NTNU – Trondheim
Norwegian University of
Science and Technology

Reliability assessments of railway signaling systems: A comparison and evaluation of approaches

Lichao Tang

Safety, Health and Environment
Submission date: June 2015
Supervisor: Eirik Albrechtsen, IØT
Co-supervisor: Mary Ann Lundteigen, Institutt for produksjons- og kvalitetsteknikk
Terje Sivertsen, Jernbaneverket

Norwegian University of Science and Technology
Department of Industrial Economics and Technology Management

Problem Description

Railway signaling systems are used to ensure the safe operation of railway traffic. Such signaling systems have evolved from purely relay-based systems (e.g. NSI-63, NSB-84) to computerized systems (e.g., NSB-94 and Merkur). Signaling systems may be designed to accommodate large stations with multiple tracks, like Oslo S, or smaller two-track stations, with single entry and departure track. The main focus on this master thesis is devoted to the latter, as most stations in Norway are of this type.

It is vital to demonstrate that the reliability and availability of railway signaling systems are according to railway authority regulations, and references standards such as EN 50126, EN 50128, and EN 50129. The last mentioned standards were introduced after NSB-94 was put into operation, which means that some of the prevailing requirements were not fully adapted. One example is the compilation of a technical safety report, to document the reliability performance and compliance against EN 50129.

The main purpose of this master thesis is to suggest an approach for developing the technical safety report in accordance with EN 50129, with focus on the steps necessary to carry out a reliability assessment. The approach is based on a review of how such assessments have been carried out in the past, also utilizing experience from reliability assessments carried out before the compilation of a technical safety report became mandatory.

Detailed tasks:

1. Define and describe what are the main safety-critical functions in relation with signaling systems, supported by functional block diagrams that identify the most important components.

2. Identify and explain requirements for setting reliability targets and assessing reliability of the functions, with basis in the mentioned standards.

3. Identify and describe the main content of a technical safety report, in light of regulatory requirements and the EN standards, and explain the relationship between technical safety reports generated for a generic product, generic application, and a specific application.

4. Document and discuss previous adoptions of the requirements, with basis in previously

developed technical safety reports. Elaborate in particular on the methods used to quantify the reliability of the individual functions, and the data to support the analyses.

5. Propose an approach for developing a technical safety report, including the methods, data, and other input (e.g., documentation) at each step.

6. Demonstrate the application of the approach by using a case study for one selected safety-critical function (e.g. setting green light signal).

Preface

This master project is written for TIØ4925 - Health, Safety and Environment, Master's Thesis at Norwegian University of Science and Technology (NTNU) spring 2015. This project was written in cooperation with Norwegian National Rail Administration.

Railway signaling systems are used to ensure the safe operation of railway traffic. Such signaling systems have been evolved from purely relay-based systems to computerized systems. It is important to demonstrate that the reliability and availability of railway signaling systems are according to railway authority regulations, and reference standards such as EN 50126, EN 50128 and EN 50129. Those standards were introduced after NSB-94 had been put into operation, which means that some of the prevailing requirements were not fully adopted. One example is the compilation of a technical safety report, which is to document the reliability performance and compliance against EN 50129.

The main purpose of this master thesis is to suggest an approach for developing the technical safety report in accordance with EN 50129, with focus on the steps necessary to carry out a reliability assessment. The approach is based on a review of how such assessments have been carried out in the past, also utilizing experience from reliability assessments carried out before the compilation of a technical safety report became mandatory.

Trondheim, 2015-06-11

Lichao Tang

Acknowledgment

First of all, I would like to express sincere gratitude to Professor Mary Ann Lundteigen for her aspiring guidance, invaluably constructive criticism and friendly advice during this master thesis. I would like to thank Terje Sivertsen, who provided an oppturnity for writing this thesis for Norwegian National Rail Administration. Terje has years of extensive experience of signaling systems. During my visit to Norwegian National Rail Administration, he provided me with valuable suggestions on my thesis. Without his help, I could not finish my thesis. I am also grateful to Geir Melting, who helped me a lot on finding relevant documents.

Finally, I would like to thank my family for grateful support during my whole study. Their encouragement made me never feel lonely when I spent seven years aboard.

LC.T

Summary and Conclusions

The railway signaling system is the key system to ensure the safe operation of railway traffic. It is therefore important to have a safe and reliable railway signaling system. The railway authority defines requirements that should be complied with. The technical safety report is a vital documentation for the demonstration of fulfillment of requirements to the railway authority.

A literature review of the signaling system is presented first. It describes the different technologies used for railway signaling system. Moreover, challenging problems in the design of two track station, based on the situations in Norway, were discussed. In addition, some relevant regulations and standards were introduced.

Further, safety-critical functions performed by a signaling system were presented. The methods for determination of tolerable hazard rate, which is the safety requirements for safety-critical functions, were introduced. These methods distinguished two different demand modes, i.e., low-demand mode and high-demand mode.

It described different roles and responsibilities involved for the whole signaling system life cycle. As a safety case is a product from one phase of system life cycle, a brief introduction to safety case was presented. The discussion of differences among three categories of safety cases was followed. The structure of technical safety report and the different categories of technical safety reports were described.

Two technical safety reports from Norwegian National Rail Administration were evaluated in the light of the requirements from EN 50129. In particular, the reliability measures of safety-critical functions that were presented in the reports were discussed in this thesis. Some examples of inadequacy from these technical safety reports were discussed. An approach for improving the inadequacy was proposed.

Finally, it performed a fault tree analysis as a comparison with the method used in the technical safety report.

Contents

Chapter 1

Introduction

1.1 Background

Railway signaling system is a safety-related electronic system that is used to ensure the safe operation of railway traffic. To guarantee that a railway signaling system is safe, CENELEC published standard EN 50129 defining requirements for acceptance and approval of safety-related electronic systems in the railway signaling field.

EN 50129 requires demonstrating system safety tughhrough the safety case. In order for a signaling system to be put into operation, related safety cases needs to be accepted by the relevant safety authority through a formal approval process. One important part of this Safety Case is the technical safety report. The technical safety report shall include technical evidence for the safety of the design. It is required in EN 50129 to document how the hardware design achieves the required integrity in respect of reliability.

There were some signaling systems that had been put into operation before EN 50129 was introduced, which means that some of the prevailing requirements were not fully adopted. Even if it is not required to prepare a technical safety report retrospectively for an existing installation, different types of technical safety reports were prepared for NSB-94 which is a most used signaling system in Norway. There are also other technical safety reports prepared for another signaling system Merkur, which is developed based on the concept of NSB-94. These technical safety reports were developed after EN 50129 had been introduced. It is interesting to compare how these technical safety reports developed for different signaling systems that had been put into

operation before and after the introduction of EN 50129, particularly, how reliability assessment were carried out in these technical safety reports.

1.2 Motivation

Over 40,000 Norwegians affected every day by average 223 trains which are either delayed or suspended(NTB, 2015). One of most common reasons is 13.129 delays were caused by failures in signaling system, interlocking system or remote control and 2,804 trains were entirely suspended for the same reasons (NTB, 2015).

As much of the signaling system in Norway is reaching its technical service life, it is decided to renew the Norwegian railway signaling system by adopting the European Rail Traffic Management System (ERTMS) in period 2015 - 2030.

To ensure that the new signaling system is safe to be put into use, it is vital to demonstrate the safety of design to the safety authority which approves the signaling system. The experience from previous demonstration of safety may be a valuable treasure for developing technical safety reports for the new signaling system. Identified issues from previous technical safety reports shall be avoided in the future.

1.3 Objectives

The main objectives of this Master's project are

1. Define and describe what are the main safety-critical functions in relation with signaling systems, supported by functional block diagrams that identify the most important components.

2. Identify and explain requirements for setting reliability targets and assessing reliability of the functions, with basis in the mentioned standards.

3. Identify and describe the main content of a technical safety report, in light of regulatory requirements and the EN standards, and explain the relationship between technical safety reports generated for a generic product, generic application, and a specific application.

4. Document and discuss previous adoptions of the requirements, with basis in previously developed technical safety reports. Elaborate in particular on the methods used to quantify the reliability of the individual functions, and the data to support the analyses.

5. Propose an approach for developing a technical safety report, including the methods, data, and other input (e.g., documentation) at each step.

6. Demonstrate the application of the approach by using a case study for one selected safety-critical function (e.g. setting green light signal).

1.4 Limitations

In this study the Norwegian signaling system is used as an example. The two technical safety reports evaluated were developed for two types of signaling systems. NSB-94 had been put into operation before EN 50129 was introduced. The technical safety report was developed therefore retrospectively. Back to that time, people did not have much experience of preparing such documentation. The content of the report may be not deep enough. Regarding to reliability assessment of NSB-94, it referred a document that may include some information about this. However, it could not be found at the time the author writing this thesis. It is therefore difficult to compare how reliability assessments were carried out in two technical safety reports.

Ideally, it is better to compare the same type of technical safety reports at the same time. In such way, man may identify pros and cons of the way developing technical safety report from the same type of technical safety reports. However, it evaluated two different types of technical safety reports for different signaling systems.

When evaluating technical safety reports, it was difficult to understand some contents in the reports since it might require some experience in preparing such reports. It may not consider thoroughly when evaluating these reports.

1.5 Structure of the Report

The rest of the report is structured as follows:

- Chapter 2 gives an introduction to the railway signaling system.
- Chapter 3 discusses relevant reliability concepts.
- Chapter 4 describes different roles and responsibilities involved for a signaling system life cycle and gives an introduction to the safety case.
- Chapter 5 gives an introduction to the technical safety reports and discusses the relationship between technical safety reports generated for a generic product, a generic application, and a specific application.
- Chapter 6 evaluates two technical safety reports and elaborates on the methods used to quantify the reliability of the safety-critical functions.
- Chapter 7 proposes an approach for developing a technical safety report.
- Chapter 8 performs a fault tree analysis as a comparison with the method used in the technical safety report.
- Chapter 9 presents the summary and conclusions for this thesis and makes some recommendations for future work.

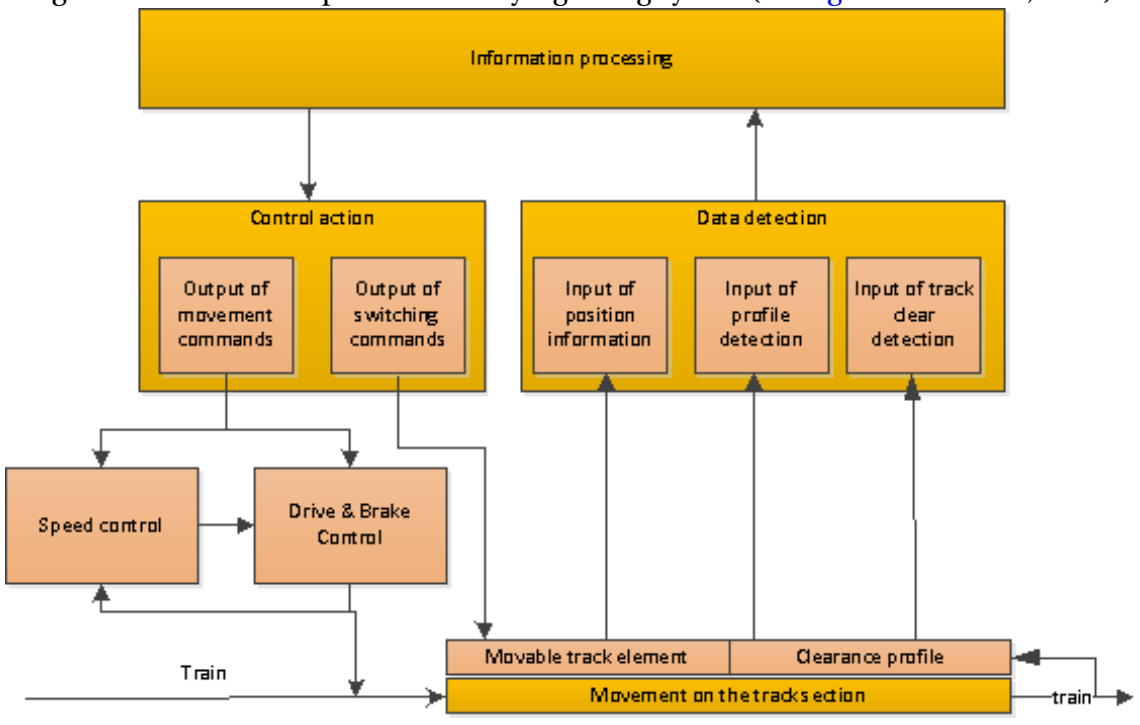
Chapter 2

Introduction to railway signaling system

2.1 Railway Signaling System

Railway signaling system is needed for ensuring the safe operation in rail traffic. The signal devices are located on the side of railway line to give information of the state of railway line ahead to train drivers. A generic interpretation of the control loop of the railway signaling system is presented in Figure 2.1.

Figure 2.1: Control loop of the railway signaling system(Theeg and Vlasenko, 2009)



The methods behind railway signaling system are information transmission and information processing. The function of *information processing* is typically realized by interlocking. The purpose of *interlocking* is to connect the track elements and signals so that a dangerous situation can be avoided. This can be achieved by means of *data detection* and *control action*. Here *data detection* includes discovering the position information of the movable track elements and information of track occupation. *Control action* involves evaluating the received information and giving instructions to the train drivers via signals. These two actions form the basic principles for interlocking functions(Theeg and Vlasenko, 2009):

- A train movement can be permitted only if all track elements are in desired positions and locked.
- It is only allowed to enter a section for one train, no other train may be permitted to enter that section.

An interlocking system has many functions. Generally, they can be categorized into three levels of functions: *operation control level*, *interlocking level* and *element control level*. They are defined as(Theeg and Vlasenko, 2009):

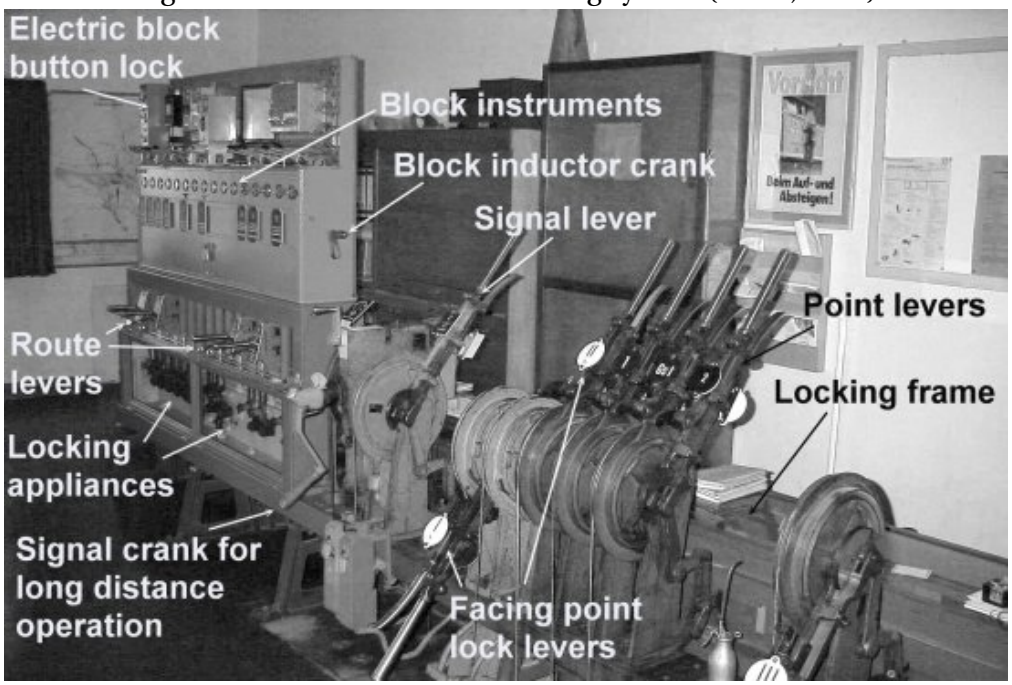
- The **operation control level** includes the interface to the signaler and may include different non-vital functions of automatic operation control such as automatic train routing etc.
- The **interlocking level** includes the vital functions to interlock signals, routes, movable track elements, block applications with each other.
- The **element control level** includes functions of commanding, power and information transmission to and from the field elements, such as signals, movable track elements, track sections, level crossing etc.

Since the safe operation of railway is always primary concern, different technologies have been implemented for those interlocking systems to ensure the safety worldwide in the rail transport. They are *human interlocking*, *mechanical interlocking*, *electric (relay) interlocking* and *electronic interlocking*.

The oldest solution for interlocking is the human interlocking. Human is in charge of checking the preconditions for clearing signals, switching movable track elements and for transmitting information to the field elements by walking between them(Theeg and Vlasenko, 2009).

The mechanical interlocking system was introduced in the late 1800's, see Figure 2.2. In mechanical interlocking system, the mechanical levels that are interlocked with each other are operated by signaler. The safety of this system is secured by using robust mechanical and/or electrical components(Theeg and Vlasenko, 2009, Ch. 2.2, p. 27).

Figure 2.2: Mechanical interlocking system (Pachl, 2015)

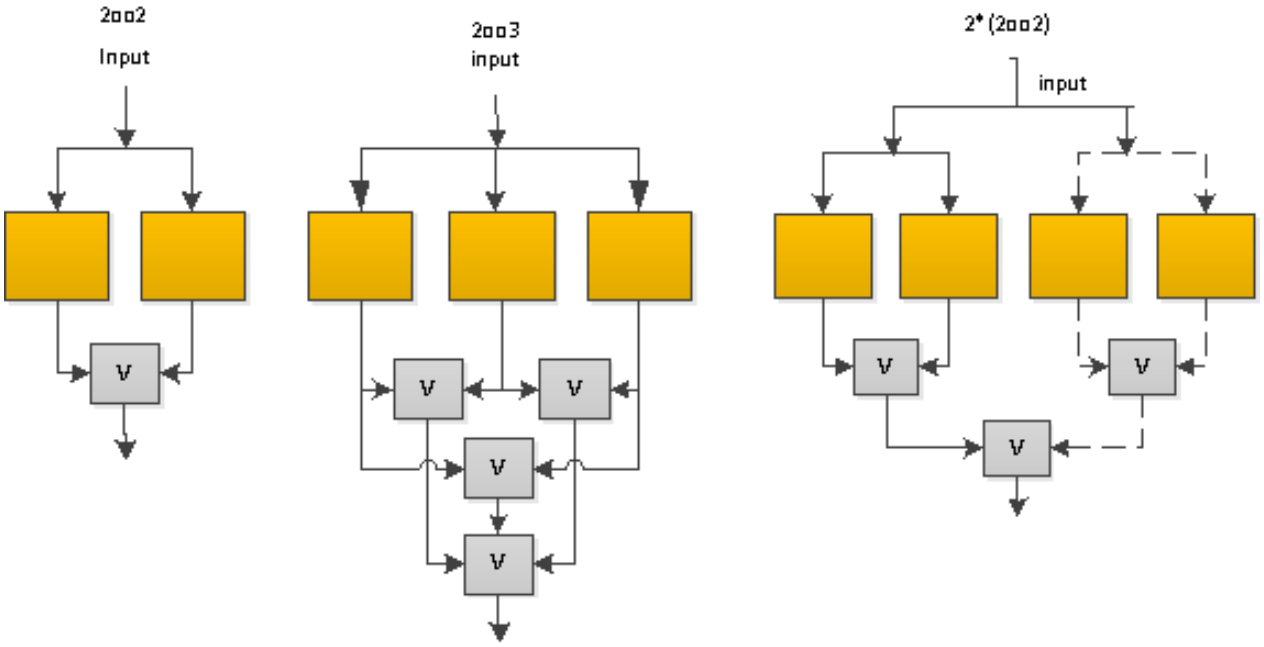


Relay-based interlocking system was introduced after mechanical interlocking system. A signal relay is specially designed for the safety-related operation. The interlocking consists of complex circuitry implemented by relays and the field elements are operated and controlled purely electrically.

Electronic interlocking systems became prevailing after 1980s. The systems have high degree of complexity and are easily affected by external influences. The interlocking functions are programed by software, and the hardwares are made by electronic components which are not robust as mechanical components. These cause that the inherent fail-safe design is hardly applied to electronic interlocking systems as before. To increase the reliability, hardware depen-

dency are widely used in electronic interlocking systems. There are three major forms of system redundancy, depended on special national requirements, in various electronic interlocking systems. They are *2oo2 system*, *2oo3 system* and *2*2oo2 system*, illustrated in Figure 2.3.

Figure 2.3: Different redundancy in electronic systems



For *2oo2 system*, same inputs are processed by two independent channels. The outputs of two independent channels are compared using a voting circuit. The interlocking functions are carried out only if both results are equal, otherwise the system will enter into safe state. This system significantly reduces the probability of a spurious trip compared with *1oo2 system*. On the other hand, the system has the disadvantage that the average frequency of dangerous failures is twice higher than that of a *1oo2 system*, given that only DU failures are considered. Consider the *2oo3 system*, the system is able to operate as long as there are two channels functioning. The availability is increased compared with *1oo2 system*. Same as *2oo2 system*, the average frequency of dangerous failures is three times as high as that of a *1oo2 system*, given that only DU failures are considered. From both safety and availability point of view, *2*2oo2 system* provide better safety and availability. This is because one redundant *2oo2 system* is in active mode and another works in standby mode. If a failure occurs in the active one, the process is continued by the standby subsystem.

2.2 Norwegian Railway Signaling System

Norwegian railway signaling system consists of 9 subsystems(Jernbaneverket, 2015). They are the interlocking system, level crossing, train detection, switch, signals, ATC infrastructure, control center, other technical systems and other facilities. It is illustrated in Figure 2.4.

Figure 2.4: Norwegian railway signaling system(Jernbaneverket, 2015)

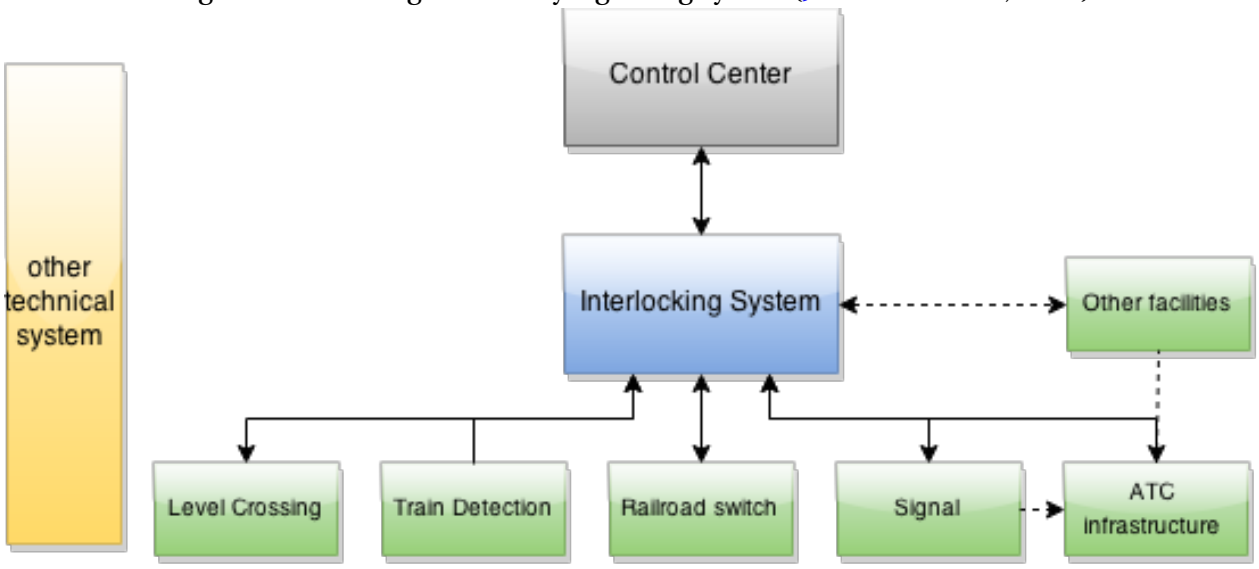
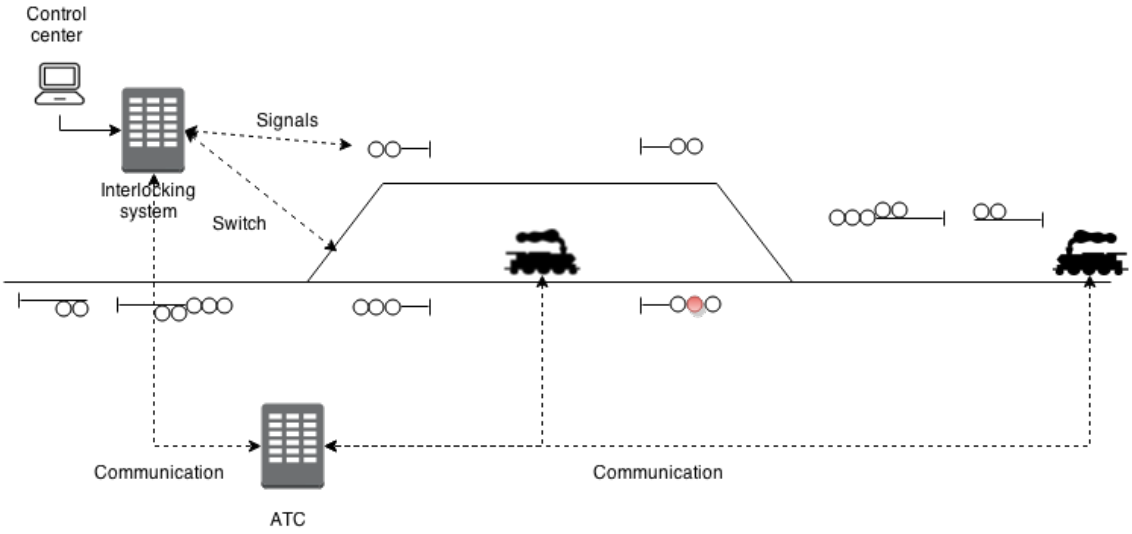


Figure 2.4 shows how 9 subsystems compose a railway signaling system. How a signaling system is deployed in a two track station is illustrated in Figure 2.5.

Figure 2.5: Signaling system in a single track station



2.2.1 Challenges in Design of a Two Track Station

It is a very challenging task to deploy a signaling system into a two track station. In order to understand how the design of a signaling system impacts the safe operation of trains, it is better to start from basic scenarios in a two track station.

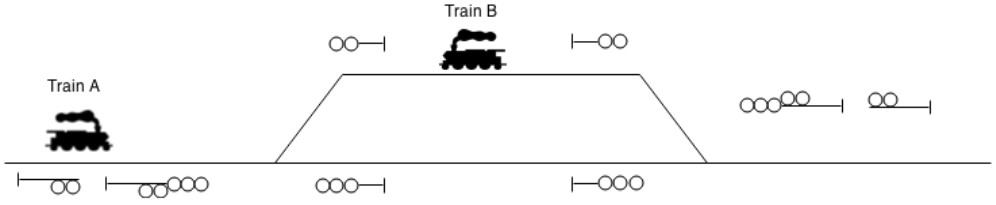
The first scenario to be considered is that two trains are passing the station from opposite directions. This situation is illustrated in Figure 2.6.

Figure 2.6: Two trains passing station from opposite directions

The interlocking system has to determine which train enters the station first and waits at station until the other train passes the station. The interlocking system can not undertake the tasks without assistance of other systems. The interlocking system first has to detect which train is near the station and let this train enter the station first. If Train B is near station, for instance, the signals must indicate the train driver to slow down the train. Meanwhile, the rail switch needs to be switched to the position that can lead the train entering the upper track. Train B has to stop in front of the main signals at the upper track. In addition, the interlocking system has to give the Train A the signals to reduce speed. The rail switch has to be moved to main track to ensure the train passing thr ough the station safely. This is the normal situation. If Train B gets erroneously a green signal, or the rail switch is in the wrong position, collision or derailment may occur if the train drivers could not stop the trains in time.

The second scenario is that a train stops at the station while the other train is entering the station from the opposite directions. This situation is illustrated in Figure 2.7.

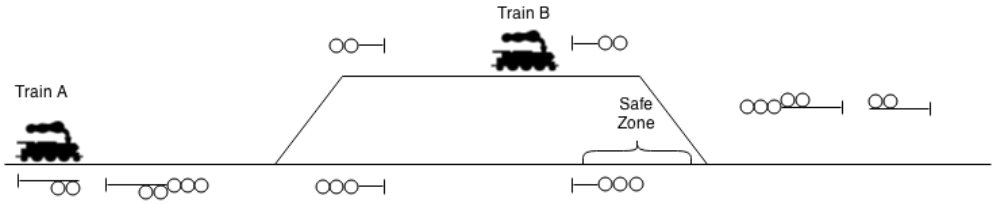
Figure 2.7: Two trains entering station from opposite directions



The interlocking system has to set a red signal to ensure that Train B remains still until Train A passes through the station or stops at the station. If Train B gets erroneously a green signal, it may collide with Train A. Meanwhile, the rail switch has to be in the right position so that Train A can pass through. If the interlocking system can not set the rail switch in the right position, Train A may derail at switch point or collide with Train B which stops at the station.

The third scenario is that a train stops at the the station while the other train is entering or passing the station from the same direction. This situation is illustrated in Figure 2.8.

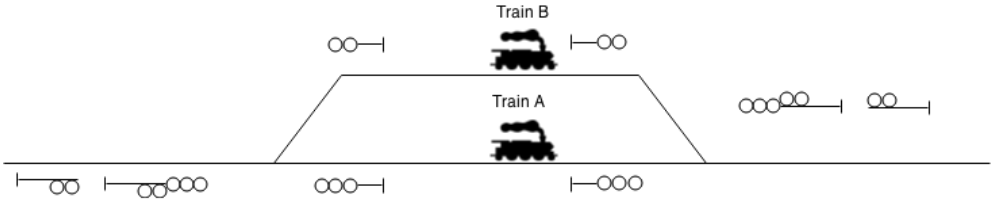
Figure 2.8: Two trains entering station from opposite directions



This scenario is more complicated than the two scenarios above. There are three possible cases for this scenario. First, Train A waits for that Train B leaves the station. In this case, the interlocking system has to give a stop signal to Train A. If Train A gets erroneously a green signal, it may collide with Train B when Train B has not left the station completely. Secondly, Train B stops at the station until Train A passes through the station completely. The interlocking system has to set a stop signal to Train B. If Train B gets erroneously a green signal, it may collide with Train A which has full speed when passing through the station. The consequence of such event will be catastrophic. Finally, both Train A and Train B can drive at the same time. It is assumed that it exists a safe zone that is long enough so that a train can stop in front of the switch point if it passes the main signal mistakenly. In this case, Train B is allowed to leave the station. Train A gets a signal of reducing speed before Train B leaves the station. If Train A gets erroneously a green signal, which gives a command that Train A continues with full speed, it may collide with Train B that is leaving the station.

The last scenario is that both trains stop at the station and wait for driving signals. This situation is illustrated in Figure 2.9. In this case, the interlocking system has to ensure that only one train can get a green signal. If Train A gets erroneously a green signal at the same time Train B leaving the station, it may collide with Train B at the switch point.

Figure 2.9: Two trains entering station from opposite direction



ATC infrastructure, which is a technical barrier against human error, plays a vital role in assuring the safe operation of the train. There are two main functions performed by ATC in a two track station. Consider the third scenario above, Train A is approaching the station and is going to stop before the main signal. The ATC monitors the speed of the trains continuously. The ATC will ensure that Train A brakes before the main signal. However, if the speed is over 40 km/h at the main signal, which is measured by ATC, the train is brought to a full stop. Moreover, ATC will ensure that the speed is lower than 40 m/h at the switch point to avoid derailment.

2.2.2 Standards and Regulations

In this section, some of the relevant standards and regulations framing the design of signaling system are briefly introduced.

EN 50126

EN 50126 is a standard that provides a consistent approach to the management of reliability, availability, maintainability and safety, based on the system life cycle and tasks within it. In other words, it describes all the essential elements for a *Safety Management System*. These elements are a company policy, a safety plan, a hazard log, internal audit and a failure reporting and corrective actions system, a risk estimation process etc (Winther, 2015). EN 50126 consists of three parts. They are described below:

Part 1:*Basic requirements and generic process*, defines RAMS elements in railway system.

Part 2:*Guide to the application of EN 50126-1 for safety*, specifies approaches for applying safety process requirements in EN 50126-1 to a railway system and for dealing with the safety activities during the different system life cycle phases.

Part 3:*Guide to the application of EN 50126-1 for rolling stock RAM*, provides a guideline on applying EN 50126-1 to rolling stock.

EN 51028

En 50128 is a standard that specifies procedures and technical requirements for the development of programmable electronic systems which are used in railway control and protection applications.

This standard provides a set of requirements with which the development, deployment and maintenance of any safety-related software intended for railway control and protection applications shall comply. The main concept of this standard is the software safety integrity levels. The lowest software safety integrity level is 0 and 4 is the highest one. Some techniques and measures are identified for the five levels of software safety integrity.

EN 50128 defines the process of specifying the safety functions allocated to software. The processes include identifying hazards, identifying risk reduction measures, defining overall System Safety Requirements Specification(SSRS), selecting a system architecture and translating SSRS into a Safety-related system of a validated safety integrity.

EN 50129

EN 50129 defines requirements for the acceptance and approval of safety-related electronic systems in the railway signaling field. The requirements for safety-related hardware and for the overall system are defined in this standard. This standard applies to the life cycle of complete signaling systems, and also to individual subsystems and equipment within the complete system. This standard is not applicable to those systems which had been in operation prior to the creation of this standard.

This standard is concerned with what evidences are needed to demonstrate the safety of a signaling system. The evidence shall include the conditions that shall be satisfied in order that a safety-related railway system can be accepted as adequately safe for its intended application.

Railway Technical Regulations

The Railway Technical Regulation is an important management tool and an important guideline for design, construction and dimensioning of railway infrastructure in Norway. These regulations define the requirements that are needed to be complied with for signals in Norway. The regulation for signals consists of five parts, that is, *501 Common provisions, 550 Design, 551 Construction, 552 Maintenance* and *553 Control.*

The *550 Design* defines the overall RAMS requirements for signals. It includes the rules for development, construction, and design of signaling system, and its components and objects.

The *551 Construction* contains the rules for the construction of the signaling system and the components for the signaling system and objects in relation to other railway infrastructure. It also specifies the rules for assembly, setting and adjustment of the signaling system and the components for the signaling system and objects.

The *552 Maintenance* contains the necessary requirements for signaling systems, components for the signaling system and objects that must be fulfilled to ensure the proper and safe operation. It defines triggering requirements for implementing corrective maintenance.

The *553 Control* specifies the rules for the control of signaling systems and their components and objects for both new systems and existing systems.

2.2.3 Regulatory Practice in Norway

The Railway Infrastructure Regulation, which is published by Ministry of Transport and Communication, stipulates the minimal national technical requirements for safety and appropriate design, construction, operation and maintenance of railway infrastructure. It stipulates explicitly that infrastructure administrator shall utilize process standard EN 50126 for construction of new infrastructures and for modification of programmable technical system together with development and modification of Specific Transmission Modules(STM) units. In addition, it stipulates that infrastructure administrator shall use EN 50128 and EN 50129 for procurement of new signaling systems and for modification of electronic signaling systems. It is the superior regulation for the railway infrastructure. This indicates that use of other standards or Railway Technical Regulations can not deviate from requirements given in this regulation.

Railway Technical Regulations for signals mentioned above define the applicability of CENELEC series standards. It defines that signaling systems and their life cycle shall fulfill the requirements in EN 50126, EN 50128 and EN 50129. Moreover, it states that documentation shall be prepared and treated pursuant to guidelines in EN 50126, EN 50128 and EN 50129.

The Norwegian railway network is equipped with traditional signaling systems. In order to achieve higher safety and reliability and further increase in cross-border train traffic, ERTMS will be the replacement of current railway signaling system. Technical specifications for interoperability (TSIs) shall be covered by subsystems or part of subsystem in order to meet the essential requirements and to ensure the interoperability of the ERTMS and current railway signaling system. The following standards are mandatory to be followed for the Control-Command and Signaling(CCS):

Table 2.1: Mandatory standards for the Control-Command and Signaling(European Commision, 2012)

Reference	Document name and comments	Version
EN 50126	Railway applications — The specification and demonstration of reliability, availability, maintainability and safety (RAMS)	1999
EN 50128	Railway applications — Communication, signaling and processing systems — Software for railway control and protection systems	2001
EN 50129	Railway applications — Communication, signaling and processing systems — Safety related electronic systems for signaling	2003
EN 50159-1	Railway applications — Communication, signaling and processing systems — Part 1	2001
EN 50159-2	Railway applications — Communication, signaling and processing systems — Part 2: Safety related communication in open transmission systems	2001

Chapter 3

Reliability concepts

3.1 The Generic IEC 61508 Standard

IEC 61508, which is an "umbrella" standard covering different industries and applications, is an international standard for computer-based systems composed of electrical and/or electronic and/or programmable electronic (E/E/PE) elements that are used to perform safety functions(IEC, 2010). It gives overall requirements and is served as a basis for development of sector-specific standards. A significant feature of this standard is that it emphasizes on a risk-based approach to determine the safety requirements of a safety-related system in a safety life cycle.

3.2 Safety-Critical Systems

Safety-critical system is a system whose failure may have a severe consequence. Many safety-critical systems nowadays are designed on the basis of *electrical, electronic, or programmable electronic (E/E/PE)* technology. These systems are named by the term *E/E/PE safety-related system* in the standard IEC 61508. Safety-critical systems have wide application areas. They can be used in process industry, machinery industry, nuclear industry. In the railway context, signaling systems and automatic train control systems are two examples of safety-critical systems.

The term *safety-critical system* is mainly used in this thesis instead of using the term *E/E/PE safety-related system*, since the the railway signaling system is the main topic in the thesis and has the significant impact on railway safety.

3.3 Safety Functions

A *Safety Function* is implemented to protect against a specific *undesired event* that can cause harm(Rausand, 2013). A *Safety-critical system* may have one or more safety functions. To define safety functions, it is important to identify the undesired events first. Considering the Norwegian signaling system in chapter 2 as an example, the undesired events that have most severe consequences are collisions between trains and derailment (Løkberg and Øien, 2005). Safety functions shall be defined to prevent those two undesired events related to the signaling system from happening. As illustrated in Figure 2.4, the most important five elements of the signaling system are interlocking system, train detection, railroad switch, signals and ATC infrastructure. The functions performed by these five systems that can mitigate the consequence of the undesired events can be considered as safety functions of the signaling system. The safety functions were defined by Norwegian National Rail Administration(NNRA)(Løkberg and Øien, 2005).The defined safety-critical functions are listed in the Table 3.1. It should be noticed that the term *Safety-critical function(SCF)* is used by NNRA to denote *safety function*. To be consistent, the term *safety-critical function* is used in the rest of thesis.

Table 3.1: Safety-critical functions, failure mode and failure(Løkberg and Øien, 2005)

	Safety-critical functions	**Failure mode**	**Failure**
SCF 1	The interlocking system shall set correct output signals/send correct data to the controlled objects, given correct input signals/data into the interlocking system.	The interlocking system gives the less restrictive instructions than they are allowed based on the prerequisites to the signals.	Erroneous commands about driving signals(failures in the interlocking system)

Table 3.1: Safety-critical functions, failure mode and failure(Løkberg and Øien, 2005)

	Safety-critical functions	**Failure mode**	**Failure**
		The interlocking system gives the commands to movable track element even if the conditions are not fulfilled.	Erroneous commands about switching tracks(Failures in the railroad switch)
		The interlocking system gives the less restrictive instructions than they are allowed based on the prerequisites to the ATC infrastructure.	Erroneous driving signals/overspeed (Failures in ATC-messages from the interlocking system)
SCF 2	Railroad switch will lock switches and give the correct information about position and locking status to the interlocking system.	Railroad switch does not lock the movable parts when the conditions for locking are fulfilled, and not ensure that the movable parts remain locked.	False control of switches(Failures in railroad switch)
		Railroad switch does not give the correct information about control of locking and position to the interlocking system.	

Table 3.1: Safety-critical functions, failure mode and failure(Løkberg and Øien, 2005)

	Safety-critical functions	**Failure mode**	**Failure**
SCF 3	Train detection shall detect an unoccupied railway section and give correct information about whether a railway section is occupied or not to the interlocking system.	Train detection does not detect certainly about a track element which is not occupied by a train.	No detection of occupied railway section (Failure in train detection)
		Train detection does not give the correct information occupied or unoccupied track element to the interlocking system.	
SCF 4	Signals shall show the correct signal light for the train and give the correct information about the signal state to the interlocking system.	Signals does not show the correct signal light for the train based on the condition.	Erroneous driving signals(Failures in signals)
		Signals does not give the correct information about the signal state to the interlocking system.	
SCF 5	ATC infrastructure shall give the correct information about status of interlocking system/signals to the train.	ATC infrastructure does not give the correct information about status of interlocking system/signals to the train.	Erroneous driving signals/overspeed (Failure in ATC infrastructure)

3.4 Safety Integrity Level

A *Safety Integrity Level(SIL)* is a way to indicate the tolerable hazard rate(THR) or hazard rate of a particular safety-critical function. It is wrong to say that a safety-critical system has achieved a certain safety integrity level. SIL is allocated to safety-critical functions and corresponding subsystems implementing these functions. It should be noticed that a safety-critical system may have many safety-critical functions with different SILs.

The standard IEC 61508 defines SIL in terms of PFD or PFH, see Table 3.2:

- Average probability of a dangerous failure on demand(PFD) in low-demand modes of use
- Probability of a dangerous failure per hour(PFH) in high-demand modes of use

Table 3.2: SIL Table

Safety Integrity Level	**Probability of dangerous failure on demand**	**Probability of dangerous failure per hour**
SIL4	10^{-5} to 10^{-4}	10^{-9} to 10^{-8}
SIL3	10^{-4} to 10^{-3}	10^{-8} to 10^{-7}
SIL2	10^{-3} to 10^{-2}	10^{-7} to 10^{-6}
SIL1	10^{-2} to 10^{-1}	10^{-6} to 10^{-5}

EN 50129 defines SIL in terms of THR, see Table 3.3:

- Tolerable hazard rate per hour and function(THR)

Table 3.3: THR/SIL relationship

SIL	**THR(h^{-1})**
SIL4	$10^{-9} \leq \text{THR} < 10^{-8}$
SIL3	$10^{-8} \leq \text{THR} < 10^{-7}$
SIL2	$10^{-7} \leq \text{THR} < 10^{-6}$
SIL1	$10^{-6} \leq \text{THR} < 10^{-5}$

One may ask why EN 50129 recommends THR other than PFD and PFH for determining SIL. It may be interesting to know that PFD and PFH were still defined and used in earlier draft versions of EN 50129(Braband et al., 2009). Only THR is used for determining SIL in the present EN 50129. However, one simple argument for not choosing PFD is that signaling systems in railway

operate in continuous mode or in high-demand mode. The PFH used in IEC 61508 concerns only about *E/E/PE safety-related system*, not about *EUC control system* and *EUC*(Braband et al., 2009). In the EN 50126 series of standards, it does not distinguish *E/E/PE safety-related system*, *EUC control system* and *EUC*. This is the reason of choosing THR values, since THR values can be applied to the entire technical system but PFH can only be applied to *E/E/PE safety-related system*. However, it should be known that the THR associate to a SCF coincides with the PFH of the entire system implementing the SCF, i.e., THR = $PFH_{\text{entire system}}$.

3.4.1 Intention of the SIL concept

When a SIL level is determined for a safety-critical function in terms of THR, what does this SIL level indicate in railway application? In railway, the *safety integrity* comprises two parts(CENELEC, 2003):

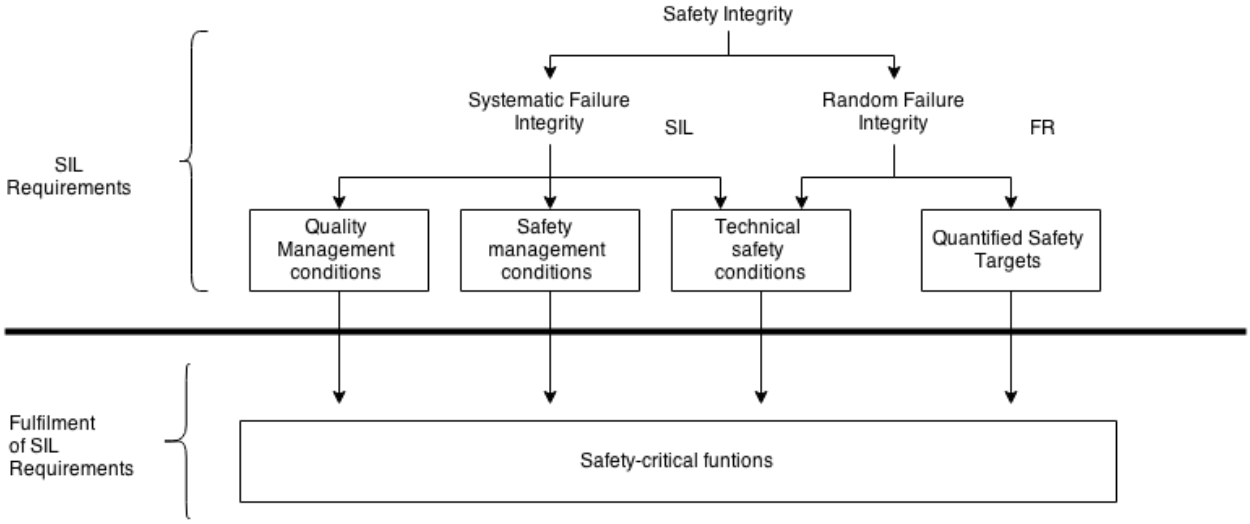
- Systematic Failure Integrity(SFI): is the non-quantifiable part of the safety integrity and relates to hazardous systematic faults (hardware or software). Systematic faults are caused by human errors in various stages of the system/subsystem/equipment life cycle.
- Random Failure Integrity(RFI): relates to hazardous random faults, in particular random hardware faults, which concerns about the reliability of hardware components

To achieve systematic failure integrity, the quality management and safety management strategies shall be established. Technical aspects of systematic faults shall also be demonstrated according to standards. All methods, tools and techniques against these systematic faults are recommended in the EN 50129, Annex E. These qualitative measures are used to adverse consequences of human errors during the life cycle of a system.

Failure rate is the quantified safety target that is used for random failure integrity. For a system/subsystem, failure rate can be calculated based on known data for hardware components failures. The relationship among *Safety Integrity*, *Systematic Failure Integrity* and *Random Failure Integrity* is illustrated in Figure 3.1.

Figure 3.1 also illustrates the distinctions between SIL requirements and SIL performance of a SCF. The upper part of the figure shows that SIL requirements are defined for SCFs, which is the responsibility of railway authority. The lower part reflects the SIL performance of a SCF.

Figure 3.1: Relationship among SI, SFI and RFI



To verify the SIL performance of a SCF, failure rate of a SCF is calculated and is compared with SIL requirements. If SIL requirement is not satisfied, the realization of a SCF must be modified, either by changing architecture, or by using other components.

3.5 THR Determination

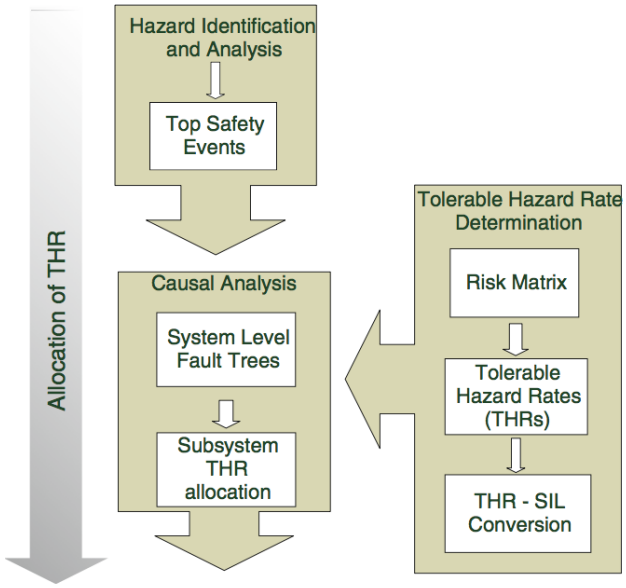
Safety requirements, in the form of *Tolerable Hazard Rate(THR)*, are assigned to functions. It is required that a list of hazards and associated THRs within the system shall be defined. The main activities that should be carried out in allocation of THR are illustrated in Figure 3.2.

These activities includes a systematic approach of identification of hazards, THR determination and THR allocation to subsystems. The step *THR determination* will be discussed here. Other steps are not in the scope of this thesis.

3.5.1 THR for Continuous Mode Functions

A method, called MODURBAN method(MODSafe, 2011), is introduced for allocation of THR for continuous mode functions. This method is based on the risk matrix introduced in EN 50126. It introduces three more parameters other than *frequency of occurrence* and *severity level* used in the risk matrix. These parameters may reduce the severity level. The three parameters and their descriptions are defined in (MODSafe, 2011):

Figure 3.2: Overall SIL analysis process allocation of THR(Zhang et al., 2014)



- Exposure Probability to Hazard **(E)**: the probability of exposure of members of the risk group to hazard
- Accident Probability Reduction **(P)**: the reduction rate of a certain hazard into an accident by additional barriers
- Consequence Reduction Probability **(C)**: the probability that a member of the risk group can avoid being subject to the consequences of a certain hazard

Further, it gives numerical interpretation of risk parameters for this method. The numerical interpretation of these parameters are expressed as follows(MODSafe, 2011):

- Severity Levels:
  - Catastrophic: THR = $10^{-9}/h$
  - Critical: THR = $10^{-8}/h$
  - Marginal: THR = $10^{-7}/h$
  - Insignificant: THR = $10^{-6}/h$
- Exposure Probability to Hazard **E**:

  - $E = 1$: Exposure of members of the risk group to hazard is conservatively to be assumed frequent or permanent
  - $E = 10^{-1}$: Exposure of members of the risk group to hazard can conservatively assumed to be rare, only in exceptional cases
  - $E = 10^{-2}$: Exposure of members of the risk group to hazard is only in very rare cases to be expected

- Accident Probability Reduction **P**:
  - $P = 1$: There can no additional barrier to be conservatively assumed that would reduce the probability of the hazard evolving into accident
  - $P = 10^{-1}$: There exists means or circumstances to clearly reduce the probability that a certain hazard evolves into an accident
  - $P = 10^{-2}$: There exists two means or circumstances to clearly reduce independently the probability that a certain hazard evolves into an accident

- Consequence Reduction Probability **C**:
  - $C = 1$: There is no reason to conservatively assume that a member of the risk group may avoid being subject to the consequences of a certain hazard
  - $C = 10^{-1}$: There is a good reason to conservatively assume that a member of the risk group can avoid being subject to the consequences of a certain hazard
  - $C = 10^{-2}$: There are two independent reasons to conservatively assume that a member of the risk group can avoid being subject to the consequences of a certain hazard

Considering the severity level of hazards and the three risk reduction factors, a rate of frequency can be estimated that represent the THR:

$$\text{THR} = \frac{\text{Severity}}{\text{E} \cdot \text{P} \cdot \text{C}} \tag{3.1}$$

Example of application

An example of how to use this method is given in Table 3.4.

Table 3.4: Example of application of MODURBAN method

Item		**Description**
Name of SCF		The interlocking system shall set correct output signals/send correct data to the controlled objects, given correct input signals/data into the interlocking system.
Reason of failure		Erroneous commands of driving signals
Hazardous situation		The interlocking system gives the less restrictive instructions than they are allowed based on the prerequisites to the signals.
Hazard consequences		Collision
Exposure probability to hazard		Passenger are permanently in train
Accident probability reduction		No barrier can be assumed
Consequence reduction probability		Passenger cannot escape consequences
Severity of consequences		Catastrophic
Initial THR per hour		10E-9
Risk reduction factors	E	1
	P	1
	C	1
Final THR		10E-9
Final SIL		10E-9

3.5.2 THR for Low-demand Mode Functions

The current standard does not cover the concept of SCFs operating in low-demand mode. Considering the situation when the train is entering into a station with too high speed, the ATC has to force the train to stop. For this SCF performed by ATC, it operates in low-demand mode since this situation is rare. To determine THR for such system, a Markov method may be helpful(Scholz et al., 2012). The states and transitions have to be defined to model such system, which are described in the list below. The safety element of this system may go into a state, with a failure rate λ_{SE}, where it may not be able to provide its safety function. A potentially unsafe incident may occur with a rate λ_I.

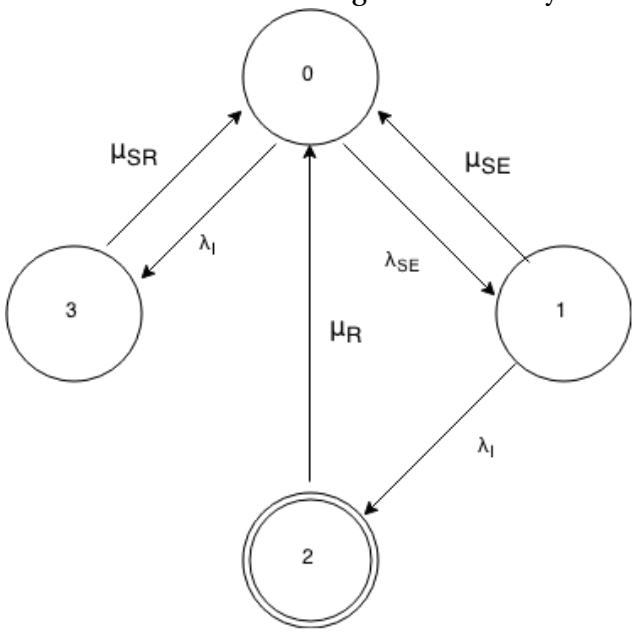
- **State 0**: The system is in a safe state, the safety element is working as it is intended.
- **State 1**: An undetected failure in the safety element has occurred with a failure rate λ_{SE} until a test reveals the failure, and the potentially unsafe incident has not occurred. The system remains in a safe state. The system can be repaired with a repair rate μ_{SE}.

- **State 2**: The potentially unsafe incident occurred with the hazard rate λ_I meanwhile the undetected failure in the safety element is not fixed. The system can be repaired with a repair rate μ_R. This system is in the unsafe state.

- **State 3**: The potentially unsafe incident occurs with the hazard rate λ_I. The system returns to the safe state with rate μ_{SR}.

The detected failures are not considered as critical failures from a safety point of view. Only undetected failures are critical. It is assumed that μ_{SE} is much larger than the failure rate and the rate of a potentially unsafe incident. A state transition diagram of the system is illustrated in Figure 3.3.

Figure 3.3: State transition diagram of a safety element.



The transition matrix is

$$\begin{pmatrix} -(\lambda_{SE}+\lambda_I) & \lambda_{SE} & 0 & \lambda_I \\ \mu_{SE} & -(\mu_{SE}+\lambda_I) & \lambda_I & 0 \\ \mu_R & 0 & -\mu_R & 0 \\ \mu_{SR} & 0 & 0 & -\mu_{SR} \end{pmatrix} \tag{3.2}$$

The steady-state probabilities are determined by

$$[P_0, P_1, P_2, P_3] \cdot \begin{pmatrix} -(\lambda_{SE}+\lambda_I) & \lambda_{SE} & 0 & \lambda_I \\ \mu_{SE} & -(\mu_{SE}+\lambda_I) & \lambda_I & 0 \\ \mu_R & 0 & -\mu_R & 0 \\ \mu_{SR} & 0 & 0 & -\mu_{SR} \end{pmatrix} = [0,0,0,0] \tag{3.3}$$

and

$$P_0 + P_1 + P_2 + P_3 = 1$$

The solution is

$$P_2 = \frac{\lambda_I \cdot \lambda_{SE} \cdot \mu_{SR}}{\mu_R \cdot \mu_{SE} \cdot \mu_{SR} + \mu_R \cdot \lambda_I \cdot \mu_{SR} + \mu_R \cdot \lambda_{SE} \cdot \mu_{SR} + \lambda_I \cdot \lambda_{SE} \cdot \mu_{SR} + \mu_R \cdot (\mu_{SE} + \lambda_I) \cdot \lambda_I^2 \cdot \lambda_{SE}} \tag{3.4}$$

where P_2 is the mean proportion of time that the system is spending in an unsafe state.

We assume that the repaired rates $\mu_{SE}, \mu_{SR}, \mu_R$ are much larger than the failure rates, and we have an approximate result of P_2.

$$P_2 \approx \frac{\lambda_I \cdot \lambda_{SE} \cdot \mu_{SR}}{\mu_R \cdot \mu_{SE} \cdot \mu_{SR}} = \frac{\lambda_{SE}\lambda_I}{\mu_R \mu_{SE}} = \frac{\frac{\lambda_{SE}\lambda_I}{\mu_{SE}}}{\mu_R} \tag{3.5}$$

The frequency ω_F of the system failure is the steady-state frequency of transitions from a functioning state (in State 1) to a failed state (in State 2), that is,

$$\omega_F = \nu_2 = P_2 \cdot \alpha_2 = P_2 \cdot \mu_R = \frac{\lambda_{SE}\lambda_I}{\mu_{SE}} \tag{3.6}$$

where α_2 is the rate at which the process leaves state 2.

Discussion of the Results

The ω_F has dimension in failures/hours, this is the rate that the system may be in the dangerous state. This rate is equivalent to the THR, which determines the acceptable risk level.

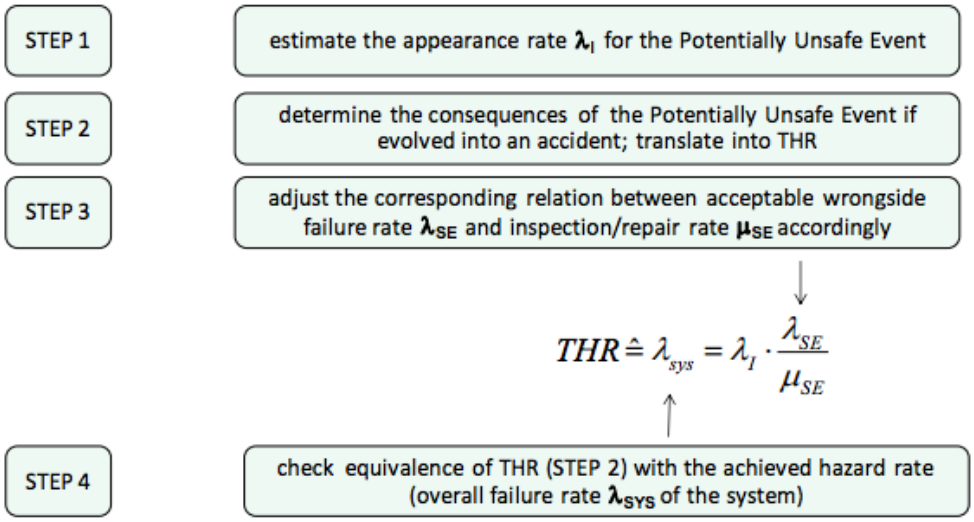
The Formula refeq:5 can be interpreted from another angle. The λ_I is the rate at which a potentially unsafe event may occur, but since the safety element has been implemented, the

potentially unsafe event may not lead to a hazard. Therefore, $\frac{\lambda_{SE}}{\mu_{SE}}$ can be treated as the likelihood that the potentially unsafe event may cause a hazard. This likelihood is determined by the failure rate and repair rate of the safety element, and can be expressed as

$$P = \frac{\lambda_{SE}}{\mu_{SE}} = \frac{\omega_F}{\lambda_I} \tag{3.7}$$

The first step for determining an equivalent safety integrity requirement for low-demand mode system is to decide the potentially unsafe event and the consequences(THR). The failure rate λ_{SE} of the safety element and the repair rate μ_{SE} shall be determined based on the THR value. The steps are shown in the Figure 3.4.

Figure 3.4: Determination of a safety integrity requirement for functions operating in low-demand mode(Scholz et al., 2012)



We assume that there is a fire detection device on the train, and the potentially unsafe event, i.e. fire, occurs with a rate $\lambda_I = 10^{-5}/h$. The THR for such event is $10^{-9}/h$. Consequently, the failure likelihood is $P = 10^{-4}$. As a result, $\lambda_{SE} = 10^{-6}/h$ and $\mu_{SE} = 10^{-2}/h$ or $\lambda_{SE} = 10^{-5}/h$ and $\mu_{SE} = 10^{-1}/h$ would satisfy this failure probability. However, which one is the best solution should be justified by the operator depending on the maintenance strategies(inspection/repair rate).

It is interesting to find out what is the link between Formula 3.6 and *Hazardous Event Frequency(HEF)*. The frequency of hazardous events for a low-demand system will depend on the

frequency of demands and the reliability of a SCF, and is given by

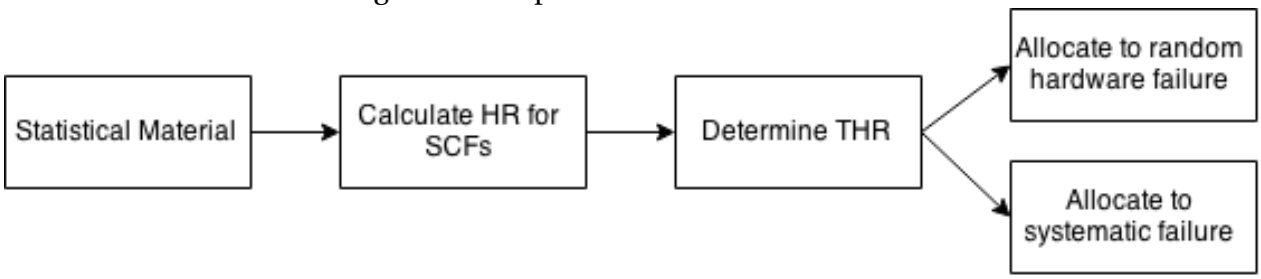
$$\text{HEF} = \text{PFD}_{\text{avg}} \cdot \lambda_{de} \tag{3.8}$$

There are some similarities between Formula 3.8 and Formula 3.6. Both parameter λ_I and parameter λ_{de} express the frequency of undesired events, even though the denotations of parameters are not the same. As explained above, $\frac{\lambda_{SE}}{\mu_{SE}}$ is the probability that the potentially unsafe event may cause a hazard, given a SCF is failed. This coincides with PFD_{avg}, which is the probability that a dangerous fault is present so that a SCF cannot be performed. Thus, Formula 3.8 and Formula 3.6 are equivalent.

3.5.3 THR Determination Method Used in Norway

SINTEF, the largest independent research organization in Scandinavia, performed analysis on five central SCFs for railway signaling system in Norway(Løkberg and Øien, 2005). They proposed a method for determining the THR for SCFs based on experienced failure rates, see the Figure 3.5.

Figure 3.5: Steps for determination of THR.



All railway authorities may maintain a database for failures related to the railway infrastructures, including a classification of whether these failures were safety-critical or not. Those safety-critical failures can be further classified into the associated SCFs. It is possible to determine how many of the total number of failures were hazards. Consequently, Hazard Rate(HR) of the SCF can be estimated from registered failures in the database. This empirical HR is considered as the lowest value that the acceptable THR should maintain for the SCF. The expression

is

$$\text{HR} = \frac{\text{N}}{\text{T} \cdot 8760 \cdot n_s} \text{failures per hour per signalling system} \tag{3.9}$$

where N denotes the total safety-critical failures registered in the period T, n_s is the total signaling system that contributes safety-critical failures.

THR reflects both random hardware failures and systematic failures. Random hardware failures are triggered by random events, and systematic failures are failures which will reoccur if the situation triggering the failure is recreated. The maintainer may or may not distinguish such failures when he registered the data. It is therefore important to assign different portions of THR-value of a SCF to systematic failures and random hardware failures.

Some uncertainties accompany with this method. Firstly, it concerns the degree of reporting. From the Formula, HR is lower when the N is lower, given that other parameters remain the same. The number of the safety-critical failures is lower may due to the underreporting of failures. This is possible caused by the unstructured reporting routines. Secondly, the accuracy of registered data may be compromised. Some failures may be registered as safety-critical when they are not. Finally, the search criteria may influence the results. It is possible that the search criteria were defined in an improper way that people may fetch too much or too little safety-critical failures from database.

Chapter 4

Safety case

4.1 Different Roles and Responsibilities

The development of a railway system consists usually of 14 phases according to EN 50126(CENELEC, 1999). The whole system life cycle involves different roles and responsibilities for each phase. Typically, those main participants in the development of a railway system are the *Operator*, the *Supplier*, the *Safety Authority* and the *Independent Safety Assessor*.

The main responsibilities for the operator are related to life cycle phases 1-4 and life cycle phase 10-14. The typical activities for the operator are for example:

- Define the system, functional, RAMS requirements
- Check fulfillment of system requirements
- Check fulfillment of RAMS requirements
- Determine operation, maintenance and service strategies
- Acceptance of the system
- Communication with the safety authority, the independent safety assessor and supplier

The supplier is responsible for the design, manufacture, installation and system validation life cycle phases. The typical activities for supplier are for example:

- Design of the system/subsystem/products

- Refine the system requirements to subsystem/design
- Manufacture, install, test and commission the system/subsystem/products
- Demonstrate fulfillment of system requirements
- Demonstrate fulfillment of safety requirements
- Communication with safety authority, the independent safety assessor and operator

The safety management is important in railway industry. The safety authority, served as an independent agency, supervises the activities in all phases of a railway system. It is safety authority's duties to :

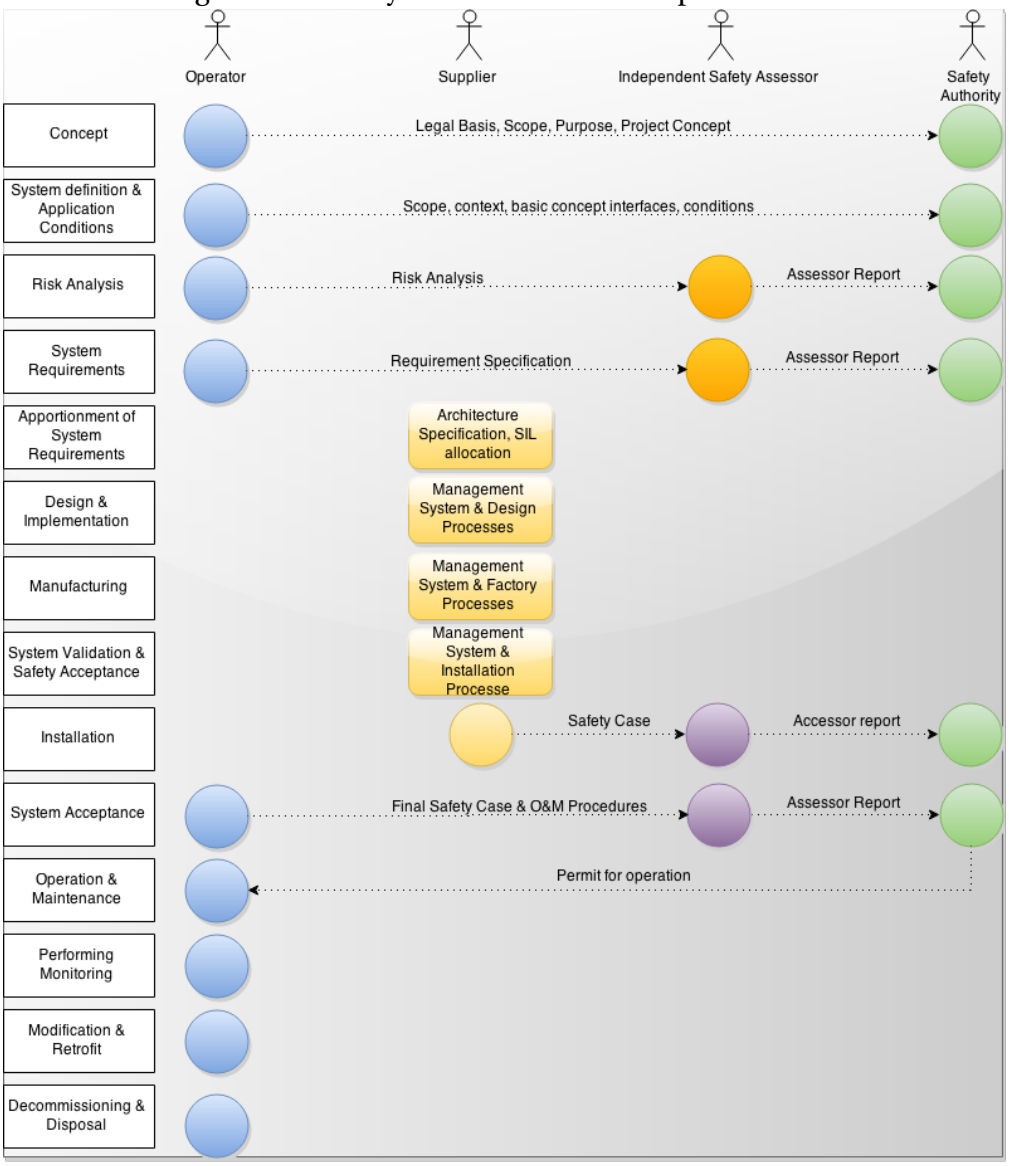
- Specify the operator's obligations
- Give the guidance on relevant standards, rules, technical principles
- Approve new / modified system
- Approve safety, functional and system requirements of the system

The safety authority must approve the operation of a railway system after system validation and safety acceptance based on the evidence that operator and supplier provided. To guarantee the trustworthiness of the evidence, a third party, the independent safety assessor, shall assess whether a system being designed is in accordance with the relevant safety standards and safety requirements. The typical activities includes(Sághi, 2012):

- Assessment of operator's system criteria
- Assessment of supplier's quality management system
- Assessment of supplier's safety management system
- Assessment of supplier's safety process implementation
- Assessment of functional and technical safety
- Assessment of related safety cases

Figure 4.1 shows the involvement of different roles.

Figure 4.1: Life cycle with roles and responsibilities



4.2 Safety Case

The safety case is defined as(Adelard, 1998):

> A documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment

The safety case is a collection of disparate pieces of information that form safety arguments for showing the safe operation of a system. The concept of using the mechanism of the safety case is to ensure a certain level of safety and to maintain the safety in every part of the lifetime of

the system. Evidence and argument are two essential elements for the safety case. The former are the results of analyzing, testing, simulating and validating the properties of a system that can be used as a basis for inferring the safety of a system. The latter clarifies why an adequate level of safety is achieved by the available evidence.

The safety cases shall be made for infrastructures, train operations and station operations. Ideally those safety cases shall be independent. The interdependencies will always exist because of the complexity of the systems. It is therefore important to record the references to the safety cases of any subsystems or equipment. A safety case is developed for justifying that a railway system is safe enough for operation in a specific operating environment. The structure of a safe case is given by EN 50129(CENELEC, 2003):

- **Part 1** Definition of System (or sub-system/equipment)
- **Part 2** Quality Management Report
- **Part 3** Safety Management Report
- **Part 4** Technical Safety Report
- **Part 5** Related Safety Cases
- **Part 6** Conclusions

4.2.1 Different Categories of Safety Case

The size and details in safety case are the major problems that a Safety Authority has faced since the safety case was introduced. Too much details will increase the size of the documents. It is inevitable that some of the documents are useless for safety demonstration. To ensure the decisions on the acceptability of or the quality of the Safety Case, EN 50129 suggests that the following three categories of safety case can be considered (CENELEC, 2003):

- **Generic Product Safety Case(GPSC)**: A generic product can be re-used for different independent applications. It is one of the building blocks for the applications.
- **Generic Application Safety Case(GASC)**: A generic application can be re-used for a class/type of application with common functions. It is configurable, but is not ready configured

- **Specific Application Safety Case(SASC)**: A specific application is used for only one particular installation. It is ready configured.

The distinctions between GPSC and GASC are sometimes unclear. This is due to a system which can be applied as a generic product or which can be used as a subsystem in a more complex system. However it will clear the ambiguities if we consider systems, hazards and causal factors as a whole(International Railway Industry, 2013).

To identify the hazards, the supplier often makes assumptions about the circumstance in which their product will be used. Correspondingly, the supplier will design the product to eliminate the hazards. This is a generic product and shall be recorded in the GPSC. The hazards vary from application to application. A GASC is made for ensuring the risk which are controlled without considering the environment where the product will be applied. For a particular application of a system/product, the boundary of this system/product is therefore determined. A SASC shall keep the records of how this system/product reaches an adequate level of safety within its boundary.

Chapter 5

Technical Safety Report

The technical safety characteristics of the system are described in this part of safety case. It shall describe how the system achieves safety in the light of safety standards. The evidences of achieved safety properties of the system, i.e. test and analysis results, verification and validation reports, certificates and so on, shall be presented in this technical safety report(Nordland, 2000). EN 50129 defines the structure for the technical safety report:

- **Introduction:** This section shall provide an overview of description of the design and indicate the standards used as the basis for the technical safety of the design.
- **Assurance of correct functional operation:** This section shall contain all the evidences necessary to demonstrate correct operation of the system/subsystem/equipment under fault-free normal conditions, in accordance with the specified operational and safety requirements.
- **Effects of faults:** This section shall demonstrate that the system/sub-system/equipment continues to meet its specified safety requirements and demonstrate which technical measures have been taken to reduce the consequent risk to an acceptable level. This section shall also include demonstration that faults in any system/sub-system/equipment having a SIL level lower than that of the overall system cannot reduce the safety of the overall system.
- **Operation with external influences:** This section shall demonstrate that when subjected

to the external influences defined in the System Requirements Specification.

- **Safety-related application conditions:** This section shall specify the rules, conditions and constraints which shall be observed in the application of the system/sub-system/equipment.
- **Safety qualification tests:** This section shall contain evidence to demonstrate successful completion, under operational conditions, of the Safety Qualification Tests.

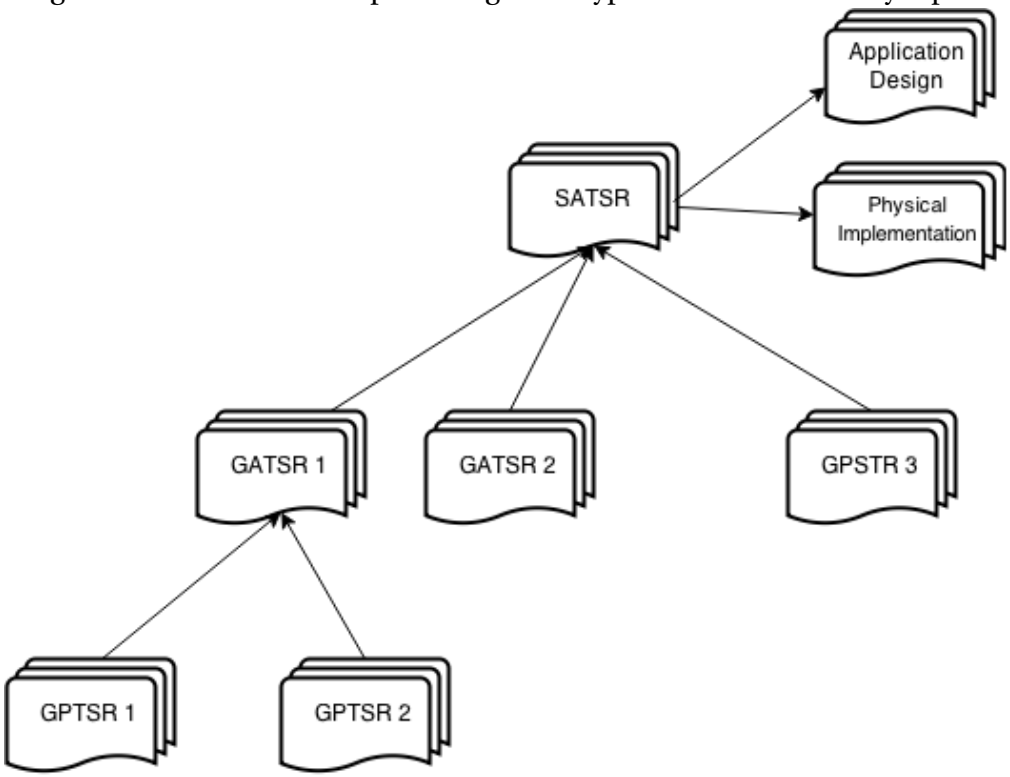
Since the technical safety report is one part of safety case, this report shall have three categories, i.e. *generic product technical safety report*(GPTSR), *generic application technical safety report*(GATSR) and *specific application technical safety report*(SATSR). Two interesting questions are what are the relationships among those three technical safety reports and what are the contents in each type of technical safety report.

For a generic product, it is usually Off-The Shelf system/component that is designed for safety-critical application in railway. It is a commercial benefit for the vendor to obtain some form of certification, e.g. SIL level for this generic product. However, this generic product will eventually become a part of other systems. It is therefore essential to provide enough raw evidences about safety in the GPTSR according to standard. When a generic application uses this generic product, the vendor of the generic application can verify whether the safety requirement of its generic application can be achieved based on the GPTSR of that generic product.

Further, the generic application may be used for an installation, namely, a specific application. The GATSR of this generic application can be used as an evidence for the development of SATSR, if this generic application fulfills the functional and safety requirements. The SATSR includes two parts, one for the design and one for the physical implementation. The former one contains the evidences that can demonstrate that it is safe to accept this installation assuming that the application is correctly installed. The latter one gives the evidences that the application is installed in accordance with the assumptions made in former technical safety report. The reason for this is that the physical implementation is often related to the concrete condition of the installation. It is therefore that the final testing is possibly only a short time before the system is to be brought into use. Because of this, it is practical to approve the design of a technical solution first before it begins to install this specific application and to test this application. The real implementation related to this application shall be approved based on the evidences

of safety-related activities, i.e., records of control activities and testing of this application in the infrastructure. An illustration of the relationships among these three types of technical safety report is in the Figure 5.1.

Figure 5.1: The relationships among three types of technical safety report



Chapter 6

Evaluate of Existing Technical Safety Report

6.1 Adoption of TSR for Existing Installations

Five generations of interlocking systems have been implemented in Norway, namely, NSB-63, NSB-84, NSB-87, NSB-94 and Merkur. Since EN 50129 can only be applied to electronic signaling system, only NSB-94 and Merkur should have their technical safety reports. However, it had been difficult to prepare the technical safety reports retrospectively for NSB-94 since it was implemented before EN 50129 was published. Three types of technical safety reports should be prepared for Merkur since it was developed after the introduction of EN 50129.

In addition to technical safety reports, which are delivered as a part of *Safety Case* by supplier, a safety report should be prepared by railway authority and should be delivered to safety regulatory authority. According to Safety Regulation,the safety report is the superior document which should demonstrate that the safety activities defined in the safety plan are carried out with satisfactory results. The hazard log shall also be included, and this shall show how each element in it is handled, closed or transfered to safety following plan. This report is mandatory for the overall safety acceptance of commissioning of signaling system.

6.2 Report 1 SATSR for NSB-94

It will evaluate mainly four parts of a technical safety report in this and next sections, that is, *fulfillment of system requirements specification, fulfillment of safety requirements specification,*

assurance of correct hardware functionality and *effects of faults.*

The report evaluated here is the SATSR for Harran station(Grong - Mosjøen)(Jernbaneverket, 2005).This report followed the report structure suggested in EN 50129. However, the first impression of this report is that this report did not completely fulfill the requirements listed in standard since the total pages of it are only 10 pages. The purpose of the technical safety report is to convince the authorities that the system is safe to operate. Based on the contents in this report, it is hardly to demonstrate the safe design of the system. The main reason is due to lack of solid and logic argumentation to prove its safety. Some examples are discussed below.

The system requirements specification(SRS) addresses the customer's requirements and expectations. It is therefore important to provide the necessary evidences for the demonstration of fulfillment of SRS. In this case, it is essential to show how the system can be adapted into Harran station. It referenced to a lot of documents to demonstrate the fulfillment of SRS. For instance, it referenced four sketches including schematic plans of internal and external system and interlocking table. A fundamental question related to those documents is which requirements are fulfilled by providing those documents. It is not straightforward to understand how schematic plans and interlocking table can be linked to the fulfillment of system requirements. It did not claim which requirements they wanted to demonstrate conformance. Moreover, whether it is sufficient to only provide those four documents is questionable, since it did not explain how the claim of fulfillment of requirements could be built up on the basis of these four documents.

It seems more problematic to demonstrate the fulfillment of safety requirements specification in this report. First and foremost, the safety requirements are not defined for NSB-94 system(Jernbaneverket, 2005). It did not mentioned the safety-critical functions and their associated safety targets for NSB-94 in this report. However, it defined project-related safety requirements for design and implementation (Jernbaneverket, 2005). Unfortunately, the two problems talked above still existed, and it is difficult to verify how the requirements were fulfilled by provided evidences.

Regarding to the effects of faults, it referred to a generic safety case. In this generic safety case, it stated that a FMECA was performed to identify the undetected failures including single faults, systematic faults and hidden faults. The CCF was not considered in this report.

6.2.1 Reliability Assessment in This Report

In this part, according to EN 50129, it shall describe the system hardware architecture and explain how the design achieves the required integrity in respect of reliability, availability, maintainability and safety.

This report did not provide any evidences that can meet requirements above. In particular, any evidences that may be linked to reliability assessment, which is our focus in this thesis, are not able to be identified.

When talking about safety, it justified that the correct hardware functionality was ensured by using standard components and configurations as those "Proven in use" systems have already been in operation. It referred to another document that stated:

> NSB-94 signaling system has been in operation on 11 stations and there are not system failures or dangerous failures demonstrated in those systems.
>
> The total operation time for NSB-94 is over 550000 hours.

EN 50129 does not give any guidelines about how to use "Proven in use" arguments to demonstrate conformance with requirements. Only providing these two statements without giving any reasonable argumentation is therefore not sufficient to prove that it has achieved the required integrity, even though the statements may describe the fact. To improve this, according to IEC 61508, it may emphasize on how to build solid documentary evidence to demonstrate that the likelihood of any dangerous systematic faults is low enough that the required safety integrity levels of the safety functions that use this system is achieved, based on the analysis of operational experience of this system(IEC, 2010).

6.3 Report 2 GPTSR for Merkur

The report evaluated here is the GPTSR for Merkur(Lundteigen et al., 2005). This report was developed after EN 50129 had been published. Compared with previous report, regardless the type of technical safety report, this one explained comprehensively about the technical aspects of Merkur product. For instance, it described the different redundancies of Merkur for the improvement of availability and evaluated how systematic approaches used for achieving the re-

quired systematic safety integrity level. However, there are still some issues in this report. Some of them are discussed in this section.

The first thing that needs to be said is that Norwegian National Rail Administration(NNRA) did not define the system requirements and safety requirements separately. It used requirements specifications to cover both system requirements and safety requirements. Thus, it only demonstrated how Merkur fulfilled the requirements specifications from NNRA. This did not followed strictly as EN 50129 required to demonstrate them separately. NNRA may distinguish system requirements and safety requirements in the future work.

To ensure the fulfillment of requirements from NNRA, it carried out a verification activity, i.e., *verification of fulfillment of requirements in EN 50129*. In particular, it evaluated techniques and measures for the avoidance of systematic faults listed in Table E.4, Table E.5, Table E.6 and Table E.10 in Annex E of EN 50129. The results were documented as an attachment in the TSR and the conclusion was that Merkur fulfilled those requirements. It is to be doubted whether this is a good way of evaluating the techniques and measures for the avoidance of systematic faults that were used in Merkur product. Since the systematic faults have different effects in the different life-cycle phases, a number of activities shall be performed at each phase(CENELEC, 2003). For this purpose, some suggested techniques and measures are listed as tables in Annex E of EN 50129. In my opinion, only verification of these techniques without saying how they are used in each phase is not sufficient. For instance, methods to identify and evaluate the effects of faults are given in the Table E.6 in EN 50129. In the report, it gave the references to the documentation in which those methods were used. It did not explain how these methods were used in the referred documentation and why using those methods could reduce the systematic faults. It may be difficult for the safety assessor to understand the purpose of providing those documentary evidences and time-consuming for them to verify those evidences. For example, it referred "RAM and safety plan report" when evaluating *Preliminary Hazard Analysis* technique in Table E.6. A curious safety assessor may ask why it mentioned this report here and what he could get from this report. The safety assessor has to look into this report and to identify the useful information himself.

It discussed how the hardware could contribute to the correct functionality in the section *assurance of correct hardware functionality*. Although it explained clearly how Merkur achieved

correct functionality, it did not comply with requirements defined in EN 50129. Same as previous one, it did not provide any evidences that could prove the design achieved the required integrity in terms of RAMS in this section.

When talking about effects of faults, it followed the structure suggested in EN 50129. It evaluated the failures in different modules that could lead the signaling system to the critical failure state. A FMEA that covered single faults and double faults was attached at the end of the report.

6.3.1 Reliability Assessment in This Report

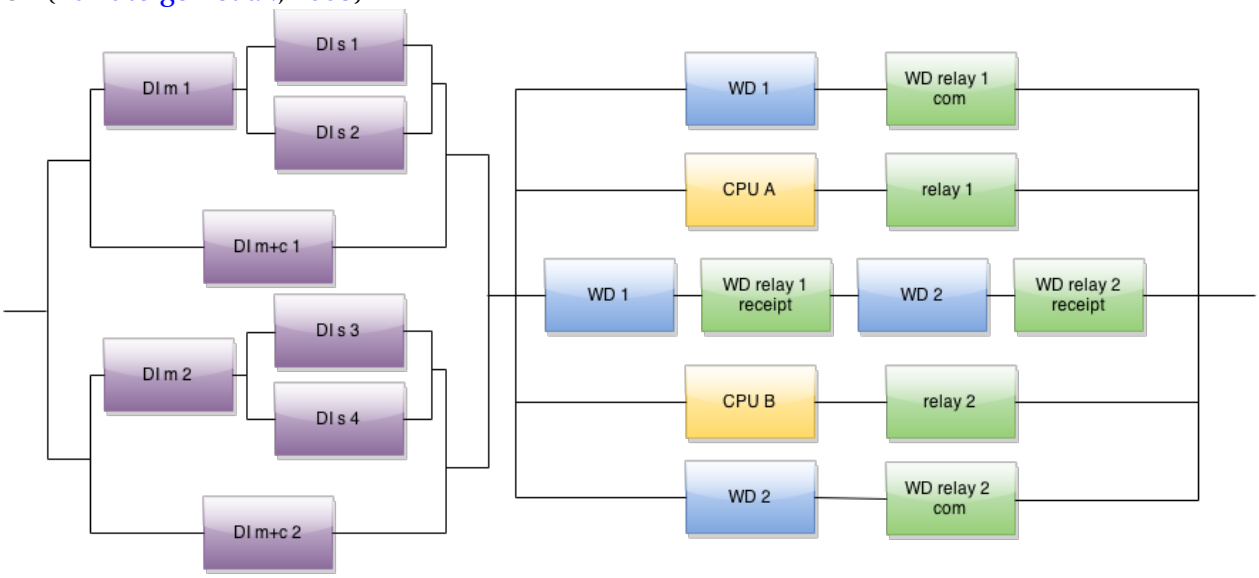
In this report, it defined a safety-critical event called "erroneous green light". The functional diagram of the interlocking system is illustrated in Figure B.1.

A short description of the components is:

- **DI**: Digital input modules that take care of input signals
- **DO**: Digital output modules that transfer the results from CPU to WDs.
- **WD**: Watch dogs that monitor the I/O dynamically
- **CPU**: Central processing unit, including PLC A and PLC B, is responsible for safety-critical tasks
- **PLC C**: is responsible for non-safety-critical tasks
- **Relays**: Safety relays
- **WD relay**: There are two types of this relay. *WD relay com* is the relay connected with WDs that ensures that CPUs are no failures and can communicate with I/O modules. *WD relay receipt* is the relay connected with WDs that monitors that feedbacks of output relays agree with relay's program status.

The hazard rate of such event was calculated based on Reliability Block Diagram(RBD) in this report. This method will be studied in this part, and will be compared with Fault Tree Analysis(FTA) in Chapter 8.

Figure 6.1: Reliability block diagram for "prevent setting erroneous green light", modified based on (Lundteigen et al., 2005)



The following formula is used in this report in order to fine total failure rate:

$$\lambda_{DU,TOT} = \lambda_{DU} \cdot \beta \cdot C_{koon} \tag{6.1}$$

where $\lambda_{DU} = \lambda_{TOT} \cdot (1 - DC) *$ Dangerous Failure Portion and $\lambda_{DU,TOT}$ is equivalent to THR.

Modification factors for voting configurations are defined:

- $C_{1oo3} = 0.3$
- $C_{1oo4} = 0.15$
- $C_{1oo5} = 0.1$

It should be noticed that in the newest PDS methods, these modification factors are slightly different(Hauge et al., 2013).

β-factors for systematic failures are defined(β_2 is used for tighter connection than β_1):

- $\beta_1 = 0.01$
- $\beta_2 = 0.015$

The average failure rate for n channel in the RBD 6.1:

$$\lambda_{avg} = (\lambda_1 \cdot \lambda_2 \cdots \lambda_n)^{\frac{1}{n}} \tag{6.2}$$

The average failure rate for each channel of DI:

$$\lambda_{DU,avg,DI} = \left(\left(\lambda_{DU,DIm} + \beta_2 \cdot \lambda_{DU,DIs}\right) \cdot \lambda_{DUm+c}\right)^{\frac{1}{2}} = 1.87311E-08 \tag{6.3}$$

Total failure rate for DI(1oo4 voting):

$$\lambda_{DU,DI} = \lambda_{DU,avg,DI} \cdot \beta_2 \cdot C_{1oo4} = 4.21E-11 \tag{6.4}$$

The average failure rate for channels with relays is:

$$\begin{aligned}\lambda_{DU,avg,relay} = \Big(&\left(\lambda_{DU,WD} + \lambda_{DU,WDcom}\right) \cdot \lambda_{relay} \cdot \left(\lambda_{DU,WD} \cdot 2 + \lambda_{DU,WDrelays} \cdot 2\right) \\ &\cdot \lambda_{relay} \cdot \left(\lambda_{DU,WD} + \lambda_{DU,WDreceipt}\right)\Big)^{\frac{1}{5}} = 1,7138E-08\end{aligned} \tag{6.5}$$

where the CPU is not included in this calculation since it is assumed that there is no CCFs between CPUs and relays.

The total failure rate contributed from relays are :

$$\lambda_{DU,relay} = \lambda_{DU,avg,relay} \cdot \beta_2 \cdot C_{1oo5} = 2,57E-11 \tag{6.6}$$

The total failure rate contributed from independent failure of relays and CPU is:

$$\begin{aligned}\lambda_{DU,ind,relay+CPU} = \Big(&C_{1oo3} * \beta_2 \cdot \Big(\left(\lambda_{DU,WD} + \lambda_{DU,WDcom}\right) \cdot \left(\lambda_{DU,WD} \cdot 2 + \lambda_{DU,WDrelays} \cdot 2\right) \\ &\cdot \left(\lambda_{DU,WD} + \lambda_{DU,WDreceipt}\right)\Big)^{\frac{1}{3}}\Big) * \left(\lambda_{DU,CPU} \cdot \beta_1\right) \cdot (1-\beta)^2 \cdot 2 \cdot \frac{\tau}{3}\end{aligned} \tag{6.7}$$

where $\tau = 15$ years is the test interval for signaling system.

In Formula 6.7, β-value was not defined in the report. It is unclear why this β was introduced. To proceed the calculation, it is therefore assumed that this β has the same value as β_1 or β_2. The corresponding results of using different β-value are $6.16E-16$ and $6.10E-16$. The results are

almost the same, $6.16E-16$ is chosen for further calculation, i.e. using $\beta = \beta_1$.

The total failure rate for hardware in signaling system is:

$$\lambda_{DU,TOT,HW} = \lambda_{DU,DI} + \lambda_{DU,relay} + \lambda_{DU,ind,relay+CPU} = 6.79E-11 \tag{6.8}$$

Reflections about this methods

This approach is a very straightforward way to calculate the failure rate. However, some assumptions were not mentioned in the report and they might confuse the readers who do not have such knowledge. In the following part, it will explain thoroughly about the ideas behind this method.

This method is an adoption of PDS-method(Lundteigen et al., 2005).In this report, it used only equation 6.1 to calculate the total failure rate. In the PDS-method handbook, it states that:

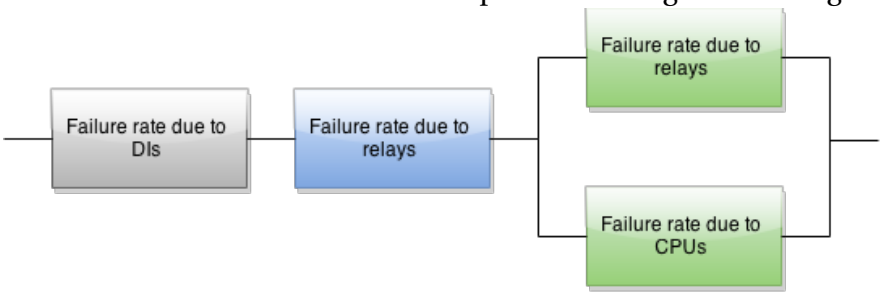
> The rate of common cause failures explicitly depends on the configuration, and the beta-factor of an MooN voting logic maybe expressed as:
>
> $$\beta_{MooN} = \beta \cdot C_{MooN}(M < N) \tag{6.9}$$
>
> This means that if each of the N redundant modules has a failure rate λ_{DU}, then the MooN configuration will have a system failure rate due to CCF that equals to $C_{MooN} \cdot \beta \cdot \lambda_{DU}$.

Hence, equation 6.1 is the failure rate due to CCF. The results of equation 6.4 and 6.6 were CCFs due to systematic failures. The total failure rate of a system consists of "independent" failures and CCFs. When including CCF into the calculation of total failure rate, the total failure rate will be dominated by the CCFs. It is therefore in this report only equation 6.1 was used for the calculation of the total failure, i.e., only CCFs were accounted for the total failure rate.

The RBD in Figure 6.1 was presented for a success-oriented network describing the function of "prevent setting erroneous green light". This function fails if all channels of left side of RBD fails or all channels of right side of RBD fails. It may be, in an extreme case, that all components fail simultaneously. In this report, it considered three situations that would lead to the system failure. The first situation was that all channels of the left side of RBD failed, calculated

by equation 6.2. The second situation was that relays of the right side of RBD failed, calculated by equation 6.6. In the third situation, it treated failure rate due to CPUs and failure rate due to relays as two independent cases. The idea of calculating the total failure rate is illustrated in Figure 6.2.

Figure 6.2: Total failure rate of the function "prevent setting erroneous green light".



Some uncertainties were related to the use of this method to calculate total failure rate. It is doubted whether it was appropriate to calculate the total failure rate for DI by using Formula 6.4. The result of Formula 6.3 was the average failure rate for two upper channels of DIs in RBD. It could not represent for the average failure rate of four channels of DIs in RBD, even though two upper channels and two lower channels are identical.

What was logic behind Formula 6.7 is uncertain. It is possible that the authors of this report might want to calculate the failure rate based on a Formula $\lambda_t = \lambda_1 \cdot P_1 + \lambda_2 \cdot P_2$, which has the same concept as Formula 3.8. λ_1 and λ_2 represent failure rates of two different channels in a parallel structure. P_x means that the probability one channel will fail if there is a failure in a parallel structure.

In Formula 6.7, the channels with relays but without CPU fail with a rate that was calculated in the first parenthesis. This is contribution to failure rate due to relays. It can be read from Formula 6.7 that the probability of a CPU fails given that the channels with relays failed can be calculate by $\left(\lambda_{DU,CPU} \cdot \beta_1\right) \cdot (1-\beta)^2 \cdot \frac{\tau}{3}$. It is not sure why it could use for calculating the probability of a CPU fails given that the channels with relays failed. $\lambda_{DU,CPU} \cdot \beta_1$ represents the rate of CCF due to CPU. The meaning of $(1-\beta)^2 \cdot \frac{\tau}{3}$ is difficult to guess.

Since it is hard to guess what was the purpose of using Formula 6.7, it proposes another approach to calculate the failure rate for the third situation. First, a DU failure, which may be relays(λ_1) or CPU(λ_2), occurs at some time t in $(0,\tau)$ and then another dangerous failure occurs

in the remaining part of the interval, that is, in (t,τ). The channel to fail first with a DU failure can be one of those two. The probability of this is

$$\begin{aligned}
\Pr &= \int_0^\tau (1-e^{-\lambda_2(\tau-t)})\lambda_1 e^{-\lambda_1 t}dt + \int_0^\tau (1-e^{-\lambda_1(\tau-t)})\lambda_2 e^{-\lambda_2 t}dt \\
&\approx \int_0^\tau \lambda_2(\tau-t)\lambda_1 dt + \int_0^\tau \lambda_1(\tau-t)\lambda_2 dt \\
&= 2\lambda_1\lambda_2 \int_0^\tau (\tau-t)dt \\
&= 2\lambda_1\lambda_2 [\tau t - \frac{t^2}{2}]_0^\tau \\
&= 2\lambda_1\lambda_2 \frac{\tau^2}{2} \\
&= \lambda_1\lambda_2\tau^2
\end{aligned} \tag{6.10}$$

The failure rate can be calculated as follows:

$$\text{FR} = \text{PFH} = \frac{E[N_G(0,\tau)]}{\tau} \approx \lambda_1\lambda_2\tau \tag{6.11}$$

By inserting equations for Formula λ_1 and λ_2 into Formula 6.11, the total failure rate contributed from independent failure of relays and CPU is

$$\begin{aligned}
\lambda_{DU,ind,relay+CPU} = \Big(C_{1oo3} * \beta_2 \cdot \Big(&\big(\lambda_{DU,WD} + \lambda_{DU,WDcom}\big) \cdot \big(\lambda_{DU,WD}\cdot 2 + \lambda_{DU,WDrelays}\cdot 2\big) \\
&\cdot \big(\lambda_{DU,WD} + \lambda_{DU,WDreceipt}\big)\Big)^{\frac{1}{3}}\Big) * \big(\lambda_{DU,CPU}\cdot\beta_1\big)\cdot\tau
\end{aligned} \tag{6.12}$$

Compared with Formula 6.7, Formula 6.12 gives a more conservative result, which is about $\frac{1}{3}$ larger, than Formula 6.7 since $(1-\beta)^2 \approx 1$. This result does not have significant impact on the final result, $\lambda_{DU,relay}$ and $\lambda_{DU,relay}$ dominating the final result, but it is a easier way to understand the logic behind the formula.

Chapter 7

A proposed Approach for the Development of Technical Safety Report

7.1 Problems from Existing Technical Safety Reports

From previous chapter, two different types of technical safety reports were evaluated. Some problems may influence the quality of the technical safety report. To summarize, three representative problems are going to be discussed here. Firstly, it is not clear what the technical safety report wants to demonstrate. The concept of the technical safety report is used in the sense as the documented functional and technical safety demonstration, i.e. the demonstration of the system concerned complying with the system requirements and safety requirements. It is therefore crucial to have a clear claim of what system requirements or safety requirements it want to demonstrate conformance. If there are several requirements that need to be complied with, it may have different claims respectively. In such way, the safety assessor will understand easily the purpose of the demonstration.

The next problem concerns about the quality of evidences. Some evidences were provided in the reports. Unfortunately, it may be confusing to understand why these documentation were referred. There was no clue how to combine them to the requirements to which it wanted to demonstrate compliance.

Finally, the argumentation and its quality were not satisfactory and comprehensible. The argumentation is the bridge that connects the claim and the evidences. A good argumentation

shall be constructed in a logical, valid and sound way so that the safety assessors are convinced that the claim is true in terms of given evidences.

7.2 Proposed Approach for Developing a Technical Safety Report

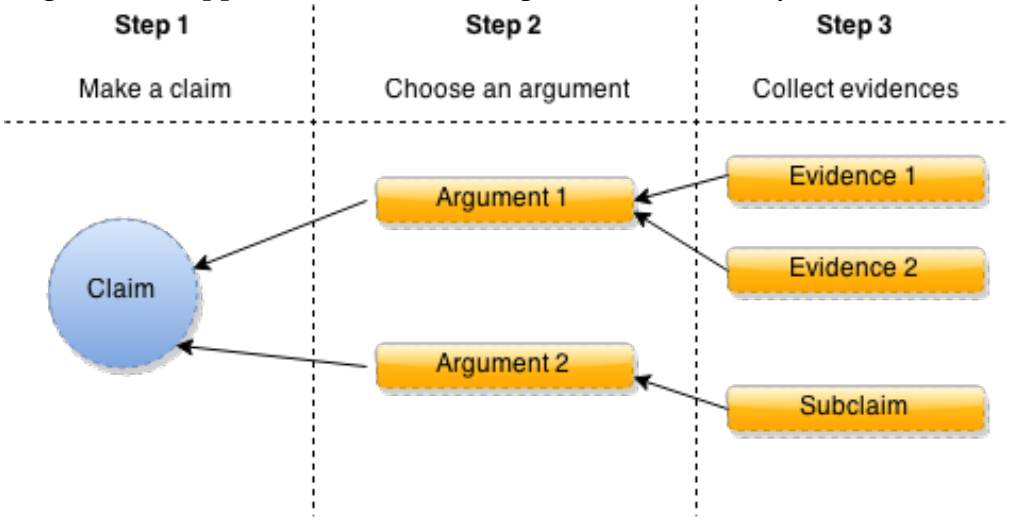
In order to achieve approval and acceptance to put the system into operation, the technical safety report must present the claims in such way that the safety assessors are convinced that the system can be accepted as adequately safe for its intended operation. Two principles for the approval and acceptance of a system are whether the system requirements and safety requirements are taken into consideration in the technical solutions and whether the technical solutions fulfill these requirements (Sivertsen, 2013).

A good technical safety report should be developed in such way that those two principles are reflected in the report. The systems concerned here vary from application to application. It may be a generic product, a generic application and a specific application in terms of their generality. The context for different applications of a technical safety report may be focused on different aspects, even though the structure of the technical safety report follows the guideline. It is difficult to propose an approach for developing a technical safety report without any relevant experience. Considering the issues identified from previous reports, it will propose a way of constructing a reasonable safety demonstration which can be served as a fundamental principle for all types of technical safety reports. This approach is proposed in the Figure 7.1.

The claim is the thing that you want to demonstrate and has to address the context suggested in EN 50129 Clause 5.4. It should be constructed in a clear manner that a safety assessor understands what you are doing in the following part of technical safety report.

The argument is the bridge linking the evidences and claim. Thus, the argument should be sound, logic and comprehensible(Sivertsen, 2013). Argument needs to also reflect two principles for the approval and acceptance of a system mentioned above. The argument should therefore demonstrate that necessary and appropriate analysis methods have been adopt. Moreover, the argument should present that the methods have been correctly applied, in a way that it is sufficient to convince a safety assessor of the fulfillment of the requirements. Finally, it must

Figure 7.1: A approach for constructing a reasonable safety demonstration



be proven that the specified requirements reflect the results of the analysis. Different types of argument can be used to support claims(Adelard, 1998):

- Deterministic application of predetermined rules to derive a true/false claim(given some initial assumptions), e.g. formal proof of compliance to a specification, or demonstration of a safety requirement(such as execution time analysis or exhaustive test of logic)
- Probabilistic quantitative statistical reasoning, to establish a numerical level(e.g. MTTF, MTTR, reliability testing)
- Qualitative compliance with rules that have an indirect link to the desired attributes(e.g. compliance with QMS standards, staff skills and experience)

The evidences are utilized for supporting the argument. An argument can have many evidences as long as they are sufficient and appropriate. As explained in the previous chapter, the technical safety reports can be constructed in a hierarchical way. A subclaim, which is derived from lower level arguments in a technical safety report for a safety-related electronic systems involved, can be also used as evidence. Such a recursive structure representing arguments can avoid bloated top document and reveal the evidences deep down in the document hierarchy.

One important question related to evidences is that what kind of documentation can be regarded as solid evidences. Considering two principles for the approval and acceptance of a

system, the evidences concerning the satisfaction of the requirements are essential to support the arguments. Some of examples are listed as follows:

- Verification reports from each phase of product life cycle: The essence of verification is to check that the product is being built right. This indicates that verification activities will ensure that the design complies with the requirements. The results of verification activities satisfy the first principle for the approval and acceptance of a system. It relates to assurance of correct functional operation.

- Validation reports from each phase of product life cycle: The essence of validation is to check that right product is being built. This indicates that validation activities will ensure that the product conforms to the requirements. The results of validation activities satisfy the second principle for the approval and acceptance of a system. It relates to assurance of correct functional operation.

- Reliability assessment reports: The reliability assessment includes functional analysis, fault tree analysis etc. It relates to assurance of correct functional operation.

- FMEA/FMECA: It will identify the failure modes, and their causes and effects of components or system. It relates to effects of faults.

7.3 Example of Claim

The THR for Merkur product was defined as $3.18E-10$ failure/hour by NNRA (Lundteigen et al., 2005). To demonstrate the fulfillment of this requirement, it can be demonstrated as:

Table 7.1: Demonstration of the fulfillment of random failure integrity

Claim	Argument	Evidence
Quantified Random Failure Integrity of the system is SIL 4	It performed a FTA for Merkur. The result indicates that the system fulfills SIL requirements, with a failure rate of 3.34E-13 failure/hour	See next chapter

The claim gives what it wants to demonstrate conformance. The argument gives why it conforms with the requirement, this is, a quantified result from FTA. The argument links the evidence, which shows in next chapter, to the claim.

Chapter 8

Reliability Assessment of a Signaling System

8.1 Fault Tree Analysis

The *Reliability Block Diagram* method used for reliability assessment of the signaling system in Figure B.1 was elaborated in the last part of chapter 6. This part will introduce *Fault Tree Analysis* method for calculating the failure rate of the signaling system.

The mathematic theories about FTA will not be introduced here, and more introductions can be found in (Rausand and Høyland, 2004) and (Rausand, 2013). The Fault Tree handbook (Vesely et al., 1981) gives a detailed guideline for constructing FTA.

In this case, a FTA modeling software, GRIF-Workshop, is used for modeling this signaling system. The most advantage of using this software, compared with RBD method, is that it does not require a lot of formulas to calculate the results. It only needs to type in the various data about the components, e.g. failure rate, test interval. This software will calculate R(t), A(t), PFD(t) or PFH(t).

8.1.1 Assumptions

The simplifications are the same as they were listed in the report (Lundteigen et al., 2005). Regarding to modeling of CCF, the β-factor modeling technique is utilized in this case. It assumes that a failure of a component will affect all the other same components with probability β.

Two different values for β are used for the calculation of failure rate, reliability and availabil-

ity. The aim is to see the impact of the CCF when other parameters remain the same. It assumes that only the same elements are subject to common cause failure, that is, the CCF can only occur between those same elements, see Table 8.1. The same β-values are assumed for all the CCFs.

Table 8.1: Results from GRIF-Workshop

DI m 1, DI m 2
DI m+c 1, DI m+c 2
DI s 1, DI s 2, DI s 3, DI s 4
PLC A, PLC B
WD 1, WD 2
Relay 1, Relay 2
WD relay 1 com, WD relay 2 com, WD relay 1 receipt, WD relay 2 receipt

Moreover, the test interval equals to 15 years in this case. The influences of test interval are not tested in this case, since the average $W(t)$ or PFH(t) goes down then the length of the interval increases while the reduction with time is very small(Rausand, 2013).

8.1.2 Results

The modeling of Figure B.1 by FTA can be found in the Appendix B.2 and B.3.

Table 8.2: Results from GRIF-Workshop

	$\beta = 0.05$	$\beta = 0.1$
$W(t)$ or PFH(t)	3.3439E-13	1.2944E-12
$R(t)$	0.9999999636	0.9999998586
$A(t)$	0.9999999856	0.9999999437

The results of the different values of β-factor are summarized in Table 8.2. Apparently, this result is much smaller than the result calculated by RBD method. The CCF is included as a virtual component in series with the parallel structure comprising the components of the common cause component group in RBD method. The CCF-related basic event is "OR-ed" to the basic events representing individual random failures of the same components in fault tree. For this reason, the different modeling techniques for CCF may cause the difference of the results.

Another reason may be the introduction of C_{MooN} modification factors. The intention of this factor is to distinguish the common cause failure contribution from various voting configuration. In the RBD method, applying this C_{MooN} to the geometric mean of the parallel connected

different elements may contribute to the difference of the two results. In contrast, FTA uses standard β-factor method.

In this analysis, it assumes that the whole system is proof-tested. In RBD method, only the CPU is proof-tested according to Formula 6.7. This may cause the different in the results.

The failure rate of system increases as the β-value increases. Even if $\beta = 0.1$, which is 100 times larger than it was used in RBD method, it still gives a lower value than RBD method. It can also be read from Table 8.2 that the β-vale has small impact on the reliability and availability.

The results meet the required THR value, which is 3.18^{-10} failure/hour(Lundteigen et al., 2005). It can be therefore concluded that this system is in compliance with the SIL 4 Random Failure Integrity requirement by using FTA method.

Chapter 9

Summary and Recommendations for Further Work

9.1 Summary and Conclusions

A general description of Norwegian railway signaling system was described in Chapter 2, including an illustration of how it can be applied in a two track station. It explained also some challenging problems in design of such two track station in Chapter 2.

The main SCFs of the signaling system were presented in Chapter 3. It explained why it preferred THR rather than PFD or PFH as reliability requirements in railway application. After that, some methods that can be used for setting and assessing reliability targets were introduced in Chapter 3. Particularly, a method that can be used for low-demand system was discussed in Chapter 3.

The technical safety report is one main part of the safety case to demonstrate technical safety of a railway signaling system. Thus, it introduced safety case in Chapter 4 first, and the relationship of different types of safety cases was discussed in this chapter. In Chapter 5, it identified the main content of a technical safety report and explained the relationship between technical safety reports generated for a generic product, a generic application and a specific application.

Two technical safety reports were evaluated briefly in Chapter 6. Some issues were identified from those two technical safety reports. The first one was that it was unclear which system requirements or safety requirements it wanted to demonstrate fulfillment of requirements. The

second one concerned about the quality of evidences. Finally, the quality of argumentation presented in the reports was not comprehensible enough. It elaborated in particular on the methods used to quantify the reliability of a function in both reports.

In Chapter 7, it proposed a way of constructing a solid safety argumentation which can be considered as the principle for developing all types of technical safety reports. The last chapter presented a fault tree analysis approach for assessing of the reliability of the functions.

9.2 Recommendations for Further Work

The most challenging task in this thesis is to elaborate PDS method used to quantify the reliability of a SCF in technical safety report of Merkur. Many assumptions were made for this RBD method but they were not fully discussed in the report. In particular, it was difficult to understand the way of modeling CCF. It may use standard β-factor to model CCFs for those components that have the same failure rates. Afterwards, this result can be compared with the result from PDS method to find out whether there is significant difference between two different modeling techniques.

The result from FTA is much smaller than PDS method. It is unfortunate that those two results are not comparable. It is common that FTA gives a more conservative result than RBD does. In this case, it gave totally an opposite conclusion. Some reasons that might cause this were discussed in the thesis, but it did not verify the correctness. In the future, it is interesting to investigate what are the causes that lead to an opposite conclusion.

There are some issues in the existing technical safety reports. If possible, it is very curious to learn some experiences from other countries. These experiences may contribute to the improvement of the quality of technical safety reports.

Appendix A

Acronyms

CCF Common cause failure

FTA Fault tree analysis

GPTSR Generic product technical safety report

GATSR Generic application technical safety report

HR Hazard rate

MTTF Mean time to failure

NNRA Norwegian National Rail Administration

RAMS Reliability, availability, maintainability, and safety

SCF Safety-critical function

SRS System requirements specification

SSRS System Safety Requirements Specification

SFI Systematic failure integrity

RFI Random failure integrity

SATSR Specific application technical safety report

Appendix B

Appendix

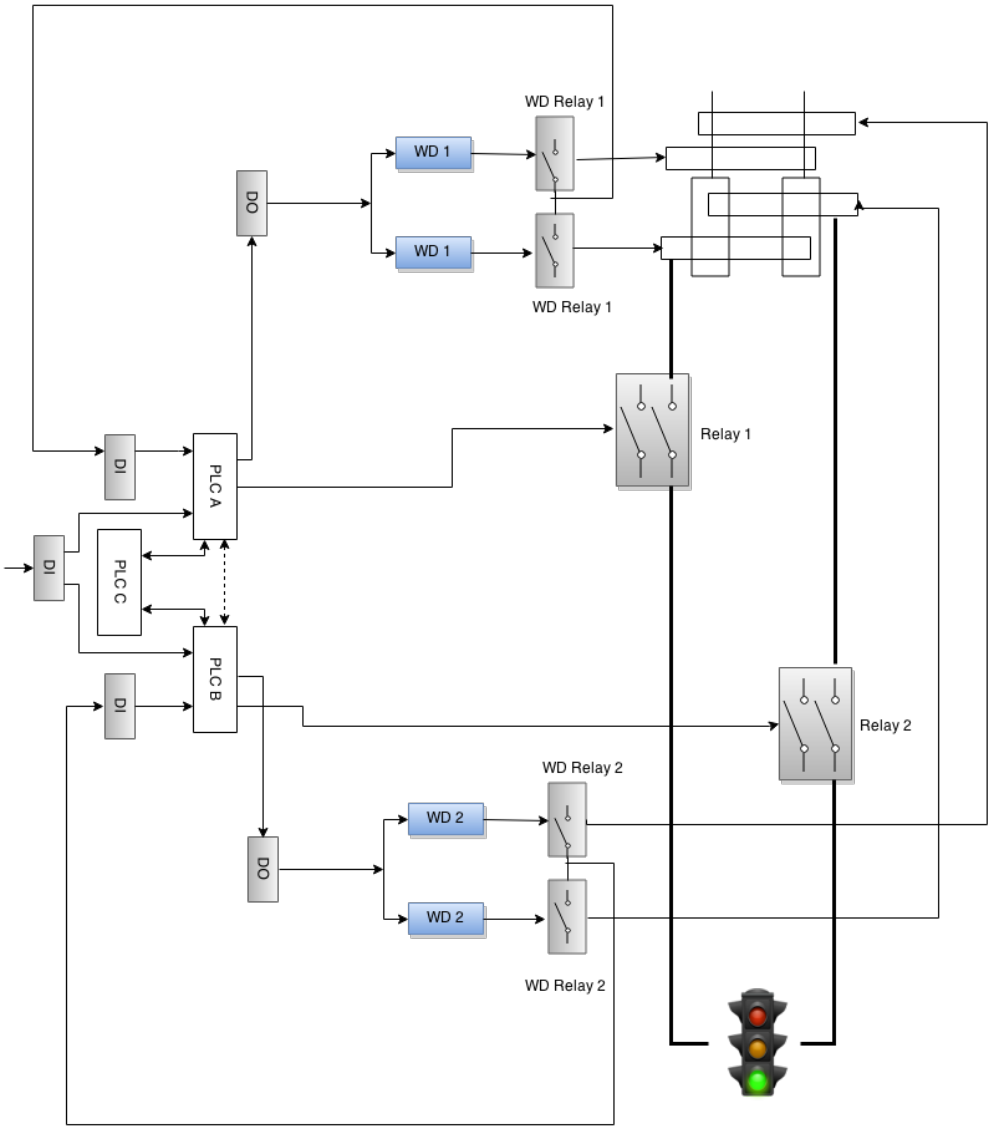
B.1 Failure rates for different components

Table B.1: Failure rates for different components(Lundteigen et al., 2005)

Components	λ_{DU}
PLC A & B	$6.5^{-9}/h$
Relay 1& 2	$1^{-8}/h$
DI m	$1.5^{-8}/h$
DI s	$8.2^{-9}/h$
DI m+c	$1.5^{-8}/h + 8.2^{-9}/h$
WD 1& 2	$4.8^{-10}/h$
WD relay com & receipt	$1.9^{-8}/h$

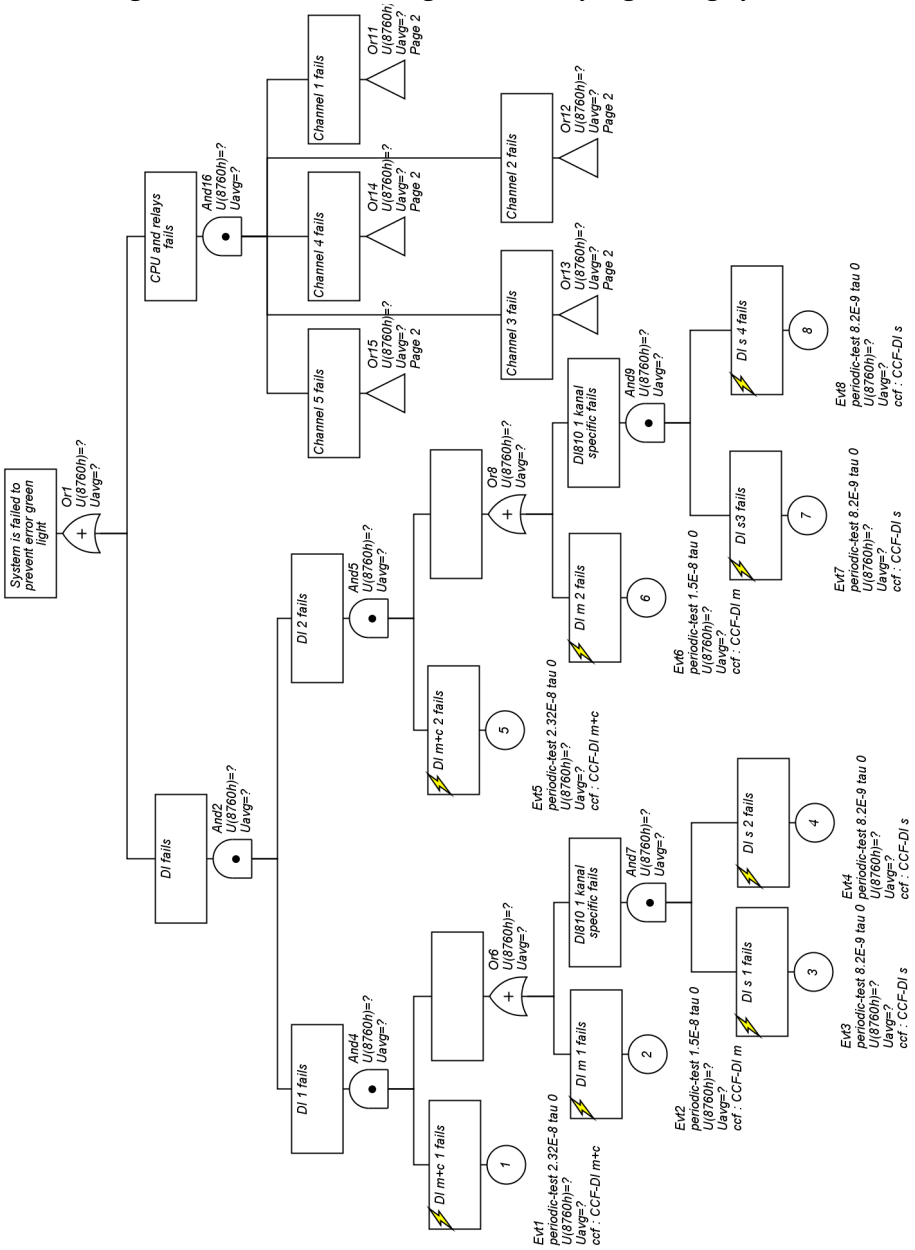
B.2 Functional diagram of a railway signaling system

Figure B.1: The functional diagram of a signaling system



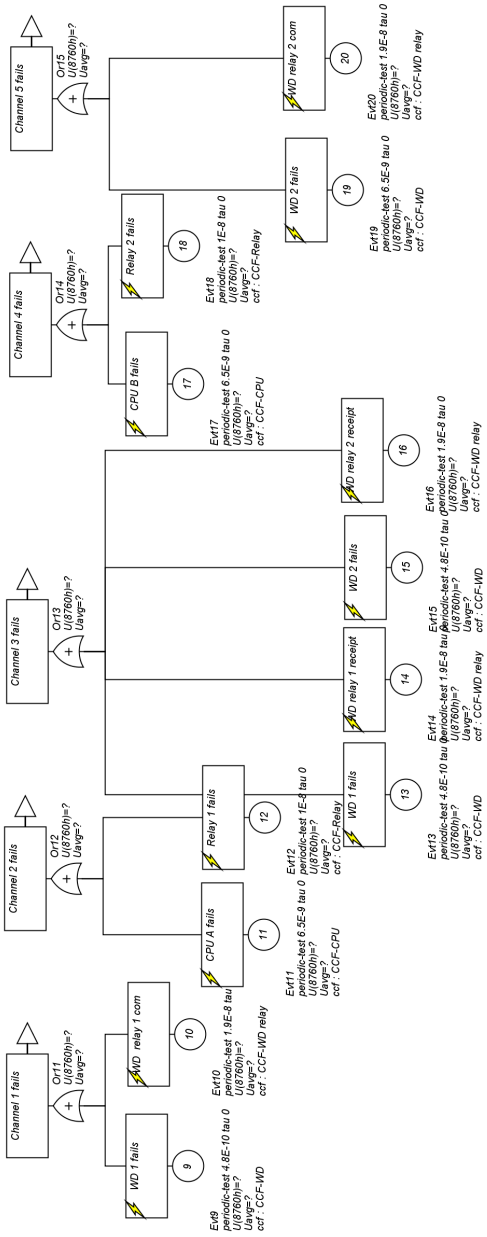
B.3 FTA modeling of a railway signaling system

Figure B.2: FTA modeling of a railway signaling system



B.4 FTA modeling of a railway signaling system

Figure B.3: FTA modeling of a railway signaling system, continued



B.5 Results from GRIF Fault Tree Analysis

Figure B.4: Results from $\beta = 0.05$

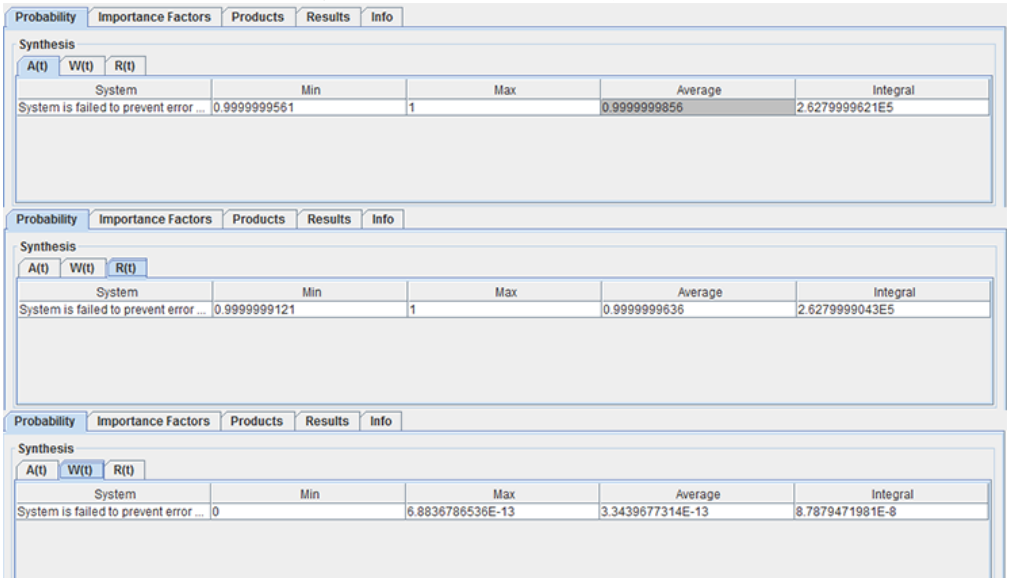
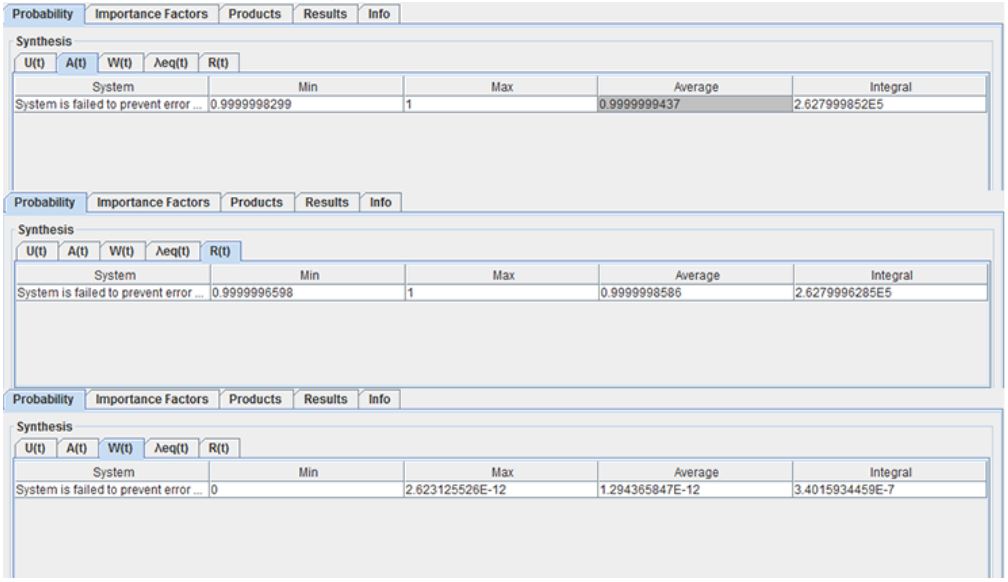


Figure B.5: Results from $\beta = 0.1$



Bibliography

Adelard (1998). Adelard safety case development manual. Technical report, Adelard.

Braband, J., vom Hövel, R., and Schäbe, H. (2009). Probability of failure on demand – the why and the how. In Buth, B., Rabe, G., and Seyfarth, T., editors, *Computer Safety, Reliability, and Security*, volume 5775 of *Lecture Notes in Computer Science*, pages 46–54. Springer Berlin Heidelberg.

CENELEC (1999). Railway applications - the specification and demonstration of reliability, availability, maintainability, and safety(rams), part 1: Basic requirements and generic process. Technical report, European Committee for Electrotechnical Standardization.

CENELEC (2003). Railway applications – communication, signalling and processing systems – safety related electronic systems for signalling. Technical report, European Committee for Electrotechnical Standardization.

European Commision (2012). Commission decision of 25 january 2012 on the technical specification for interoperability relating to the control-command and signalling subsystems of the trans-european rail system.

Hauge, S., Kråkenes, T., Hokstad, P., Solfrid, H., and Hui, J. (2013). Reliability prediction method for safety instrumented systems. Technical report, SINTEF Technology and Society.

IEC (2010). Iec 61508-2 : Functional safety of electrical/electronic/programmable electronic safety- related systems – part 2: Requirements for electrical/electronic/programmable electronic safety- related systems. Technical report, International Electrotechnical Commission.

International Railway Industry (2013). international engineering safety management: Good practice handbook. Technical report, International Railway Industry.

Jernbaneverket (2005). Spesifikk safety case for harran stasjon(grong - mosjøen). Technical report, Jerbaneverket.

Jernbaneverket (2015). Signal/prosjektering/generelle krav.

Løkberg, O. and Øien, K. (2005). Fordeling av tolerable hazard rates i signalanlegg. Technical report, SINTEF IKT.

Lundteigen, M. A., Bjertnes, A., Berstad, H., and Herrera, I. A. (2005). Teknisk sikkerhetsrapport merkur generisk produkt. Technical report, SINTEF IKT.

MODSafe (2011). Analysis of safety requirements for modsafe continuous safety measures and functions. Technical report, MODSafe Modular Urban Transport Safety and Security Analysis.

Nordland, O. (2000). Undertaking a safety case in a rail environment.

NTB (2015). Hver dag blir 223 tog forsinket eller innstilt.

Pachl, J. (2015). German block and interlocking principles.

Rausand, M. (2013). *Reliability of Safety-Critical Systems: Theory and Applications*. Wiley, 1st edition.

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

Sághi, B. (2012). Proposal for a generic aac process(guidance for case to case adaptation). Technical report, European Commission Seventh Framework Programme MODSafe Modular Urban Transport Safety and Security Analysi.

Scholz, S., Schuette, J., and Matousek, M. (2012). Analylsis of on-demand functions. Technical report, European Commission Seventh Framework Programme MODSafe Modular Urban Transport Safety and Security Analysi.

Sivertsen, T. (2013). Software safety demonstration.

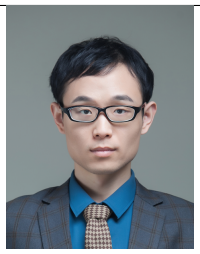
Theeg, G. and Vlasenko, S., editors (2009). *Railway Signalling & Interlocking: International Compendium*. EurailPress.

Vesely, W., Goldberg, F., Roberts, N., and Haasl, D. (1981). Fault tree handbook. Technical report, U.S. Nuclear Regulatory Commission.

Winther, T. (2015). Quick guide to safety management based on en 50126 / iec 62278.

Zhang, L., Li, T., and Xu, Y. (2014). Application of fault tree analysis in software safety integrity level allocation of train. In Jia, L., Liu, Z., Qin, Y., Zhao, M., and Diao, L., editors, *Proceedings of the 2013 International Conference on Electrical and Information Technologies for Rail Transportation (EITRT2013)-Volume I*, volume 287 of *Lecture Notes in Electrical Engineering*, pages 373–381. Springer Berlin Heidelberg.

Curriculum Vitae



Name:	**Lichao Tang**
Gender:	Male
Date of birth:	11.February 1985
Address:	Vegamot 1P,Rom 309 7048 Trondheim
Nationality:	Chinese
Email :	tlc.lichao@gmail.com
Telephone:	+47 97875216

Language Skills

- Norwegian Fluent in both oral and written
- English Fluent in both oral and written
- Chinese Mother Tongue

Education

- Norwegian University of Science and Technology

Computer Skills

- C, Java, Python
- LaTeX

Experience

- Technical Safety Summer Intern in Teekay Petrojal
- Part-time job in St.Olav Hospital

Hobbies and Other Activities

- Skiing, Reading
- Jogging