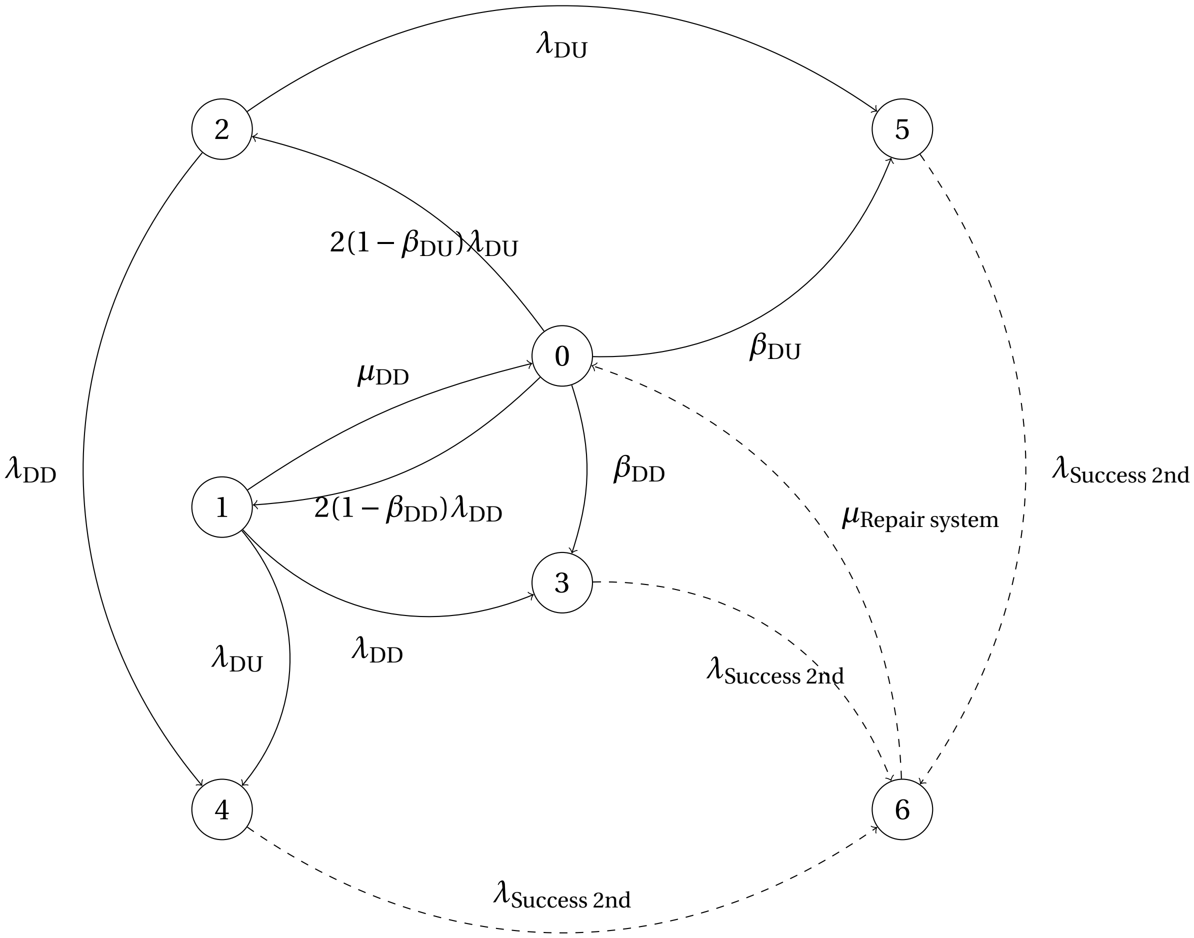

λ_{DU}
2
5
$2(1-\beta_{\text{DU}})\lambda_{\text{DU}}$
0
β_{DU}
μ_{DD}
λ_{DD}
1
$2(1-\beta_{\text{DD}})\lambda_{\text{DD}}$
β_{DD}
$\mu_{\text{Repair system}}$
$\lambda_{\text{Success 2nd}}$
3
λ_{DU}
λ_{DD}
$\lambda_{\text{Success 2nd}}$
4
6
$\lambda_{\text{Success 2nd}}$

Figure 5.5: Markov model of subsystem of system two

Table 5.2: States of system presented in Figure 5.5

State	Description
0	All OK
1	One DD, One OK
2	One DU, One OK
3	All DD
4	One DD, One DU
5	All DU
6	Safe state

Table 5.3: Transitions of system presented in Figure 5.5

Transition	Description
λ_{DD}	Failure rate DD
λ_{DU}	Failure rate DU
β_{DD}	CCF DD
β_{DU}	CCF DU
$\lambda_{\text{Success 2nd}}$	Success rate of succeeding barrier
$\mu_{\text{Repair system}}$	Repair rate of barrier.

5.5 Combining a SRCF and a SIF

Designing a safety barrier sequence, consisting out of a $\text{SRCF}_{\text{cont.}}$ and a safety function that acts on the failure of the SRCF, introduces the following dependencies in the design:

- The structure of a SRECS that conducts a $\text{SRCF}_{\text{cont.}}$ is dependent on the presence of a succeeding barrier. This is due to the fact that the SFF of components can be calculated differently for when they are placed within an ultimate barriers that operates in continuous mode, than for when they are placed within a non-ultimate barrier that operates in continuous mode.

- The PFH, as defined in the applicable standard, of a $\text{SRCF}_{\text{cont.}}$ is dependent on the presence of a succeeding barriers. If it is assumed that a succeeding barrier might put the machinery under control into a safe state, repairing actions of the SRECS can be conducted, if the succeeding barriers function.

The concept of adding safety layers to machinery, as done in the ISO12100 framework, to reduce risk to an acceptable level, might seem as a straight forward concept. But with the dependencies described, the incremental design of safe control systems introduces problems in the design process.This will be made clear by means of example 5.2.

Example 5.2 Let us assume we have a certain basic control system, a SRECS, that conducts a SRCF$_{\text{cont.}}$. If this SRCF$_{\text{cont.}}$ fails a hazardous event occurs. Throughout the design process, conform the IEC 62061, it is assessed that the SRECS should perform at SIL 3. After implementation and verification of the SRCF$_{\text{cont.}}$, it shows that the the SRCF$_{\text{cont.}}$ performs at SIL2. We call this **calculation one**. It is not deemed practical to introduce more SRCFs to reduce the risk of the same hazard. The designer opts for risk reduction by adding a SIF conducted by a SIS. We call this **decision one**. Assessing the risk reduction the SIF needs to perform is done through conducting a LOPA. The LOPA is conducted with the following assumptions:

- The tolerated probability of the hazardous event occurring is within SIL3
- The hazardous event occurs due to failure of the control system. Before decision one was made, it was known that the SRCF$_{\text{cont.}}$ performs at SIL2. Therefore the initial likelihood of the hazardous event occurring is assumed to be equal to the highest bound of SIL2.
- The only barriers in place are 'General design' and the 'Control system'. As failure of each causes the hazardous event, they do not contribute to the risk reduction for the considered hazardous event.

With these assumptions the SIL of the SIF is determined.

Determining the SIL of the new SIF as described in example 5.1 is conform the ISO 12100 framework, but may lead to an inaccurate assessment of the safety integrity of the full barrier sequence. This has two reasons:

1. When **calculation one** is conducted, the SRCF$_{\text{cont.}}$ is the ultimate barrier. After making **decision one**, introducing a second barrier, the SRCF$_{\text{cont.}}$ becomes a non-ultimate barrier. Meaning, that at the time of **calculation one**, the PFH is calculated from SRCF$_{\text{cont.}}$'s unreliability. Once the second barrier is introduced, the PFH of the SRCF$_{\text{cont.}}$ may be calculated from its unavailability. This is due to the fact repair of the SRCF$_{\text{cont.}}$ is made possible.

2. After **decisions one**, it is possible to change the structure of the of the SRECS that conducts the SRCF$_{\text{cont.}}$. This is due to the face that the SFF of the operating components might be calculated differently. This would result into a different system configuration and therefore a different PFH.

This makes that the incremental adding of barriers, as done in the ISO12100 framework, does not fit safety barrier sequences that consist out of at least one SRCF$_{\text{cont.}}$. A fitting approach to this design issue is proposed in Chapter 6 of this report.

5.6 Relation between HEF and SIL

To understand the relation between the SIL requirements for SRCF$_{\text{cont.}}$ and SIL requirements for a safety function that acts on demand, it is of interest to establish the relation between SIL and the Hazardous Event Frequency (HEF). Figure 5.1 shows that a hazardous event can occur when a demand for a safety function is present and a safety function (safety barrier) fails. Rausand et al. (2010) explains that for a safety function operated in demand mode, a hazardous event can occur in two different ways:

1. A demand occurs while the SRCF/SIF has a dangerous fault.

2. A dangerous failure of the the SRECS/SIS occurs while a demand situation is present

When the SRCF/SIF functions in continuous mode, a hazardous event occurs more or less immediately when a dangerous failure of the SRCF/SIF occurs. The consequence of the hazardous event depends on:

1. Whether the SRCF/SIF is the ultimate safety barrier before assets are harmed, or there are other safety barriers that may prevent or mitigate the consequences.

2. Whether or not failures can be detected fast enough to allow the EUC to be brought into a safe state before assets are harmed.

From this, Rausand et al. (2010) deduces that the HEF in case of a safety barrier acts on demand can be given as:

$$HEF = PFD_{\text{avg}} * \lambda_{\text{demand}} \tag{5.21}$$

In which the PFD_{avg} is the average probability of dangerous failure on demand and λ_{demand} represents the demand rate for the safety function.

Assuming a safety function operates in continuous mode and is the ultimate barrier, a hazardous event occurs more or less immediately when the safety function fails. Therefore it is fair to assume that:

$$HEF \approx PFH \tag{5.22}$$

Both the IEC 61508 and the IEC 62061 give the SIL reliability requirements for safety functions that operate in high demand and continuous mode in probability of dangerous failure per hour (PFH). See Table 5.4. For safety functions that act on demands with a lower frequency than once a year, the IEC 61508 gives the SIL reliability requirements in probability of failure on demand (PFD_{avg}). See Table 5.5

Table 5.4: SIL for high demand and continuous safety functions

SIL	PFH
SIL 4	10¯9 to 10¯8
SIL 3	10¯8 to 10¯7
SIL 2	10¯7 to 10¯6
SIL 1	10¯6 to 10¯5

Table 5.5: SIL for low demand safety functions

SIL	PFD
SIL 4	10¯5 to 10¯4
SIL 3	10¯4 to 10¯3
SIL 2	10¯3 to 10¯2
SIL 1	10¯2 to 10¯1

Equations (5.21) and (5.22) make clear there is a fundamental difference between a SIL expressed in PFD, and a SIL expressed in PFH. In case of a SIL for demand mode, the SIL can be interpreted as measure of risk reduction. Whilst, in case of the continuous mode, the SIL can be interpreted as a normative requirement for the maximum allowed HEF.

The HEF after a barrier sequence that consist out of a SRCF$_{\text{cont.}}$ and safety barrier that acts on the failure of the SRCF$_{\text{cont.}}$ is implemented (HEF$_{\text{Barrier sequence}}$), can be expressed as:

$$HEF_{\text{Barrier sequence}} = PFH_{\text{SRCF}_{\text{cont.}}} * PFD_{\text{second barrier}} \tag{5.23}$$

In which the failure of the $\text{SRCF}_{\text{cont.}}$ is a demand for the second barrier. The second barrier fails with a $\text{PFD}_{\text{second barrier}}$. This results in a hazardous event.

As previously discussed, the PFH of the $\text{SRCF}_{\text{cont.}}$ is not independent of the $\text{PFD}_{\text{second barrier}}$. The SIL approach might therefore not be the most fitting approach when designing a barrier sequence consisting out of at least one $\text{SRCF}_{\text{cont.}}$ and succeeding safety barrier.

5.7 Design problems

Designing a barrier sequence consisting out of a $\text{SRCF}_{\text{cont.}}$and SIF's which act on demand, is not as straight forward as it seems. Combining the two safety barriers to achieve the appropriate risk reduction, will lead to problems in the systematic design process as promoted in the ISO 12100 framework. Chapter 6 shows that these problems are caused by the following reasons:

1. There are dependencies when designing safety barrier sequences that consist out of more than one safety barrier of which the first one is a $\text{SRCF}_{\text{cont.}}$. Calculating the PFH of a $\text{SRCF}_{\text{cont.}}$ that is an ultimate barrier is done differently than calculating the PFH of a $\text{SRCF}_{\text{cont.}}$ that is a non-ultimate barrier. Once the designer makes the decision to introduce a second safety barrier, its prior reliability calculations are no longer valid, and shouldn't be used to establish the performance requirements of the succeeding barrier.

2. SIL for functions that operate in continuous mode has a different relation with the HEF than a SIL for functions that act on demand. This makes that the SIL approach, presented in the IEC standards, might not be the most suitable method to establish overall achieved risk reduction of the control system at hand.

Chapter 6

Design solution

Once it is known that the $\text{SRCF}_{\text{cont.}}$ does not reduce the risk to an acceptable level, and it is decided that a second barrier needs to be introduced, engineers will encounter problems that are described in Chapter five.

Instead of the incremental adding of barriers, such as promoted in the ISO 12100 framework, chapter six proposes and integral approach. It explores a solution that assesses the reliability of the full barrier sequence in situations that the sequences consists out of at least one $\text{SRCF}_{\text{cont.}}$. Thus, overcoming the problems with the SIL concept and the modelling of operational dependency. Resulting in a more accurate assessment of the safety integrity of the full barrier sequence.

6.1 HEF instead of SIL

Due to the fact that a SIL for a $\text{SRCF}_{\text{cont.}}$ and a SIL for a SIF that acts on demand have a different meaning, it proposed to abandon the SIL concept for now. Instead of first establishing the SIL of a designed $\text{SRCF}_{\text{cont.}}$ and use this outcome to set the SIL for the SIF, it is proposed to establish the frequency of a certain hazard (HEF) after the full barrier sequence ($\text{SRCF}_{\text{cont.}}$ and $\text{SIF}_{\text{demand.}}$) is introduced. It then can be evaluated if the HEF after the implementation of the barrier sequence meets the acceptable HEF. This approach will make it possible to:

- model the full barrier sequence. This allows for the modelling of the non-technical, but operational dependencies. Such as the introduction of repair actions of the $\text{SRCF}_{\text{cont.}}$ once the succeeding barrier ($\text{SIF}_{\text{demand.}}$) has put the machine into a safe state.

- optimize the availability of the barrier sequence with respect to the test interval of the $\text{SIF}_{\text{demand.}}$.

6.2 modelling the barrier sequence

As discussed and shown in the previous chapter, modelling the reliability of systems consisting out a $\text{SRCF}_{\text{cont.}}$ and a $\text{SIF}_{\text{demand}}$ can not be done by the Markov approach. This is due the dependencies between the possibility of conducting repair actions and the machinery being in a safe state after failure of the $\text{SRCF}_{\text{cont.}}$. A more fitting method of modelling these kinds of systems is the use of Petri-nets. Petri-nets are discussed in the IEC 61508 and author such as Seatzu et al. (2013) give a detail description of their use and possibilities.

To explore how Petri-nets can be used to establish the HEF of a full barrier sequence, we again look at system two that is introduced in chapter five. The system configuration is shown in Figure 6.1. The petri-net method lets us split this system into parts. These are:

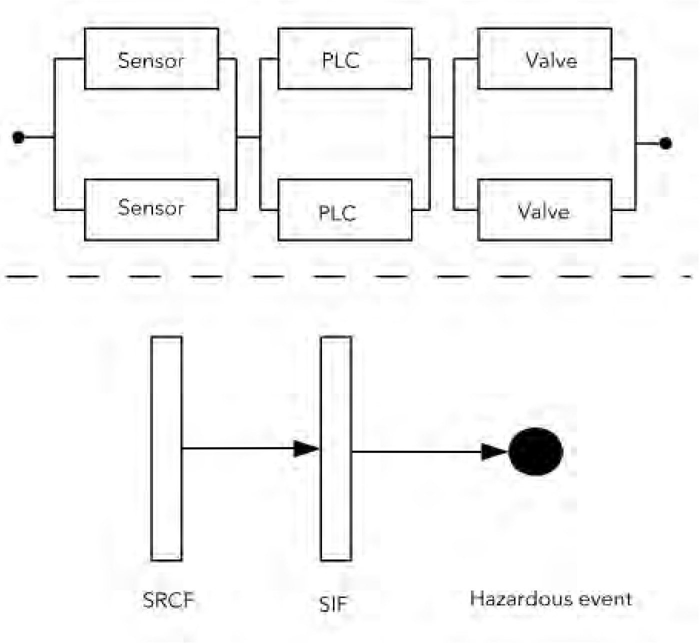


Figure 6.1: System two and full barrier sequence

1. A petri-net of the channels of the voted groups of the $\text{SRCF}_{\text{cont.}}$

2. A petri-net of the voted group of the $\mathrm{SRCF}_{\mathrm{cont.}}$
3. A petri-net of the $\mathrm{SRCF}_{\mathrm{cont.}}$
4. A petri-net of the $\mathrm{SIF}_{\mathrm{demand}}$
5. A petri-net of the interaction between the $\mathrm{SRCF}_{\mathrm{cont.}}$ and the $\mathrm{SIF}_{\mathrm{demand}}$

Petri-net of Channels of 1oo2 group

Figure 6.2 shows a Petri-net of a group voted 1oo2. The legend is shown in Table 6.1 and 6.2. The group consists out of two channels. System two consists out of three groups that are voted 1oo2. When modelling this system, the following assumptions are made:

- Each channel can have a DD **or** a DU failure, but never at the same time. If a channel has a DD, it cannot have a DU until the DD is repaired. If a channel has a DU, it cannot have a DD until the DD is repaired.
- When a DD is detected, repair of the channel is conducted
- A DU can only be repaired when the machine is put into a safe state after the SRCF has failed.

For a full description of all transitions and firing of tokens see Appendix 'Petri-nets'. For now it is sufficient to describe when a channel is in a failed state and the conditions for repair. A channel (a token in $\mathrm{P.Ch_i.f}$) is failed when:

- there is a token in P.DD.f, or
- there is a token in P.DU.f.

A channel can be repaired when:

- there is a token in $\mathrm{P.Ch_i}$, due to $\mathrm{t.DD.ch_i}$. Repair of the DD (firing of $\mathrm{t.r.DD.ch_i}$) is made possible when a token leaves P.DD.f. A token will leave P.DD.f. with the rate of μDD.

- there is a token in P.Ch$_i$, due to t.DU.ch$_i$. Repair of the DU (firing of t.r.DU.ch$_i$) is made possible when a token leaves P.DU.f. A token will leave P.DU.f when there is a token at P.SS.f.SRCF. If there is a token at P.DU.f **and** P.SS.f.SRCF, a token will leave P.DU.f with a rate of μDU.

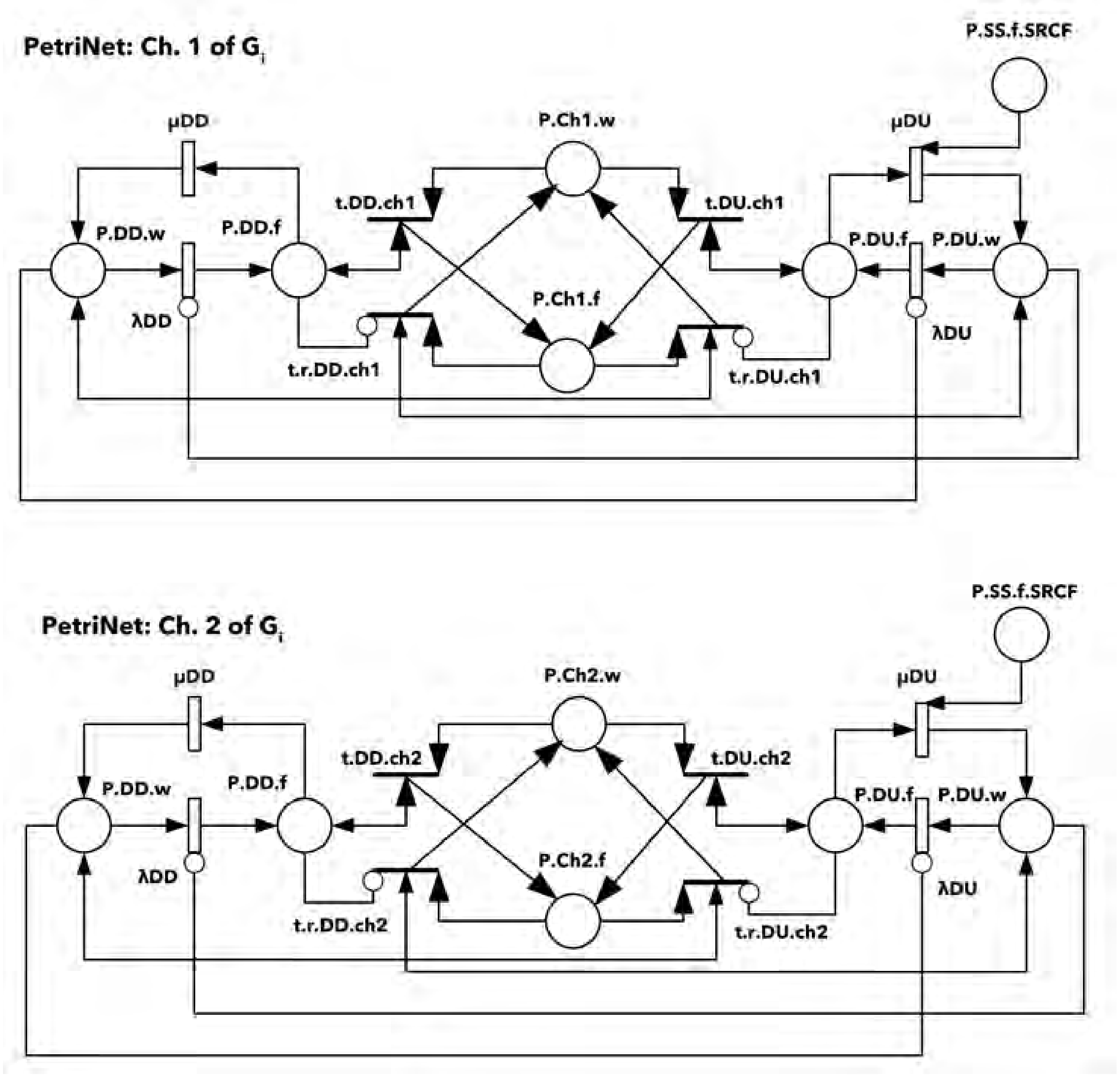


Figure 6.2: Petri-net of channels one and two from 1oo2 Group$_i$, system two

Petri-net of 1oo2 voted group

Knowing the conditions for a failed channel (a token at place P.Ch$_i$) makes it possible the construct a simple petri-net of voted group$_i$ failing. This is shown in Figure 6.3. The legend is shown in Table 6.1 and 6.2. When both P.Ch$_1$.G$_i$.f and P.Ch$_2$.G$_i$.f have a token, t.G$_i$.f will be fired. P.G$_i$.f. will receive a token. Result, G$_i$ has failed.

Table 6.1: Description of Places of the petri-net shown in Figure 6.2

Place	**Description**
P.DD.w	Channel is functioning with respect to the DD.
P.DD.f	Channel has failed with respect to the DD.
P.DU.w	Channel is functioning with respect to the DU.
P.DU.f	Channel has failed with respect to the DU.
$\mathrm{P.Ch_i.w}$	$\mathrm{Channel_i}$ is functioning
$\mathrm{P.Ch_i.f}$	$\mathrm{Channel_i}$ has failed
P.SS.f.SRCF	Machine is in safe state after failure SRCF
$\mathrm{P.Ch_1.G_i.f}$	$\mathrm{Channel_1}$ of the 1oo2 voted $\mathrm{group_i}$ has failed
$\mathrm{P.Ch_2.G_i.f}$	$\mathrm{Channel_2}$ of the 1oo2 voted $\mathrm{group_i}$ has failed
$\mathrm{P.G_i.f}$	Voted $\mathrm{group_i}$ has failed

Table 6.2: Description of Transitions of the petri-net shown in Figure 6.2

Transitions	**Description**
λDD	A DD failure
λDU	A DU failure
μDD	Repair rate DD
μDU	Repair rate DU
$\mathrm{t.DD.ch_i}$	$\mathrm{Ch_i}$ has a DD failure
$\mathrm{t.DU.ch_i}$	$\mathrm{Ch_i}$ has a DU failure
$\mathrm{t.r.DD.ch_i}$	Repair action of DD failure for $\mathrm{Ch_i}$
$\mathrm{t.r.DU.ch_i}$	Repair action of DU failure for $\mathrm{Ch_i}$
$\mathrm{t.G_i.f}$	Voted $\mathrm{group_i}$ failure

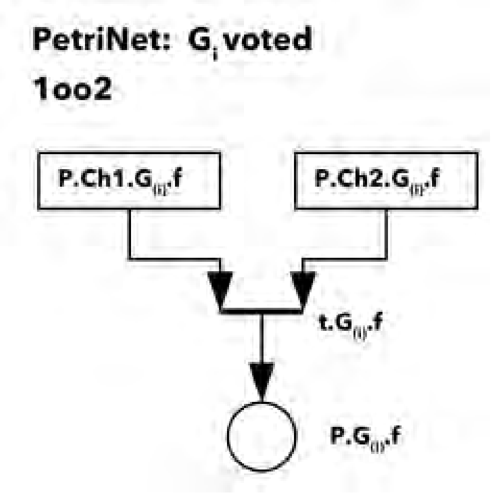


Figure 6.3: Petri-net of a 1oo2 voted group, with results from Figure 6.2

Petri-net of SRCF

As the SRCF$_{\text{cont.}}$ we are discussing consists out of the 1oo2 voted subsystems G$_{\text{sensors}}$, G$_{\text{Logic}}$ and G$_{\text{Final elements}}$, the petri-net of the full SRCF$_{\text{cont.}}$ can be modeled as shown in Figure 6.4. Legend is given in Table 6.3.

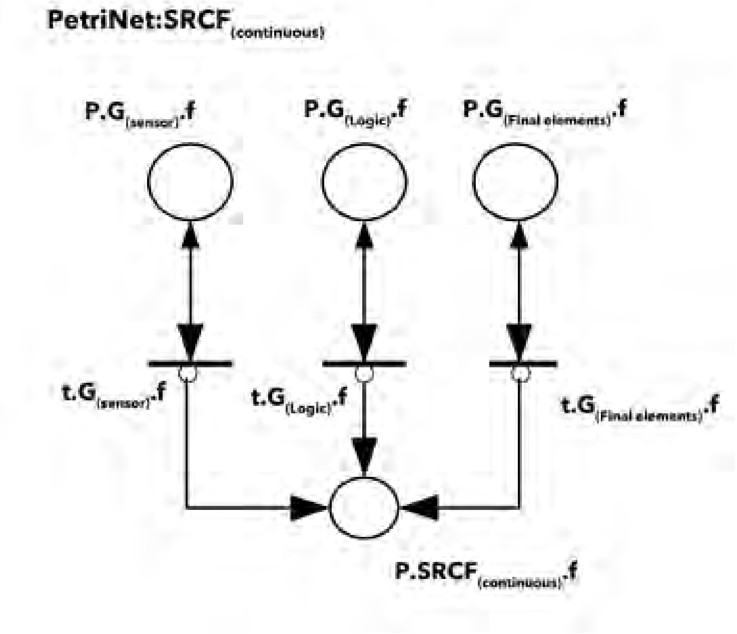

PetriNet:SRCF$_{(\text{continuous})}$
P.G$_{(\text{sensor})}$.f
P.G$_{(\text{Logic})}$.f
P.G$_{(\text{Final elements})}$.f
t.G$_{(\text{sensor})}$.f
t.G$_{(\text{Logic})}$.f
t.G$_{(\text{Final elements})}$.f
P.SRCF$_{(\text{continuous})}$.f

Figure 6.4: Petri-net of a 1oo2 voted group, with results from Figure 6.2

The SRCF$_{\text{cont.}}$ is considert to be failed if one of the three voted groups is in a failed state. Meaning that P.SRCF$_{\text{Continuous}}$ will receive a token if P.G$_{\text{Sensor}}$.f, P.G$_{\text{Logic}}$.f **or** P.G$_{\text{Final elements}}$.f has a token.

Table 6.3: Description of places and transitions of the petri-net shown in Figure 6.4

Place / Transitions	Description
P.G$_{\text{Sensor}}$.f	Voted group$_{\text{sensor}}$ has failed
P.G$_{\text{Logic}}$.f	Voted group$_{\text{logic}}$ has failed
P.G$_{\text{Final elements}}$.f	Voted group$_{\text{Final elements}}$ has failed
P.SRCF$_{\text{Continuous}}$.f	SRCF$_{\text{Continuous}}$ has failed
P.SIF.w	SIF is working
P.SIF.f	SIF has failed
t.G$_{\text{Sensor}}$.f	Failure of group$_{\text{sensor}}$
t.G$_{\text{Logic}}$.f	Failure of group$_{\text{Logic}}$
t.G$_{\text{Final Elements}}$.f	Failure of group$_{\text{Final elements}}$
t.SIF.f	Failure of SIF
t.SIF.r	Repair of SIF

Petri-net of SIF

As the report does not describe a SIF that acts on demand we model a simplified petri-net of the SIF. Only consisting out of a place with the attribute that the SIF is functioning, a place with the attribute that the SIF fails, the failure transition, and a repair transition. This model is shown in Figure 6.5. Legend is given in Table 6.3

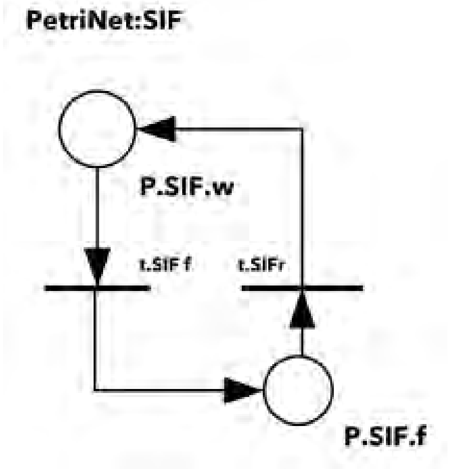


Figure 6.5: Petri-net of SIF

Petri-net of interaction between SRCF and SIF

All the sub systems of the full barrier series are modeled. It is now possible to construct a petri-net of their interaction. This petri net is shown if Figure 6.6. The legend is given in Table **??** A hazard occurs once the SRCF has failed **and** the SIF has failed. In the petri-net the failure of the SRCF is modeled with place P.SRCF.f leading to a demand. If the SIF is functioning at the time of demand, there is no token in place P.Hz.event. Meaning, the machine is put into a safe state after failure of the SRCF (place P.SS). This allows for repair of the SRCF. The system is than reset and the SRCF that is also a production function continues operation.

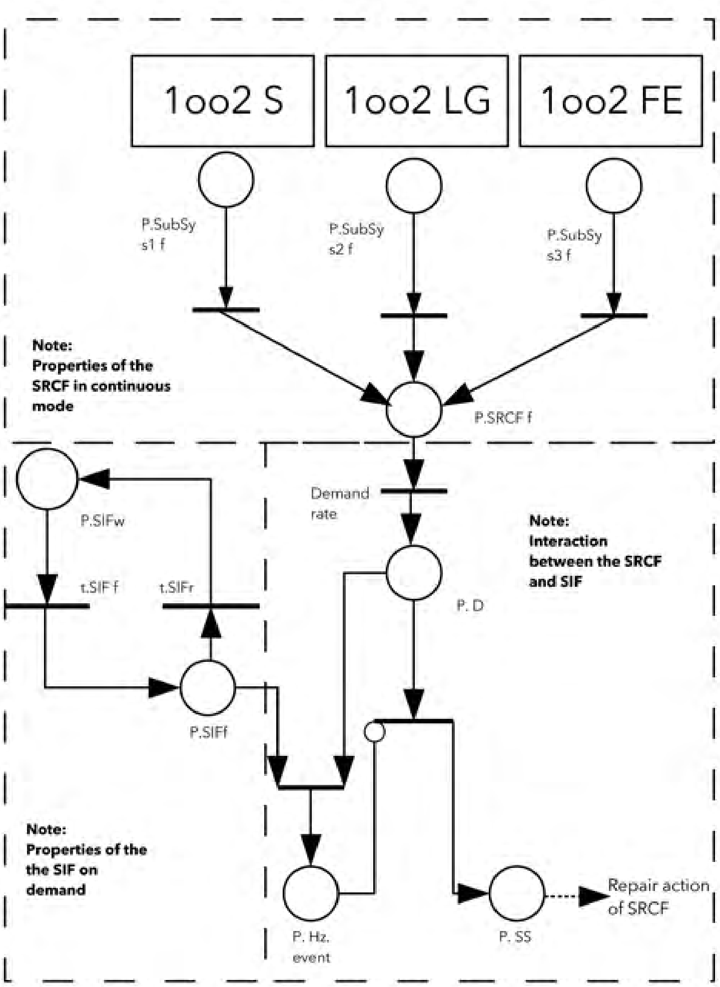


Figure 6.6: Petri-net of interaction between SRCF and SIF

6.3 Simulation

For readability the petri-nets described in paragraph 6.2 are simplified versions of the full model that is used for simulation. Appendix 'Petri-Net' presents a more complex model that is constructed in the modelling program GRIF-petri. The model shows the complete interaction between the separate-petri nets and introduces reset functions that are necessary to conduct repair actions once a 1oo2 voted group has failed.

As stated, the petri-net that describes the $\text{SIF}_{\text{demand}}$ is limited. In the GRIF model, the PFD of the $\text{SIF}_{\text{demand}}$ is simulated with a Monte Carlo simulation. At the moment the model does not include CCF and has not been peer reviewed. The model is therefore not yet completed nor is it validated. Nevertheless, the model shows some interesting and plausible results that are worth discussing.

6.3.1 HEF, PFH and PFD

As explained, it is proposed to not use the SIL concept. As SIL for demand and SIL for continuous mode mean two different things, it decided to model the HEF. A hazardous event occurs when the SRCF fails **and** the SIF fails. In the full Petri-net model this situation occurs when a token reaches the place P.HEF. In this case, the HEF can be found by:

$$HEF = \frac{\text{The amount of tokens P.HEF has received } [0, \tau]}{\tau} \tag{6.1}$$

The PFH of the $\text{SRCF}_{\text{cont.}}$ is equal to the average demand frequency of the $\text{SIF}_{\text{demand}}$. In the model this is represented by the average amount of transitions between the $\text{SRCF}_{\text{cont.}}$ and the $\text{SIF}_{\text{demand}}$. In the model this is transition $tr.299$. The PFH of the $\text{SRCF}_{\text{cont.}}$ can be found by:

$$PFH_{\text{SRCF}_{\text{cont.}}} = \frac{\text{The amount of firing } tr.299 \text{ over } [0,\tau]}{\tau} \tag{6.2}$$

A simulations is conducted. Data used, the GRIFpetri model and full outcome of the simulation is presented in Appendix 'Petri-nets'. The HEF from the simulation of system two:

$$HEF = \frac{3.804E-2}{175200} = 2.17E-7 \tag{6.3}$$

The PFH of the $\text{SRCF}_{\text{cont.}}$ from the simulation:

$$PFH = \frac{0.7621}{175200} = 4.35E-6 \tag{6.4}$$

With a PFD of the $\text{SIF}_{\text{demand}}$ set on $5E-2$ it is possible to control if the model, models the relation between the $\text{SRCF}_{\text{cont.}}$ correctly. This can be done by applying Equation (5.23). This gives:

$$HEF_{\text{overall}} = PFH_{\text{SRCF}} * PFD_{\text{SIF}} \tag{6.5}$$

$$HEF_{\text{overall}} = 4.35E-6 * 5E-2 = 2.17E-7 \tag{6.6}$$

As the outcome of Equation (6.6) and the outcome of the petri-net simulation (Equation (6.3)) are the same, it can be assumed that the model, models the relation between the $\text{SRCF}_{\text{cont.}}$ and the $\text{SIF}_{\text{demand}}$ correctly. This can be verified with varying values of the parameters and check if the outcome will show the same.

6.4 Optimizing availability with respect to the SIF test interval

The introduction of this chapter states that is possible to optimize the availability of the full barrier sequence with respect to the SIF test interval. The petri-net model shown in this report is not yet completed and optimizing is not yet possible. Once the petri-net of the $\text{SIF}_{\text{demand.}}$ is constructed and added, it is possible to vary the test interval during the simulations and find the lowest HEF. This can be researched further at a later moment.

Chapter 7

Summary and Recommendations for Further Work

7.1 Summary and Conclusions

This project had two phases. The first phase was of an exploring nature and had as main objectives to (1) give an introduction to the machinery directive, its structure, and main safety requirements with special focus on requirements regarding safety-related control systems, to (2) give an introduction to functional safety, to (3) present the two competing standards IEC 62061 and ISO 13849, highlighting their similarities and differences, and to (4) present current issues within the design of reliable and safe control system for machinery. The second phase focused on current issues within the design of reliable and safe control systems for machinery. It had as main objectives to (1) give an in-depth analysis of the issue regarding safety-functions that operate in continuous mode and to (2) present concepts and solutions that might be used to resolve the issues regarding safety-functions that operate in continuous mode. The results of the first phase of the project are presented in the first part of the report. The results of the second phase are presented and discussed in the second part of this report.

Part one

The Machinery Directive 2006/42/EC is European legislation that promotes free movement of machinery within the EU and guarantees a high level of protection of the EU workers and citizens. The introduction clarifies that compliance with the Machinery Directive 2006/42/EC is of major influence on the design of machinery. The importance of functional safety and the growing role of control systems in reducing risk are discussed. Relevant standards are mentioned and public sources of European legislation are listed.

A comprehensive literature study into the Machinery Directive 2006/42/EC, the requirements and the compliance process is presented in chapter two. It describes the scope of the directive, a detailed description of the process of compliance and the technical files manufacturers should produce and update. The process of compliance is visualised by a flowchart, presented in Figure 2.4.

Chapter three introduces the harmonised standards and explains the difference between the A,B and C standards. It is stated that at the core of achieving safety of machinery, lies a risk based approach. The main concept of this approach is described in the A-standard ISO 12100:2010; 'Safety of machinery - General principles for design - Risk assessment and risk reduction'. The chapter explains how this standard introduces systematic risk reduction and that the ISO 12100 promotes a hierarchal implementation of (1) inherently safe design measures, (2) safeguarding and complementary protective measures and (3) information for use. A flowchart of the risk assessment process from the ISO 12100 is presented in Figure 3.1. It is concluded that from the ISO 12100 it is clear that safety functions, conducted by control systems, are part of the inherently safe design of machinery.

Chapter four continues with listing the requirements from the Machinery Directive 2006/42/EC for control systems. Standards ISO 13849-1 and IEC 62061 are introduced and a short history of both standards is given. The concept of functional safety is explained. Section 4.3 describes how control systems and safety-related functions are categorized in the different standards. It is concluded that it is not clear whether both standards' definitions of safety-related control systems and functions, have the same meaning. The terms Safety-related part of a control system (SRP/CS), Safety-Related Electrical Control Systems (SRECS) and Safety-related control functions (SRCF) are introduced and explained.

Next, the chapter describes shortly how from the categorization of functions and systems, the concept of continuous mode is derived. A safety function operates in a continuous mode when the safety function retains the machine in a safe state as part of normal operation. The fact a control function can be regarded as safety critical and might be defined as such, has implications for defining integrity requirements for the control function. These implications are discussed in part two of the report.

A short contemplation on risk estimation, the meaning of tolerable risk and required risk reduction is given in section 4.4. This section introduces the concepts of performance levels(PL) and safety integrity levels(SIL). Both concepts, respectively originating from ISO 3849-1 and IEC 61508/62061, are discussed. Points of interest are highlighted by use of examples. It is concluded that, although the standards might show guidance, the designer of the control system needs to asses their applicability on the system at hand.

Chapter four ends with a short comparison of the standards ISO 3849-1 and IEC 62061. It lists possible criteria a manufacturer can base his decision on for selecting which standard to use. It is recommended to select the standard based on the scope of the standards. If the system that is to be designed fits both standards, practical selection criteria can be decisive.

Part two

Part two of this report elaborates on the issue of continuous mode that is highlighted in chapter four. Chapter five starts with the conclusion that the phenomenon of safety- related control functions that operate in continuous mode (SRCF$_{\text{cont.}}$) is underexposed in the standards and the literature. The following issues are discussed in the chapter; (1) design of a SRCF$_{\text{cont.}}$ and establishing its safety integrity, and (2) combining a SRCF$_{\text{cont.}}$ and a SIS that conducts a SIF on demand to achieve sufficient risk reduction.

The reliability measure used in IEC 62061 for SRCF$_{\text{cont.}}$ that needs to meet a certain SIL is expressed in PFH. IEC 62061 defines PFH as *"the probability of a dangerous failure per hour of a safety-related system/subsystem to perform the specified safety function over a given period of time."* With the introduction of the SRECS that conducts a SRCF$_{\text{cont.}}$, meaning the SRECS is a basic control system, a dangerous failure is a failure that terminates the ability of the control system to conduct its SRCF$_{\text{cont.}}$. This definition of a dangerous failure is fundamentally different than dangerous failure of safety functions that act on demand. Chapter five explains how and why this has a major influence on how a system is structured and how the PFH of such a system can be calculated. Section 5.2 explains that due to the definition of dangerous failure, the SFF of components is to be calculated differently than usual. Example 5.1 shows that this results in a higher measure of required redundancy to meet the architectural constraints. The chapter continues with demonstrates how the reliability of a $\text{SRCF}_{\text{cont.}}$ can be calculated with the Markov method.

Next, chapter five discusses how to establish the reliability of a $\text{SRCF}_{\text{cont.}}$ that is placed within a safety barrier sequence and is succeeded by another safety barrier. The $\text{SRCF}_{\text{cont.}}$ is not an ultimate barrier in this sequence. As explained in section 5.4, adding a second barrier that has the possibility to put the machinery in a safe state after the $\text{SRCF}_{\text{cont.}}$ has failed, gives the opportunity to conduct repair actions on the $\text{SRCF}_{\text{cont.}}$. In this case the PFH of the $\text{SRCF}_{\text{cont.}}$ can be calculated from its unavailability. This introduces a certain type of operational dependability, resulting in issues. Besides this, the fact that the $\text{SRCF}_{\text{cont.}}$ is not an ultimate barrier, makes that the SFF can be calculated in the usual manor, altering the structure of the SRECS.

From these findings, the chapter explores the issue of combining a $\text{SRCF}_{\text{cont.}}$ and a SIS that conducts a SIF on demand to achieve sufficient risk reduction. By means of example 5.2 it is explained how the dependencies between a $\text{SRCF}_{\text{cont.}}$ and its succeeding barrier make that the incremental adding of safety barriers (safety functions), such is described in the ISO 12100, ISO 13849 and IEC 62061, leads to design problems.

Another issue regarding combining a $\text{SRCF}_{\text{cont.}}$ and a SIS that conducts a SIF on demand, is caused by the fact the SIL requirements regarding the reliability of a $\text{SRCF}_{\text{cont.}}$ or a safety function that acts on demand, are two different concepts. This is highlighted in section 5.6. This makes it difficult to asses if a barrier sequence consisting out of a $\text{SRCF}_{\text{cont.}}$. and a safety function that acts on demand, meet the required risk reduction expressed in SIL.

With all the design difficulties described in chapter five, chapter six explores a possible design solution. Based on the reasoning that incremental adding of barriers is not suitable when combining a $\text{SRCF}_{\text{cont.}}$ with another safety barrier, an integral approach is proposed. Instead of establishing the reliability of the $\text{SRCF}_{\text{cont.}}$ expressed in SIL, and use this outcome to establish what levels of risk reduction the succeeding barrier needs to deliver, it's recommended to establish the frequency of a hazardous event when the full barrier sequence is implemented ($\text{HEF}_{\text{Barrier sequence}}$).

Once this is known, it can be assessed if the $\text{HEF}_{\text{Barrier sequence}}$ has achieved an acceptable level or if other measures should be implemented. To establish the $\text{HEF}_{\text{Barrier sequence}}$, the full barrier sequence needs to be modelled. It is suggested to construct a Petri-net model. This method allows to incorporate the operational dependency of conducting repair of SRECS that conducts the $\text{SRCF}_{\text{cont.}}$ when the second barrier puts the machine in a safe state. A simplified model that is constructed for a safety barrier sequence consisting out of $\text{SRCF}_{\text{cont.}}$ and safety barrier that acts on demand is shown in section 6.2. A detailed model is constructed and shown in the Appendix 'Petri-nets'. This model is made in GRIFpetri and some initial simulations are conducted.

At the end of the project, the model does not yet include common cause failures nor is it peer reviewed. The model is therefore not completed nor validated. Still, the model shows plausible outcomes and results. The result seem to show that the model is functioning correct. Chapter six ends with the proposition that with a fully validated and complete model it will not only be possible to establish the reliability of the full barrier sequence, but that optimizing the availability with respect to the SIF test interval will also be a possibility. Once the petri-net of the $\text{SIF}_{\text{demand.}}$ is constructed and added, it is possible to vary the test interval during the simulations and find the lowest HEF.

It can be concluded that most of the objectives that were set at the beginning of the project are achieved. One objective that can be researched further is the second objective of the second part; *"present concepts and solutions that might be used to resolve the issues regarding safety-functions that operate in continuous mode"*. The report shows a model that can be seen as a good start towards finding a method to overcome the modelling issues that arise when designing a safety barrier sequence that consists partly out of a SRECS that conducts a $\text{SRCF}_{\text{cont.}}$. Due to limited time and limited experience in modelling Petri-nets, the model has not yet been completed and validated.

7.2 Discussion

Some of the results from the project need to be discussed. These are:

Result: *The report describes and discusses the requirements for machinery and their control system originating from the Machinery Directive 2006/42/EC. It states that compliance with the Machinery Directive 2006/42/EC is of major influence on the design of machinery.*
The requirements from the Machinery Directive 2006/42/EC are not the only requirements from European legislation that have to be met by machinery. It might well be that other European directives are applicable to certain machinery. Examples are:

- The Directive 94/9/EC: This directive covers equipment and protective systems intended for use in potentially explosive atmospheres. It is to be replaced in April 2016 by the ATEX Directive 2014/34/EU.
- The Low Voltage Directive (LVD) 2006/95/EC: This directive ensures that electrical equipment within certain voltage limits provides a high level of protection for European citizens, and benefits fully from the EU's market. To be repealed in 2016 by LVD Directive 2014/35/EU.
- The Electromagnetic Compatibility (EMC) Directive 2004/108/EC: This directive ensures that electrical and electronic equipment does not generate, or is not affected by, electromagnetic disturbance.

Some of these directives dictate requirements that are almost always applicable on machinery. That is why some of these requirements are adopted by standards such at the ISO 138491 and the IEC 62061.

Result: *Manufacturers are free to choose between using ISO 138491 or IEC 62061 during the design of their control systems. It is recommended to select the standard based on the scope of each standard. If the system that is to be designed fits both standards, practical selection criteria can be decisive.*
Both standards are to be merged into one standard, the IEC/ISO 17305. The launch date for IEC

ISO 17305 is planned for 2016, with a transition period of 2 years.

Result: *When adding a second barrier to a $SRCF_{cont.}$ it introduces the possibility that, if the second barrier puts the machine in a safe state, a repair action on the $SRCF_{cont.}$ can be conducted before the hazardous event occurs. Thus, adding of a barrier is likely to increase the safety integrity of the $SRCF_{cont.}$.*

The decision of adding a second barrier is not a decision to take lightly. Many authors recommend to increase the reliability of the first barrier before making the decision to add a succeeding barrier. Common practice is to replace components with more reliable components or add more redundancy. If the first barrier is a $\mathrm{SRCF}_{\mathrm{cont.}}$ adding redundancy might not the best option to increase reliability. As discussed, due to the different calculation of the SFF, a system that conduct $\mathrm{SRCF}_{\mathrm{cont.}}$ already shows more redundancy than systems that conduct safety functions that act on demand. A hight amount of redundancy may make the system less safe. Favoring adding a second barrier.

Result: *SIL requirements regarding the reliability of a $SRCF_{cont.}$ and SIL requirements regarding the reliability of a safety function that acts on demand, are two different concepts. This makes it difficult to asses if a barrier sequence consisting out of a $SRCF_{cont.}$ and a safety function that acts on demand, meet the required risk reduction expressed in SIL. For this reason it is proposed to focus on the $HEF_{\mathrm{Barrier\ sequence}}$. The $HEF_{\mathrm{Barrier\ sequence}}$ can then be compared with the acceptable HEF. The acceptable HEF can be derived from the SIL the initial first barrier ($SRCF_{cont.}$) requires to meet. This is due to the fact that the PFH set for the SIL's for continuous mode, is equal to the maximum allowed HEF.*

The concept of SIL has the advantage that through a risk assessment a SIL can be set for a certain safety function. Besides the reliability requirements, other non-quantifiable requirements are assigned to the different SIL's. Examples are the architectural constrains and requirements regarding safety-related software.

In case of designing a safety barrier sequence, as proposed by the integral approach, the required risk reduction is achieved by a combination of different safety functions. The operational dependencies within the sequence make it difficult to assign a SIL to an individual safety function. It is therefore not possible to assign non-quantifiable requirements to the individual safety function during the design of the barrier sequence. The report does not propose a solution to this problem. More research should be done on this problem

7.3 Recommendations for Further Work

The project has lead to a clear description of problems concerning the design of SRCF's$_{\text{cont.}}$. The proposed integral approach of designing control systems that conduct SRCF's$_{\text{cont.}}$ is not yet complete and more research can be done.

- **Completion and verification of the Petri-net model.** The report presents a Petri-net to model the reliability of a full barrier sequence. The model is yet to be completed and verified. This can be done in the near future. The objectives of this work would be to:

    1. Verify if the Petri-net modelling is a fitting method to assess the reliability of full barrier sequences, and
    2. establish if Petri-net modelling makes it possible to optimize the availability of the barrier sequence with respect to the test interval of the safety function that acts on demand.

- **Non-quantifiable requirements to individual safety functions in the integral approach.** From the discussion it is clear that the proposed integral approach is not yet complete. On the medium-term, work can be done on how to establish which non-quantifiable requirements individual safety functions in a barrier sequence need to meet. This will contribute to developing a method specifically designed to realise safe and reliable control systems that conduct SRCF's$_{\text{cont.}}$.

Appendix A

Acronyms

ALARP As low as reasonable practicable

CCF Common cause failures

CE Conformité Européenne

DC Diagnostic coverage

DD Dangerous detected failure

DOC Declaration of conformity

DU Dangerous undetected failure

EEA European Economic Area

EMC Electromagnetic compatibility

ESD Emergency shut down

EU European union

EUC Equipment under control

GAMAB Globalement au moins aussi bon

HEF Hazardous event frequency

$HEF_{Barrier\ sequence}$ Hazardous event frequency after barrier sequence is implemented

HFT Hardware fault tolerance

IEC International Electrotechnical Commission

ISO International Organization for Standardization

LOPA Layer of protection analysis

LVD Low voltage directive

MTTF Mean time to failure

$MTTF_d$ Mean time to dangerous failure

NTNU Norges teknisk-naturvitenskapelige universitet

PFD Probability of failure on demand

PFH Probability of dangerous failure per hour.

PL Performance level

PL_r Required performance level

PLC Programmable logic controller

RAMS Reliability, availability, maintainability, and safety

RBD Reliability block diagram

SFF Safe failure fraction

SIF Safety-instrumented function

SIL Safety integrity level

SIS Safety-instrumented systems

SRCF Safety-related control function

SRCF$_{\textbf{cont.}}$ Safety-related control function that operates in continuous mode

SRECS Safety-related electrical control systems

SRP/CS Safety-related part of a control system

Appendix B

Data

Data presented in this appendix originates from the Reliability Data for Safety Instrumented System; PDS data Handbook, 2010 Edition.

Table B.1: Failure Data of a pressure transmitter. From

Pressure Transmitter	
Lambda DU	3.00E-07
Lambda DD	5.00E-07
Lambda D	8.00E-07
Lambda SU	4.00E-07
Lambda SD	1.00E-07
Lambda S	5.00E-07
SFF incl. DD as safe	77%
SFF exl. DD as safe	38%
β	4%

Table B.2: Failure Data of a Standard Industrial PLC. From

Standard Industrial PLC			
Analog input		**Logic**	
Lambda DU	7.00E-07	Lambda DU	3.50E-06
Lambda DD	1.10E-06	Lambda DD	5.30E-06
Lambda D	1.80E-06	Lambda D	8.80E-06
Lambda SU	1.40E-06	Lambda SU	7.00E-06
Lambda SD	4.00E-07	Lambda SD	1.80E-06
Lambda S	1.80E-06	Lambda S	8.80E-06
Digital output		**PLC tot.**	
Lambda DU	7.00E-07	Structure	All comp. In series
Lambda DD	1.10E-06		
Lambda D	1.80E-06	Lambda DU	4.90E-06
		Lambda DD	7.50E-06
Lambda SU	1.40E-06	Lambda D	1.24E-05
Lambda SD	4.00E-07		
Lambda S	1.80E-06	Lambda SU	9.80E-06
		Lambda SD	2.60E-06
		Lambda S	1.24E-05
		SFF incl. DD as safe	80%
		SFF exl. DD as safe	50%
		β	7%

Table B.3: Failure Data of a Solenoid valve. From

Solenoid valve	
Lambda DU	8.00E-07
Lambda DD	3.00E-07
Lambda D	1.10E-06
Lambda SU	1.70E-06
Lambda SD	2.00E-07
Lambda S	1.90E-06
SFF incl. DD as safe	73%
SFF exl. DD as safe	63%
β	10%

Appendix C

Calculations and results

This Appendix shows the models and results of the markov appraoch applied on the systems that are described in chapter five. The average state probabilities are calculated by the GRIF program. The PFH is calculated by the formulas presented in chapter five.

C.1 System one

The following calculations are for system one described in chapter five. The system is shown in figure 5.3.

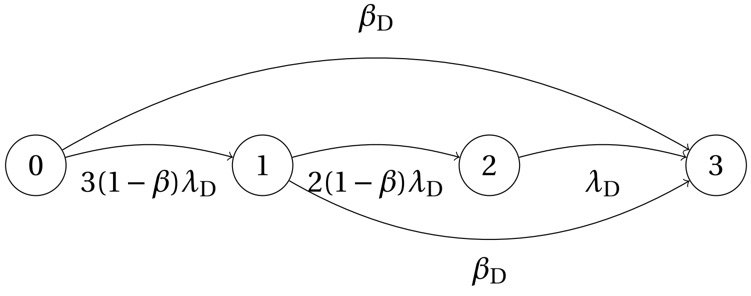


Figure C.1: The markov model for Subsystem Sensor (pressure trans.) and Subsystem Logic (PLC) of System one

Table C.1: Result markov model subsystem sensors for system one

Subsystem:	**Sensor**		
Voted:	**1oo3**		
	Av. Pr.	Rate to failed state	Controbution to PFH(s)
State 0	0.664	3.20E-08	2.13E-08
State 1	0.287	3.20E-08	9.18E-09
State 2	0.041	8.00E-07	3.31E-08
PFH(s)			6.35E-08

Table C.2: Result markov model subsystem Logic for system one

Subsystem:	**plc**		
Voted:	**1oo3**		
	Av. Pr.	Rate to failed state	Controbution to PFH(lg)
State 0	0.670	8.68E-07	5.81E-07
State 1	0.280	8.68E-07	2.43E-07
State 2	0.039	1.24E-05	4.83E-07
PFH(g)			1.31E-06

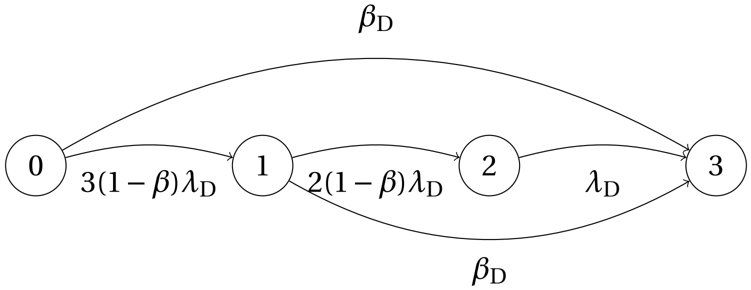


Figure C.2: The markov model for Subsystem Sensor (pressure trans.) and Subsystem Logic (PLC) of System one

Table C.3: Description of states accompanying the markov model shown in Figure C.2

State	Description	Critical
0	All sensors/PLC OK	If CCF
1	One sensor/PC D, two OK	If CCF
2	Two sensors/PLC D, one OK	Yes
3	All sensors/PLC D	Failed

Table C.4: Result markov model subsystem final elements for system one

Subsystem:	**Solenoid valves**		
Voted:	**1oo2**		
	Av. Pr.	Rate to failed state	Controbution to PFH(fe)
State 0	0.693	1.10E-07	7.63E-08
State 1	0.263	1.10E-06	2.89E-07
PFH(g)			3.65E-07

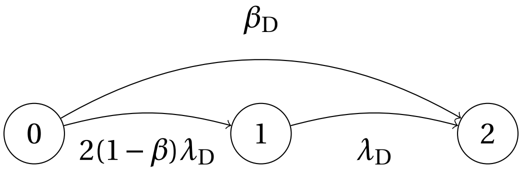


Figure C.3: The markov model for Subsystem Final Element (Solenoid valves) of System one

Table C.5: Description of states accompanying the markov model shown in Figure C.3

State	Description	Critical
0	All valves OK	If CCF
1	One valve D, one OK	Yes
2	Two valves D,	Failed

Appendix D

Petri-nets

This Appendix presents the petri-nets that are constructed in GRIF-petri and are discussed in chapter six.

Table D.1: Data used for simulation

Transitions	**Value**
$\lambda\text{DD}_{\text{sensor}}$	5.00E-07
$\lambda\text{DU}_{\text{sensor}}$	3.00E-07
$\mu\text{DD}_{\text{sensor}}$	0.125
$\mu\text{DU}_{\text{sensor}}$	0.1
$\lambda\text{DD}_{\text{PLC}}$	7.50E-06
$\lambda\text{DU}_{\text{PLC}}$	4.90E-06
$\mu\text{DD}_{\text{PLC}}$	0.125
$\mu\text{DU}_{\text{PLC}}$	0.1
$\lambda\text{DD}_{\text{Valve}}$	3.00E-07
$\lambda\text{DU}_{\text{Valve}}$	8.00E-07
$\mu\text{DD}_{\text{Valve}}$	0.125
$\mu\text{DU}_{\text{Valve}}$	0.1
PFD_{SIF}	5.00E-02

Table D.2: Simulation information

Simulation	
Time(τ)	20 years (175200 hours)
Histories	8E6

Table D.3: Legend of Petri-Net for the subsystems, places

Place	Description
P.DD.w.ch_i	Channel i is working with respect to the DD
P.DD.f.ch_i	Channel i has failed with respect to the DD
P.DU.w.ch_i	Channel i is working with respect to the DU
P.DU.f.ch_i	Channel i has failed with respect to the DU
P.ch_i.w	Channel i is working
P.ch_i .f	Channel i has failed
Group.F	Group (Subsystem) has failed
SS	Machinery is put into Safe State after failure of Group

Table D.4: Legend of Petri-Net for the subsystems, transitions

Transition	Description
DDch_i	Channel i fails with respect to DD with failure rate DD
rr.DD.ch_i	Channel i is repaired with respect to DD, with repair rate DD
DUch_i	Channel i fails with respect to DU with failure rate DU
rr.DU.ch_i	Channel i is repaired with respect to DU, with repair rate DU
DU.F.ch_i	Channel i fails with respect to DU
DD.F.ch_i	Channel i fails with respect to DD
DD.R.ch_i	Channel i is repaired with resect to DD
DU.R.ch_i	Channel i is repaired with respect to DU
f.Group	Group fails

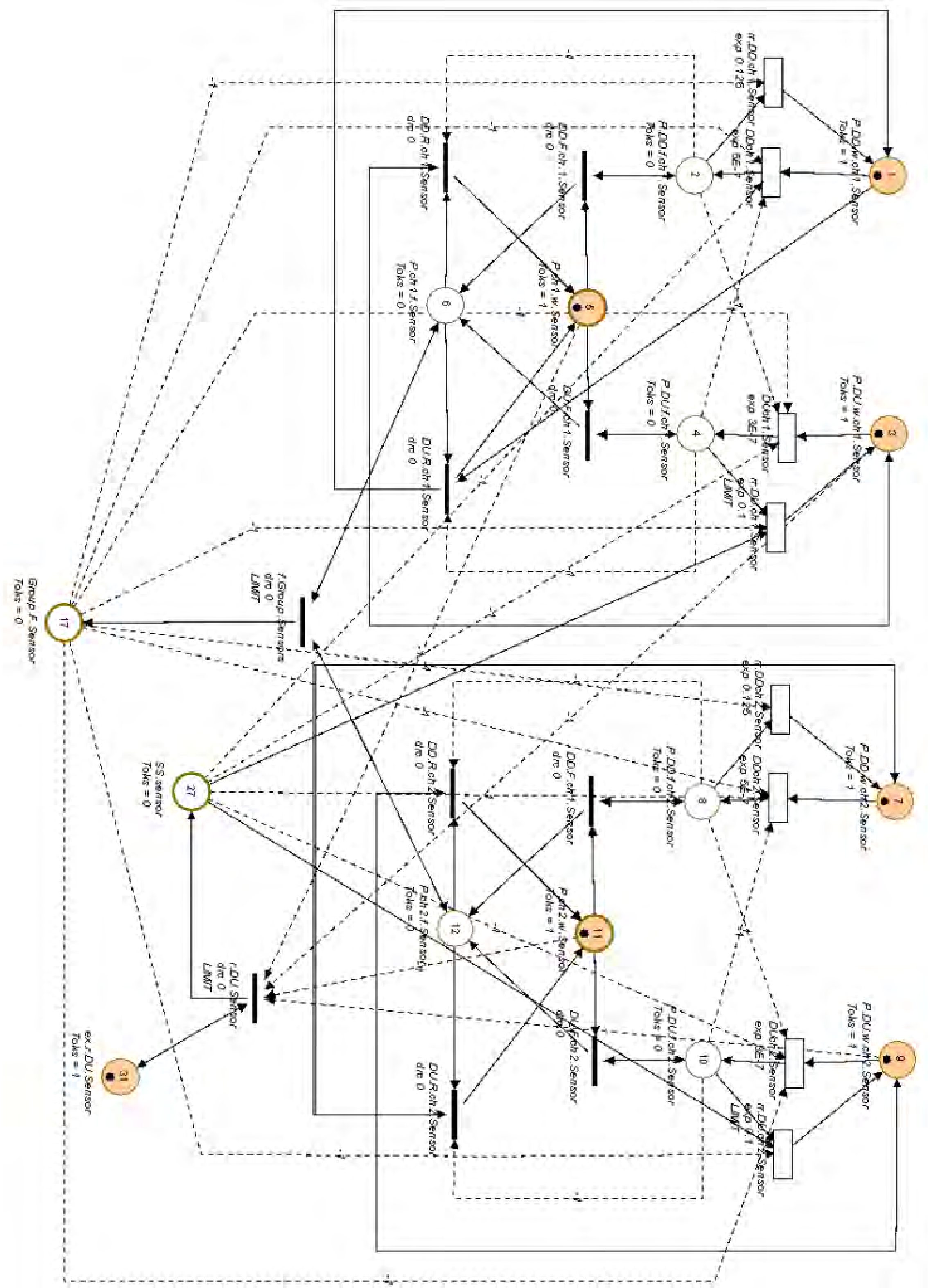


Figure D.1: Petri-net of a 1oo2 voted group, sensor

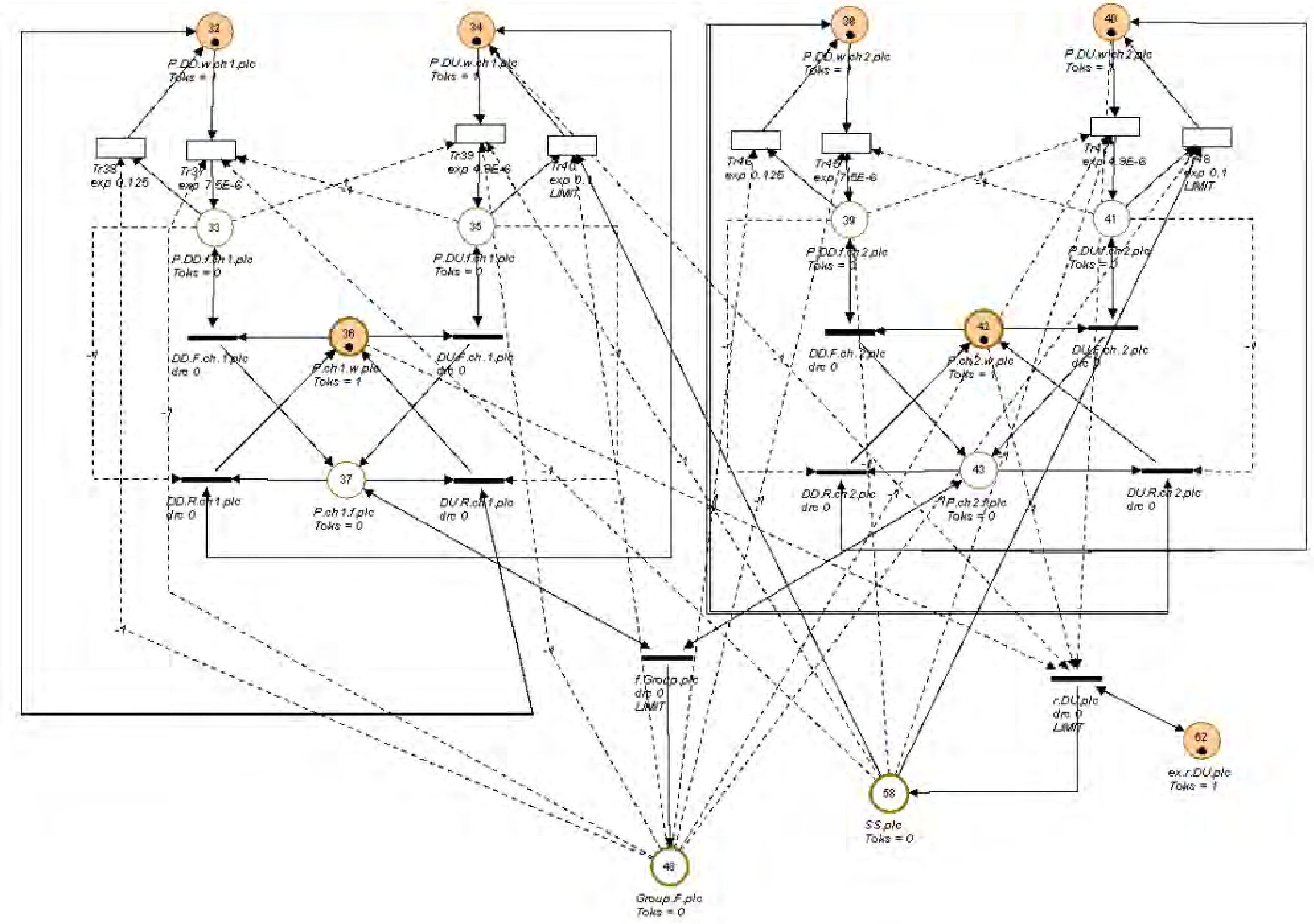


Figure D.2: Petri-net of a 1oo2 voted group, PLC

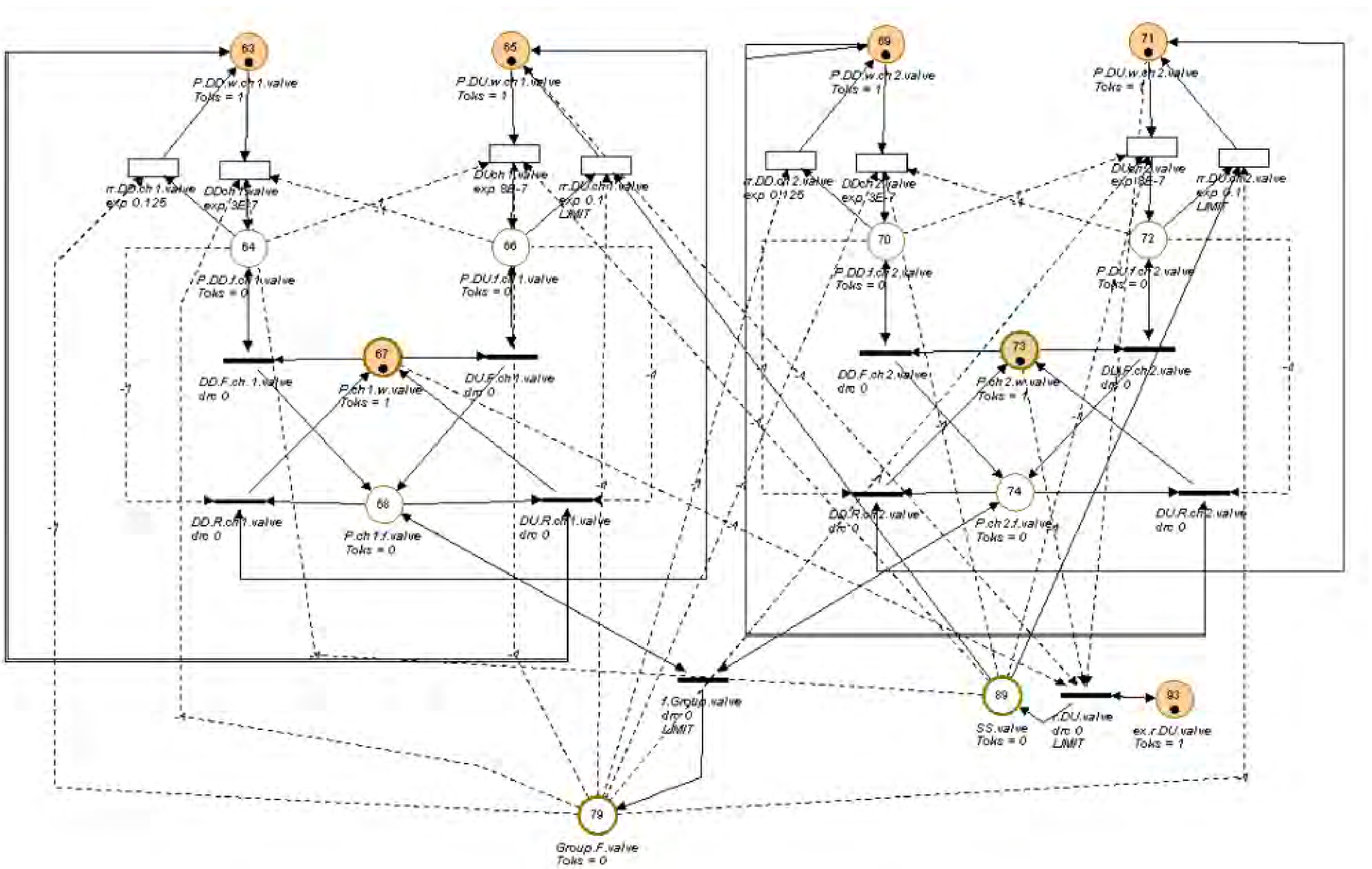


Figure D.3: Petri-net of a 1oo2 voted group, valves

Table D.5: Legend of Petri-Net for the interaction between barriers, places

Place	Description
Pl.138	Subsystem sensors has failed
Pl.137	Subsystem logic has failed
Pl.122	Subsystem valves has failed
Pl.135	SRCP has failed
P.HEF	Hazardous event
Pl.131	Machine is in safe state after failure of the SRCF

Table D.6: Legend of Petri-Net for the interaction between barriers, transitions

Transition	Description
Tr.296	Subsystem sensors fails
Tr.295	Subsystem logic fails
Tr. 381	Subsystem valves fails
Tr. 299	Second barrier fails with certrain probability, fires toke to P.HEF or Pl.131
Tr. 382	Repair of subsystem sensor if machine is put into safe state
Tr. 383	Repair of subsystem logic if machine is put into safe state
Tr. 385	Repair of subsystem valve if machine is put into safe state

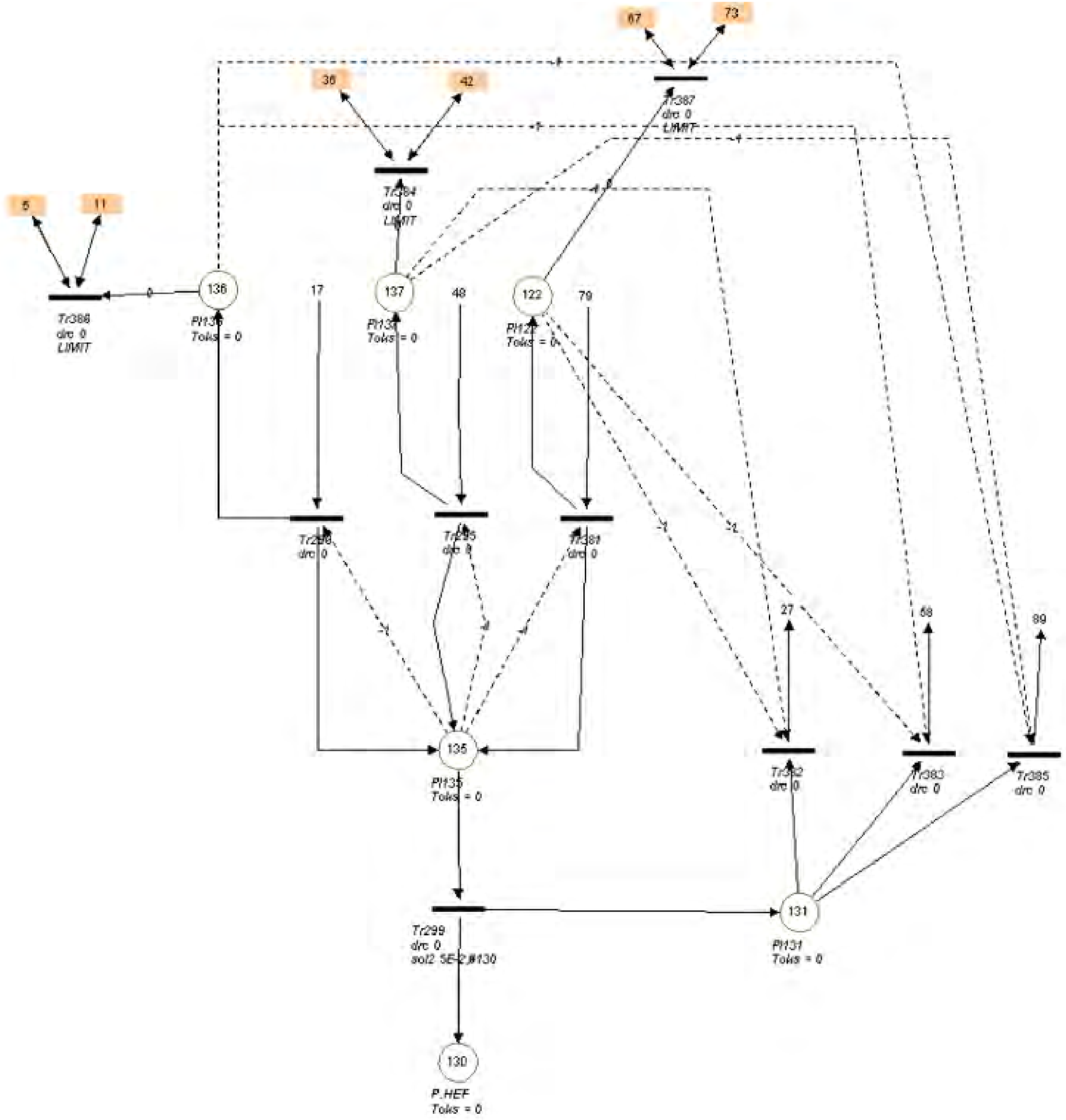


Figure D.4: Petri-net of interaction between subsystems. (Incl. PFD SIF)

Table D.7: Result of simulation, places

Name	Number	Sojourn Time	σ (Sojourn Time)	Average token number	σ (Average)	Token number at end of history	σ (end of history)
P.DD.w.ch1.Sensor	1	175199.3175	3.301627118	0.999996104	1.88449E-05	0.9999965	0.001870826
P.DD.f.ch1.Sensor	2	0.682524624	3.301627118	3.89569E-06	1.88449E-05	0.0000035	0.001870826
P.DU.w.ch1.Sensor	3	170928.5541	21764.39155	0.975619601	0.124225979	0.953083	0.211461109
P.DU.f.ch1.Sensor	4	4271.445903	21764.39155	0.024380399	0.124225979	0.046917	0.211461109
P.ch1.w.Sensor	5	170927.8716	21764.30578	0.975615705	0.12422549	0.9530795	0.211468608
P.ch1.f.Sensor	6	4272.128427	21764.30578	0.024384295	0.12422549	0.0469205	0.211468608
P.DD.w.ch2.Sensor	7	175199.3166	3.308489664	0.999996099	1.88841E-05	0.999996375	0.00190394
P.DD.f.ch2.Sensor	8	0.683437053	3.308489664	3.9009E-06	1.88841E-05	3.625E-06	0.00190394
P.DU.w.ch2.Sensor	9	170928.1759	21766.01416	0.975617443	0.124235241	0.95307725	0.211473429
P.DU.f.ch2.Sensor	10	4271.824064	21766.01416	0.024382557	0.124235241	0.04692275	0.211473429
P.ch2.w.Sensor	11	170927.4925	21765.9284	0.975613542	0.124234751	0.953073625	0.211481195
P.ch2.f.Sensor	12	4272.507501	21765.9284	0.024386458	0.124234751	0.046926375	0.211481195
Group.F.Sensor	17	0	0	0	0	0	0
SS.sensor	27	0.260136521	144.3525002	1.89847E-06	0.00115014	0.000004	0.002345205
ex.r.DU.Sensor	31	175200	0	1	0	1	0
P.DD.w.ch1.plc	32	175191.2554	12.064051	0.999950088	6.88587E-05	0.999956375	0.006604779
P.DD.f.ch1.plc	33	8.744623694	12.064051	4.99122E-05	6.88587E-05	0.000043625	0.006604779
P.DU.w.ch1.plc	34	145693.1244	43253.9629	0.83158176	0.24688335	0.777898	0.415659384
P.DU.f.ch1.plc	35	29506.87565	43253.9629	0.16841824	0.24688335	0.222102	0.415659384
P.ch1.w.plc	36	145684.3797	43251.5876	0.831531848	0.246869792	0.777854375	0.415688547
P.ch1.f.plc	37	29515.62027	43251.5876	0.168468152	0.246869792	0.222145625	0.415688547
P.DD.w.ch2.plc	38	175191.2635	12.05857163	0.999950134	6.88275E-05	0.999954625	0.006735944
P.DD.f.ch2.plc	39	8.73653111	12.05857163	4.9866E-05	6.88275E-05	0.000045375	0.006735944
P.DU.w.ch2.plc	40	145708.3601	43225.26777	0.831668722	0.246719565	0.77808175	0.415536475
P.DU.f.ch2.plc	41	29491.63989	43225.26777	0.168331278	0.246719565	0.22191825	0.415536475
P.ch2.w.plc	42	145699.6236	43222.89872	0.831618856	0.246706043	0.778036375	0.415566837
P.ch2.f.plc	43	29500.37642	43222.89872	0.168381144	0.246706043	0.221963625	0.415566837
Group.F.plc	48	0	0	0	0	0	0
SS.plc	58	19.60899632	1150.031098	0.000123487	0.007044537	0.000206375	0.015710902
ex.r.DU.plc	62	175200	0	1	0	1	0
P.DD.w.ch1.valve	63	175199.6048	2.513019188	0.999997745	1.43437E-05	0.999997625	0.001541102
P.DD.f.ch1.valve	64	0.395153989	2.513019188	2.25545E-06	1.43437E-05	0.000002375	0.001541102
P.DU.w.ch1.valve	65	164625.6362	33343.34118	0.939644042	0.190315874	0.8878325	0.315572439
P.DU.f.ch1.valve	66	10574.36376	33343.34118	0.060355958	0.190315874	0.1121675	0.315572439
P.ch1.w.valve	67	164625.2411	33343.26211	0.939641787	0.190315423	0.887830125	0.315575358
P.ch1.f.valve	68	10574.75891	33343.26211	0.060358213	0.190315423	0.112169875	0.315575358
P.DD.w.ch2.valve	69	175199.6043	2.516587252	0.999997741	1.43641E-05	0.999996875	0.001767764
P.DD.f.ch2.valve	70	0.395730768	2.516587252	2.25874E-06	1.43641E-05	0.000003125	0.001767764

Table D.8: Cont. result places of Table D.7

Name	Number	Sojourn Time	σ (Sojourn Time)	Average token number	σ (Average)	Token number at end of history	σ (end of history)
P.DU.w.ch2.valve	71	164616.9609	33345.88576	0.939594526	0.190330398	0.887720875	0.315709575
P.DU.f.ch2.valve	72	10583.0391	33345.88576	0.060405474	0.190330398	0.112279125	0.315709575
P.ch2.w.valve	73	164616.5652	33345.80711	0.939592267	0.190329949	0.88771775	0.315713412
P.ch2.f.valve	74	10583.43483	33345.80711	0.060407733	0.190329949	0.11228225	0.315713412
Group.F.valve	79	0	0	0	0	0	0
SS.valve	89	0.607560995	178.2925979	5.20627E-06	0.001957785	0.000012	0.005147801
ex.r.DU.valve	93	175200	0	1	0	1	0
Pl122	122	78.96723914	2580.130897	0.000457615	0.015070882	0.0013895	0.038151926
P.HEF	130	2652.205423	16039.4829	0.015490047	0.094814902	0.0380405	0.197517531
Pl131	131	32.54860485	1491.545985	0.000265552	0.013944095	0.001151	0.04817339
Pl135	135	0	0	0	0	0	0
Pl136	136	24.16805559	1430.429695	0.000139611	0.008301548	0.00043175	0.0211557
Pl137	137	1584.678131	10652.83133	0.0093276	0.064163749	0.0189035	0.144314449

Table D.9: Result of simulation, transitions

Name	ID	Number of triggers during period	Name	ID	Number of triggers during period	Name	ID	Number of triggers during period
DDch1.Sensor	1	0.085426375	Tr40	40	0.491627125	DD.R.ch1.valve	79	0.068933125
rr.DD.ch1.Sensor	2	0.085422875	DU.F.ch.1.plc	41	0.713729125	DU.R.ch1.valve	80	0.0845432125
DUch1.Sensor	3	0.05139325	DD.F.ch.1.plc	42	1.09297325	DDch2.valve	81	0.049426375
rr.DU.ch1.Sensor	4	0.00447625	DD.R.ch1.plc	43	1.58455675	rr.DD.ch2.valve	82	0.04942325
DU.F.ch1.Sensor	5	0.05139325	DU.R.ch1.plc	44	0.04139521	DUch2.valve	83	0.1317465
DD.F.ch.1.Sensor	6	0.085426375	Tr45	45	1.091777125	rr.DU.ch2.valve	84	0.019467375
DD.R.ch1.Sensor	7	0.089899125	Tr46	46	1.09173175	DU.F.ch2.valve	85	0.1317465
DU.R.ch1.Sensor	8	0.08236325	Tr47	47	0.71391025	DD.F.ch2.valve	86	0.049426375
DDch2.Sensor	9	0.085466875	Tr48	48	0.491992	DD.R.ch2.valve	87	0.068890625
rr.DDch2.Sensor	10	0.08546325	DU.F.ch.2.plc	49	0.71391025	DU.R.ch2.valve	88	0.065840514
DUch2.Sensor	11	0.051391625	DD.F.ch.2.plc	50	1.091777125	f.Group.valve	97	0.023376625
rr.DU.ch2.Sensor	12	0.004468875	DD.R.ch2.plc	51	1.58372375	r.DU.valve	108	0.01703875
DU.F.ch2.Sensor	13	0.051391625	DU.R.ch2.plc	52	0.723459254	Tr295	295	0.731896375
DD.F.ch1.Sensor	14	0.085466875	f.Group.plc	61	0.731896375	Tr296	296	0.006829375
DD.R.ch2.Sensor	15	0.089932125	r.DU.plc	72	0.28923325	Tr299	299	0.762102375
DU.R.ch2.Sensor	16	0.076943642	DDch1.valve	73	0.049444625	Tr381	381	0.023376625
f.Group.Sensors	25	0.006829375	rr.DD.ch1.valve	74	0.04944225	Tr382	382	0.006387125
r.DU.Sensor	36	0.002562	DUch1.valve	75	0.131658375	Tr383	383	0.69459225
Tr37	37	1.09297325	rr.DU.ch1.valve	76	0.019490875	Tr384	384	4.0684595
Tr38	38	1.092929625	DU.F.ch1.valve	77	0.131658375	Tr385	385	0.0219315
Tr39	39	0.713729125	DD.F.ch.1.valve	78	0.049444625	Tr386	386	8.100256
						Tr387	387	7.4797255

Bibliography

Baybutt, P. (2007). An improved risk graph approach for dermination of safety integrity levels. *Process Safety Progress*, 26(1).

EN-ISO13849-1 (2006). *EN ISO 13849-1 Safety of machinery: Safety-related parts of control systems - part one.*

Hauge, S., Hokstat, P., and Corneliussen, K. (2013). *Reliability prediction method for safety instrumented systems: PDS method handbook.* SINTEF Technology and Society, Safety Research.

IEC-61508 (2010). *IEC-61508 "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems".*

IEC-62061 (2006). *IEC-62061 "Safety of machinery: Functional safety of electrical, electronic and programmable electronic control systems".*

ISO-12100:2010 (2010). *ISO 12100:2010 'Safety of machinery - General principles for design - Risk assessment and risk reduction'.*

ISO/TR18569 (2004). *Safety of Machinery - Guidelines for the understanding and use of safety of machinery standards.*

Lundteigen, M. A. and Rausand, M. (2009). Architectural constraints in iec 61508: Do they have the intended effect? *Reliability Engineering and System Safety.*

Nait-Said, R., Zidani, F., and Ouzraoui, N. (2008). Fuzzy risk graph model for dermining safety integrity level. *International Journal of Quality, Statistics, and Reliability.*

Rausand, M. (2011). *Risk assessment: theory, methods, and applications.* Wiley, Hoboken, NJ.

Rausand, M. (2014). *Reiability of Safety-Critical Systems: Theory and Applications*. Wiley, Hoboken, NJ.

Rausand, M. and Høyland, A. (2004). *System Reliability Theory: Models, Statistical Methods, and Applications*. Wiley, Hoboken, NJ, 2nd edition.

Rausand, M., Jin, H., and Lundteigen, M. A. (2010). Reliability performance of safety instrumented systems: A common approach for both low- and high-demand mode of operation. *Reliability Engineering and System Safety*.

Rockwell (2011). *Safebook 4*. Rockwell Automation.

Seatzu, C., Silva, M., and van Schuppen, J. (2013). Control of discrete-event systems. Springer.