Comparison of Two Railway Signalling Systems in Denmark – Traditional Signalling and ERTMS

Filip Fiala, Filipe Alves Crusat & Vala Þöll Valgeirsdóttir

AALBORG UNIVERSITY
STUDENT REPORT

4th SEMESTER PROJECT

Master Thesis

MSc. RISK AND SAFETY MANAGEMENT

AALBORG UNIVERSITY, ESBJERG

January 10th 2019

Title

Comparison of Two Railway Signalling Systems in Denmark – Traditional Signalling and ERTMS

Theme

Master Thesis

Project period

Fall semester 2018

Project Group:

Risk-4-1

Participants:

Filip Fiala

Filipe Alves Crusat

Vala Þöll Valgeirsdóttir

Internal Supervisors:

Anders Schmidt Kristensen

Saqib Mehmood

External Supervisor:

Per Stoltze

Page Numbers

92

Date of Completion

10th of January 2019

Abstract

The aim of this project was to find out if it is possible to compare the Traditional Signalling system that has been used in Denmark for decades, with the new European Rail Traffic Management System, which is currently being implemented into the Danish railway system. Further their functions, hazards and safety barriers are analysed and also compared.

The system has been defined and the hazards identified based on the Common Safety Method. With a Hazard Log being used to for hazard identification, and Fault Tree Analysis to compare system performance in a similar hazardous situation.

The conclusion is that the two systems are comparable on the basis that both are safe to operate based on the CSM and Safety Directive. However, the systems do differentiate, when it comes to the functions, hazards and barriers.

SOLEMN DECLARETION

I hereby solemnly declare that I have personally and independently prepared this paper. All quotations in the text have been marked as such, and the paper or considerable parts of it have not previously been subject to any examination or assessment.

Preface

This project includes the authors' research study and analyses of the European Rail Traffic Management System and the older train management system used in Denmark referenced in this project as Traditional Signalling. The research report was conducted in collaboration with Atkins Engineering and design company, as a Master Thesis, which counts for 30 ECTS, during the 4th semester (Sep. 1st 2018– Jan. 10th, 2019) of the study program Master of Science in Risk and Safety Management at Aalborg University Esbjerg, Denmark.

The referencing style used for this report is IEEE. This is done by having a number within a squared bracket [X], which refers to the corresponding number in the bibliography. When directly quoting to a source quotations marks are used with the text written in italic. Tables and figures are marked with numbers, the first number referring to the chapter it is placed in, the second number depends on the order it is within the chapter. This project contains a list of abbreviations.

The contents of this thesis targets people working or interested in the Railway Industry and its future development and in Risk and safety Management.

The authors would like to thank Per Stoltze, chief engineer at Atkins Engineering and design company.

Aalborg University Esbjerg, 10th of January 2019

Vala Þöll Valgeirsdóttir
Bachelor in International Marketing and Sales
vvalge17@student.aau.dk

Filipe Alves Crusat
Bachelor in Emergency Management
fcrusat17@student.aau.dk

Filip Fiala
Bachelor in Planning and Management of Emergency Situations
ffiala17@student.aau.dk

Abbreviations

CSM - Common Safety Method

DMI - Driver Machine Interface

DSB - Danish State Railways

ERTMS - European Rail Traffic Management System

ETCS - European Train Control System

EU - European Union

GSM-R Global System for Mobile Communications for Railway

MA - Movement Authority

NGO - Non Governmental Organisation

RAMS - The Specification and Demonstration of Reliability, Availability, Maintainability, and Safety

RBC - Radio Block Centre

TSI - Technical Specifications for Interoperability

Table of Contents

List of Figures

List of Tables

1. Introduction

For the last few years Banedanmark has been working on changing the signalling system in Denmark from the old Danish State Railways (DSB) system to the European Rail Traffic Management System (ERTMS). This is a complex task, as some of the signalling systems in Denmark have not been updated or changed for years. As a result of that, a complete change of the system is necessary, as the existing system is reaching the end of its life cycle. To further complicate the process, Denmark is the first country to change the whole system in one go, even before the European Union has finalised the requirements for the system.[1]
This has caused many problems and in 2017 it was announced that the project had been delayed by 7 years due to unforeseen complications, and is now expected to be finished by 2030.[2] One of the reasons for this change now is that the ERTMS will reduce the delays due to signalling problems by astonishing 80%.[3]
The implementation of ERTMS is being conducted in stages in Denmark. The first track equipped with ERTMS was opened for passenger travels on 21st of October 2018, between Frederikshavn and Lindholm. [4] [5] These steps can be seen in Figure 1.1.

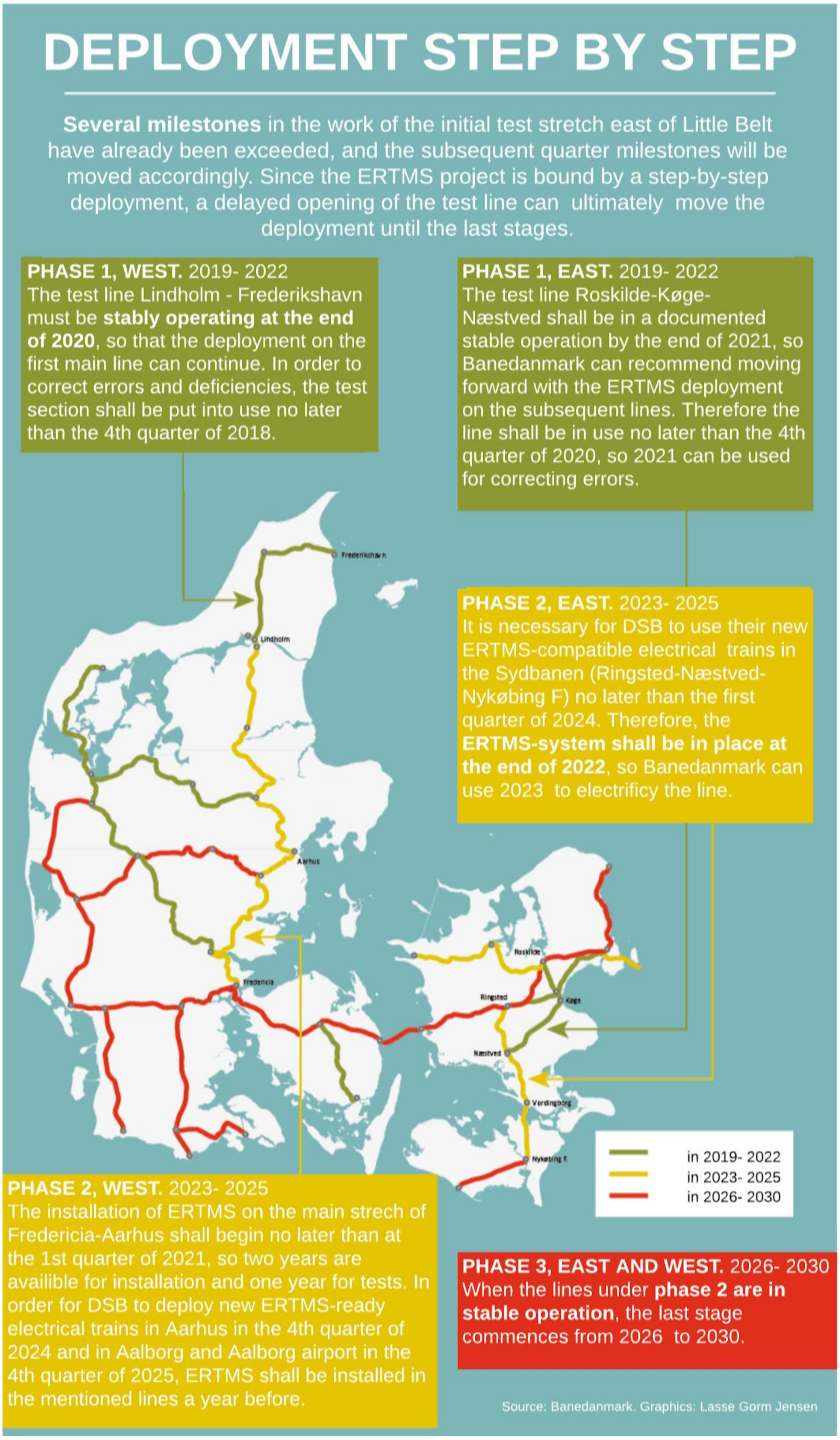


Figure 1.1 Translated Version of the Development Phases of ERTM is Denmark [2]

1.1 Problem Description

The current train management system in Denmark is being replaced by the new European Rail Traffic Management System. In some parts of Denmark, the train management systems in use have not been updated since the 1970s. What changes does that mean for small stations that are still using the older train management system? No publicly available study has been done so far as to the comparison of these two systems. There is no way of telling if systems developed this far apart are even comparable.

The purpose of this project is to find out if it is possible to compare these two systems, the Traditional Signalling nearing the end of its life cycle and the new European Rail Traffic Management System that is has just started to be implemented into service but is planned to replace the existing systems completely.

1.2 Problem Analysis

1.2.1 European Union Railway Safety and Interoperability

In 2008 the European Union sought to accelerate the integration of the rail network of its member states by establishing shared requirements and standards to guarantee high levels of safety and efficiency. This was done by launching the conditions for achieving interoperability of railways within the EU through compatibility with Directive 2004/49/EC on railway safety, resulting in Directive 2008/57/EC.

The EU adopted the Council Directive (EU) 2008/57/EC on the interoperability of the rail system within the Community on the 17th of June 2008. It became effective on the 19th of July 2008, and the deadline for it to be incorporated it into the national law of all member states was on the 19th of July 2010.

Since 2008, the EU has adopted the new Directive 2016/797 on the interoperability of the rail system within its member states. However, because the project of railway unification in Denmark commenced before the adaptation of the new directive of 2016, the Danish railway renewal project is still based on Directive 2008/57/EC. Therefore, this project of the Danish railway system is also based on the interoperability directive of 2008. For simplicity, Directive 2008/57/EC will be referred to as the 'Interoperability Directive' from now on.

Interoperability is for this purpose defined in the Interoperability Directive Article 2 (b) as:

"*…the ability of a rail system to allow the safe and uninterrupted movement of trains which accomplish the required levels of performance for these lines. This ability depends on all the regulatory, technical and operational conditions which must be met in order to satisfy the essential requirements.*"

The purpose of the Interoperability Directive can, therefore, be understood as an efficient railway system across the member states of the European Union, unified by regulatory, technical and operational conditions, which aim to revitalize the rail sector and provide a better quality of service for the passengers.

Safety on the railways in the EU is streamlined with "Directive 2004/49/EC of The European Parliament and of The Council of 29 April 2004 on safety on the Community's railways and amending Council Directive 95/18/EC on the licensing of railway undertakings and Directive 2001/14/EC on the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification." This directive will be referred to as the 'Safety Directive' from now on.

In Article 1 of the Safety Directive, it is required of member states to follow specific procedures when instating new railway projects such as using Common Safety Methods (CSM).

The Safety Directive Article. 4 binds the member states to continuously improve the railway safety where reasonably practicable. Article 6 (4) ensures that a revised version of the CSM is produced with regular intervals based on the experience gained with its application and international developments in railway safety, enabling the practical application of Article 4 and requiring member states to make amendments to their national rules accompanying CSM in Article 6 (5).

In the Interoperability Directive Article 1 it is mentioned that it is the intention that the interoperability is compatible with the Safety Directive. One of the requirements for interoperability is the level of safety of the railway sector. In the Interoperability Directive Art. 15 (1) it is mentioned that the procedures of implementation of railway services must be in accordance with the Safety Directive Article 4 (3) and 6 (3), where the latter states the purpose of the CSM.

The adaptation of the CSM used in the Danish railway project is found in the Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment. This regulation will be referred as the "Regulation of Common Safety Method".

The Regulation of Common Safety Method applies, according to Article 2 (1), when making changes to the railway system in a member state in a technical, organizational or operational manner. Article 2 (3) states that parts of The Regulation of Common Safety Method also applies if a risk assessment is required by the relevant technical specifications for interoperability (TSI) in the Interoperability Directive. The rules for the TSI are described in the Interoperability Directive Article 5 through Article 8, and for the special cases where member states are exempt of the rules, are set in Article 9.

For significant changes as described in Article 4 (2), the CSM risk management process stated in Article 5 elaborated in ANNEX I is necessary.

For the Danish railway project, the mentioned directives and associated articles are the foundation of the binding legislation. Other subjects also mentioned the legislation, such as rules for certification, and application requirements will not be used in this thesis, as they are not considered relevant.

The scope of the Union railway system within the Interoperability Directive art. 1, (1,2 and 4) and art 8, which is also shown in ANNEX I, is summarized in Table 1.1.

Scope of Directive 2008/57/EC				
Trans-European conventional rail system		**Trans-European high-speed rail system**		**Extension of the scope**
Network	**Vehicles (for national or international use)**	**Network**	**Vehicles**	**Cost safeguard considerations**
lines intended for passenger services,	self-propelling thermal or electric trains	high-speed lines equipped for speeds generally equal to or greater than 250 km/h,	at speeds of at least 250 km/h or operation at speeds exceeding 300 km/h	cost of the proposed measure
lines intended for mixed traffic (passengers and freight)	thermal or electric traction units,	high-speed lines equipped for speeds of the order of 200 km/h	at speeds of the order of 200 km/h	benefits to interoperability of an extension of the scope to particular subcategories of networks and vehicles
lines specially designed or upgraded for freight services	passenger carriages	high-speed lines which have special features & interconnecting lines between the high-speed and conventional networks		reduction of capital costs and charges due to economies of scale and better utilisation of vehicles
passenger hubs	freight wagons, including vehicles designed to carry lorries			reduction of investment and maintenance/operating costs due to increased competition between manufacturers and maintenance companies
freight hubs, including intermodal terminals				environmental benefits, due to technical improvements of the rail system
lines connecting the above mentioned elements				increase of safety in operation

Table 1.1 Scope of Directive 2008/57/EC

The scope of the subsystems is further elaborated in ANNEX II of the Interoperability Directive as summarized in Table 1.2. This project will focus on the signalling system between the network and the vehicles, as delimited in the subsystem categories “control-command and signalling” and “Telematics applications for passenger and freight services” in ANNEX II, 1.

Scope of the Union Railway Within the Directive	
Structural areas	**Functional areas**
Infrastructure	Traffic operation and management
Energy	Maintenance
Control-command and signalling	Telematics applications for passenger and freight services
Rolling stock	

Table 1.2 Scope of the Union Railway Within the Directive

Outside of the scope of the directive are local and regional railway systems that do not cross-national borders e.g. metros, trams and light rail systems.

The directive applies for the following aspects of the railway system life cycle as shown in Figure 1.2. Figure 1.2 illustrates how the directive relates to the railway system life cycle, where the blue boxes depict a generic system life cycle, while the white boxes illustrate the conditions that the directive sets requirements for which relate to the life cycle. The two first phases, of conceptual and preliminary design are not relevant in this case given that the system functions and components have already been designed, while the systems design in the directive relates to the customizations required for construction and implementation in each member state of the EU.

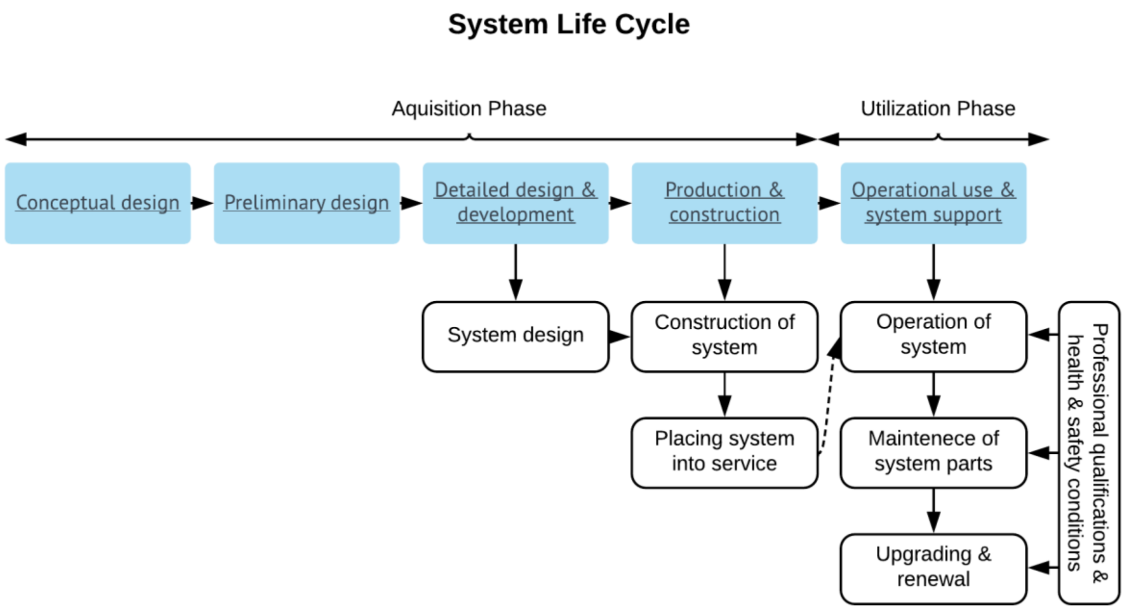


Figure 1.2 System Life Cycle

1.2.2 Railway Systems

An easy explanation of a railway system is a chain of subsystems that make it possible for a train to travel safely, and on time, from point A to point B. However, in the Safety Directive, a railway system is defined to be:

"...the totality of the subsystems for structural and operational areas, as defined in Directives 96/48/EC and 2001/16/EC, as well as the management and operation of the system as a whole".

Those definitions referred to are therefore listed here:
In the COUNCIL DIRECTIVE 96/48 EC of 23 July 1996 on the interoperability of the trans-European high-speed rail system an explanation of trans-European high-speed rail system is further explained in Article 2, as:

"(a) trans-European high-speed rail system" means the structure described in Annex I, composed of the railway infrastructures comprising lines and fixed installations, of the trans-European transport network, constructed or upgraded to be travelled on at high speeds, and rolling stock designed for travelling on those infrastructures".

Furthermore, in the DIRECTIVE 2001/16/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 March 2001, an explanation of the on the interoperability of the trans-European conventional rail system is explained in Article 2:

"trans-European conventional rail system" means the structure, as described in Annex I, composed of lines and fixed installations, of the trans-European transport network, built or upgraded for conventional rail transport and combined rail transport, plus the rolling stock designed to travel on that infrastructure."

Since this project is written with the guidance of the Safety Directive, and as the work that is done right now in regards to the problem at hand with the ERTMS and the signalling systems in Denmark, those definitions are used.

Additionally, the EU have further explained what the subsystems are, and what contribution they give to the system to make it possible to work efficiently.

1.2.3 Railway Subsystems

The railway subsystems have been divided into two categories, structural areas and functional areas. Structural areas consist of: Infrastructure, energy, trackside control-command and signalling, onboard control-command and signalling, rolling stock, and other (movable) railway material). Functional areas are then divided into: operation and traffic management, maintenance, telematics applications for passenger and freight services. According to the EU Commission directive 2011/18/EU Annex II 2.1 to Annex II 2.8.

Thus, these systems will be listed and further elaborated on, for further understanding based on the EU definition for each.

<u>Infrastructure:</u>
Everything that is built for the railway system, tracks, bridged, tunnels (other structures), stations (platforms, access points), along with protective equipment and safety.

Energy:

The way the trains gain electricity, the cables over the train and trackside consumption measuring system.

Trackside control-command and signalling

All the equipment that is used to communicate (command and control) to the trains that are authorised to travel on the railway network, to further ensure the safety.

Onboard control-command and signalling

This is all the equipment that is located on board the train, to ensure the safety and to ensure good communication to command and control the trains on the given authorised network.

Operation and traffic management

All the procedures that have to do with ensuring coherent operations of various subsystems. Both during driving the train, the planning of the driving and the train composition.

Telematic applications

The telematic applications can be divided into two elements, application for passengers and for freight services. The one for passengers includes, information sharing - both before and during a train journey, the ticketing and payment system, the management of luggage, and the management of connections between trains and other ways of transportation. The freight services telematic applications are similar to the passenger telematic applications, but is however focused on freight, as of that the system includes the information system that helps monitor real time of freight and trains, the marshalling and allocation system, reservation, payment and invoicing systems, the management of connection with other transportation and production of (electronic accompanying) documentation.

Rolling stock

The rolling stock includes all of the structure, command and control system for all of the train equipment, current collection devices traction and energy conversion units. Also including everything inside of the rolling stock, such as mechanical equipment such as braking, coupling and running gear (bogies, axles, etc) and suspension. Furthermore, it includes the doors, man/machine interfaces (driver, on-board staff and passengers, including the needs of persons with reduced mobility), along with passive or active safety devices and requisites for the health of passengers and on-board staff.

Maintenance

The maintenance means all of the procedures and logistics centres that are needed in order to maintain the railway system. This includes both the mandatory corrective and preventive maintenance that ensures the interoperability of the rail system, and guarantees the required performance, along with the associated equipment, and logistics centre for maintenance work and reserves.

1.2.4 Definition of Terms

To work most effectively with the concept of CSM, the following definitions are taken from the Commission Implementing Regulation (EU) No 402/2013 of 30 April 2013 on the Common Safety Method for Risk Evaluation and Assessment and Repealing Regulation (EC) No 352/2009, if not stated otherwise.

1.2.4.1 General Terms

Hazard

For the purposes of this project, "*hazard*" is considered to be a "*condition that could lead to an accident*";

Risk

"*Risk*" is considered to be the "*frequency of occurrence of accidents and incidents resulting in harm (caused by a hazard) and the degree of severity of that harm*", and will this definition be used in this project;

Shunting

That is when a train is moving on a route at a low speed without passengers, for purposes of e.g. starting a route from station A to B, connecting or disconnecting wagons, or etc. [6]

Movement authority

Is the permission a train gets to travel to a predetermined destination. [6]

Railway Accidents

In this project, "*Accident*" is considered to be "*An unfortunate incident that happens unexpectedly and unintentionally, typically resulting in damage or injury*". [7]

Accidents are further divided into two subcategories, catastrophic and critical. Definitions of those two are following:

"catastrophic accident" is considered to be *"an accident typically affecting a large number of people and resulting in multiple fatalities"*;

"critical accident" is considered to be *"an accident typically affecting a very small number of people and resulting in at least one fatality*"; According to,Commission implementing regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009)

In the railway industry there are further definitions for specific types of accidents, which are stated in the Safety Directive 2014/88 EU Appendix 1.5 - 1.11, and those accidents are categorized as following:

"*Collision, derailment, level-crossing accidents, accidents to persons caused by rolling stock in motion, fires and others."* (The Safety Directive: Annex I, 1.1)

Furthermore, in the same Safety Directive collisions are divided into two different groups, collision of a train with another rail vehicle and a collision of a train and an obstacle that is within the clearance gauge. A collision is when a train collides with another train either front to front, front to end, side to side, or if the train collides with another railway vehicle, or rolling stock (shunting). When there is a collision between a train and an obstacle within the clearance gauge, it means a collision between a part of the train and objects that can be either mounted or temporarily placed on or near the train track, e.g. with buffer stops (includes the overhead, however this does not include objects that are lost by a crossing vehicle or user on a level crossing).

A derailment is then explained to be when at least one wheel of the train goes off the rails. When it comes to the level crossing accident, those are considered to be when a train is in an accident at a level crossing, involving a minimum one vehicle that is crossing that level crossing and at least one railway vehicle, or with other crossing users (pedestrians) or objects (could be lost by users or passing vehicles) that are presented only temporarily at or near the crossing. The accidents to persons that involve rolling stock in motion are those accidents that involve at least one or more person, who are hit by a railway vehicle or an object attached or detached from the vehicle. These accidents include persons who fall from or inside the railway vehicle along with those who are hit by a loose object, while travelling on the train.

An accident that involves a fire in a rolling stock, is when there is a fire or an explosion that occurs either within the rolling stock, or in the goods it is transporting, while travelling between destinations (including while stopped at all the stations, along with departure and destination), along with remarshalling operations. The category of 'other accidents' are accidents that do not fit in previous listed categories.

1.2.4.2 Person Categories

In order to simplify the understanding of individuals associated by trains during an accident, the EU have made a categorization for persons, found in The Safety Directive 2014/88/EU Appendix 1.12 to 1.19. They have identified five different types of persons that are connected to trains. Those are:

Passengers: a person that is travelling with the train (excluding crew members). A person is considered to be a passenger both while boarding and leaving a moving train.

Employees (including contractors): are all individuals that are working in relation to railway at the time of an accident, such as the personnel onboard the train, employees working with rolling stock and infrastructure installations. This category does include people who are employed as contractors and self-employed contractors and working with projects related with railway.

Level crossing user: are any person that are using a level crossing to cross the railway track, by any type of transportation (car, bike, etc.) or by foot.

Trespasser: all persons whose presence around the railway is forbidden, however this does not consider level crossing users.

Other person at a platform: are those persons who are not previously mentioned, such as passenger, employee, level crossing user and trespasser, but are still located at a railway platform. Could for instance be a loved one that is either picking up or dropping off a friend or family member.

Other person not at a platform: those who are not at a railway platform, and do not fit into previously mentioned categories.

On top of these definitions, the EU has further defined what a killed person and seriously injured person means. Death, or killed person, are those who are killed either immediately or within 30 days after an accident, this does however not include suicides. Serious injury, or seriously injured person, is further explained to be, a person that is hospitalised for more than 24 hours, after being involved in a railway accident. This does not include suicide attempts.

1.2.4.3 System Definition

System definition, one of the three basic parts of risk assessment process. The other two being the risk analysis and the risk evaluation.

According Commission implementing regulation (EU) No 402/2013 of 30 April 2013, the system definition must include at least:

(a) system objective;

(b) system functions and elements, where relevant;

(c) system boundary including other interacting systems;

(d) physical (interacting systems) and functional (functional input and output) interfaces;

(e) system environment

(f) existing safety measures and, after the necessary relevant iterations, definition of the safety requirements identified by the risk assessment process;

(g) assumptions that determine the limits for the risk assessment.

Therefore, for the purpose of this project, this structure will be abided.

1.3 Common Safety Method

The process model has many similarities to The Specification and Demonstration of Reliability, Availability, Maintainability, and Safety (RAMS) process (EN 50126-1).

The Regulation of Common Safety Method process is iterative and comprised of four general phases which are significance evaluation, system definition, hazard record and safety documentation.

The first phase (significance evaluation) evaluates whether the changes are significant enough, as described in Regulation of Common Safety Method Article 4, to utilize this process. Only if the changes are found to be significant does the rest of the Regulation of Common Safety Method risk management process apply, as required in Regulation of Common Safety Method Article 5.

The second phase is the system definition where the system function, elements, boundaries, and interfaces are defined.

The third phase is the hazard record. This phase is comprised of three parts,

- the hazard identification and classification
- the risk acceptability

- the risk evaluation

The hazard identification is based on the preceding system definition. Next follows the risk acceptability that must be developed by one of three predefined acceptability methods as shown in Figure 1.3.

In the fourth and last phase, the product of the acceptability method must then be evaluated by documenting that the chosen risk acceptance principle is adequate and in compliance with the safety requirements for the system under examination.

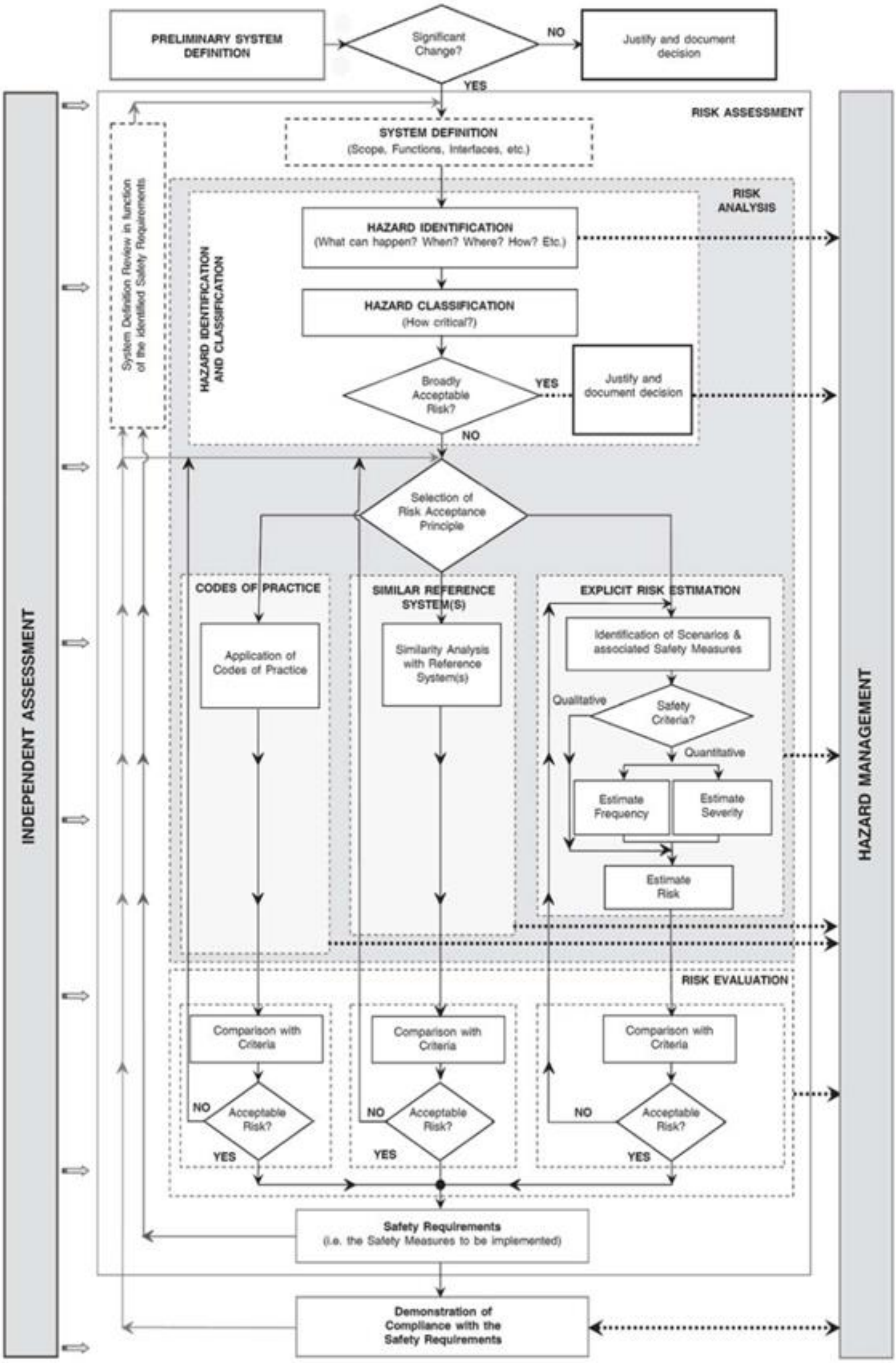


Figure 1.3 Common Safety Method (From the Common Safety Method Directive)

1.4 Traditional Signalling

Traditional Signalling has been around in Denmark for decades, but the system in question for this report has been in use since 1953. There have been some updates added to the system, however, for the purpose of this report those are not considered.

This Traditional Signalling system relies on an interlocking system. This system works in a way that when there is a required route for a train, meaning it is approaching a station and needs to access a certain platform. The train controller at the station needs to lock in the route, and if there are no obstacles, such as overlapping, or the track already being occupied, then it will lock the route so that the train can safely approach the station without any inconvenience. Thereby giving all signals connected to this specific route the appropriate signal to inform other trains if they are approaching this specific track. However, if there is already a train on the tracks, but is leaving, then the train could have the possibility to approach the station with caution. The control panel of the interlocking system at the train station would look similar to the one in Figure 1.4.

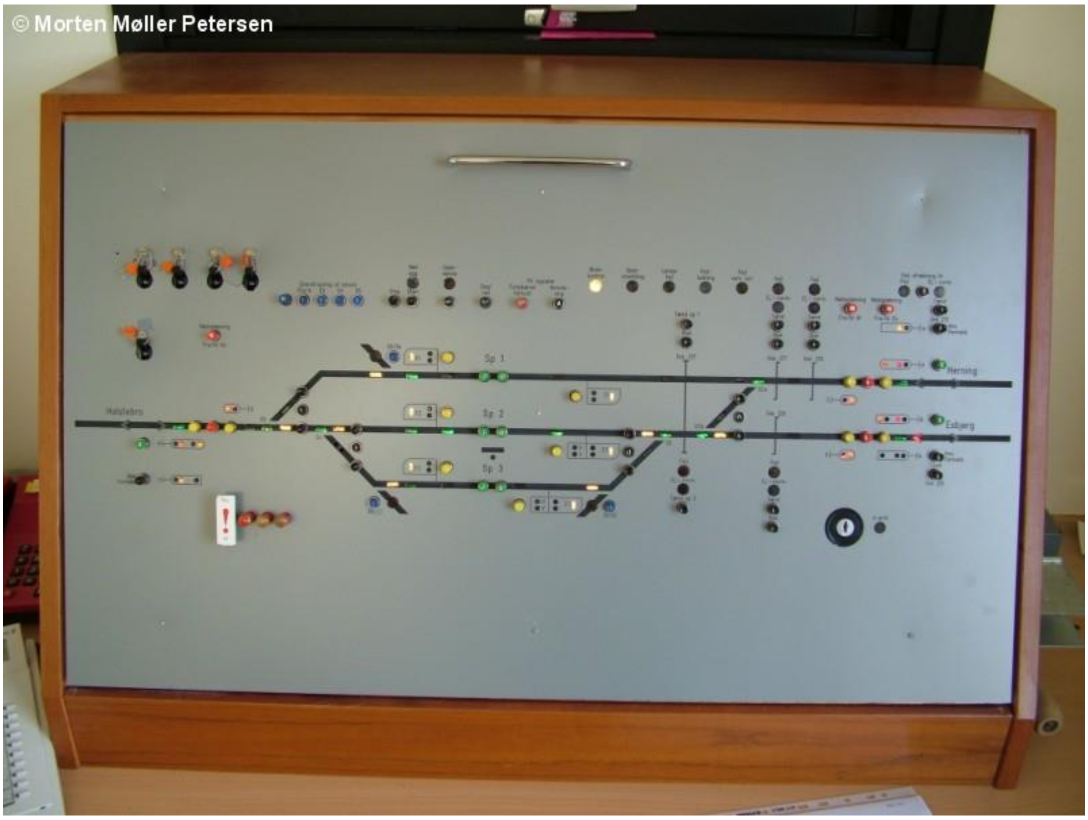


Figure 1.4 Traditional Interlocking System [8]

Traditional Signalling includes several different light signals located at the track side, which depending on the situation, will inform the driver of the availability of the track in front of him. These signals can for example show stop, drive, drive with caution and so on and can be seen in Figure 1.5. [9]

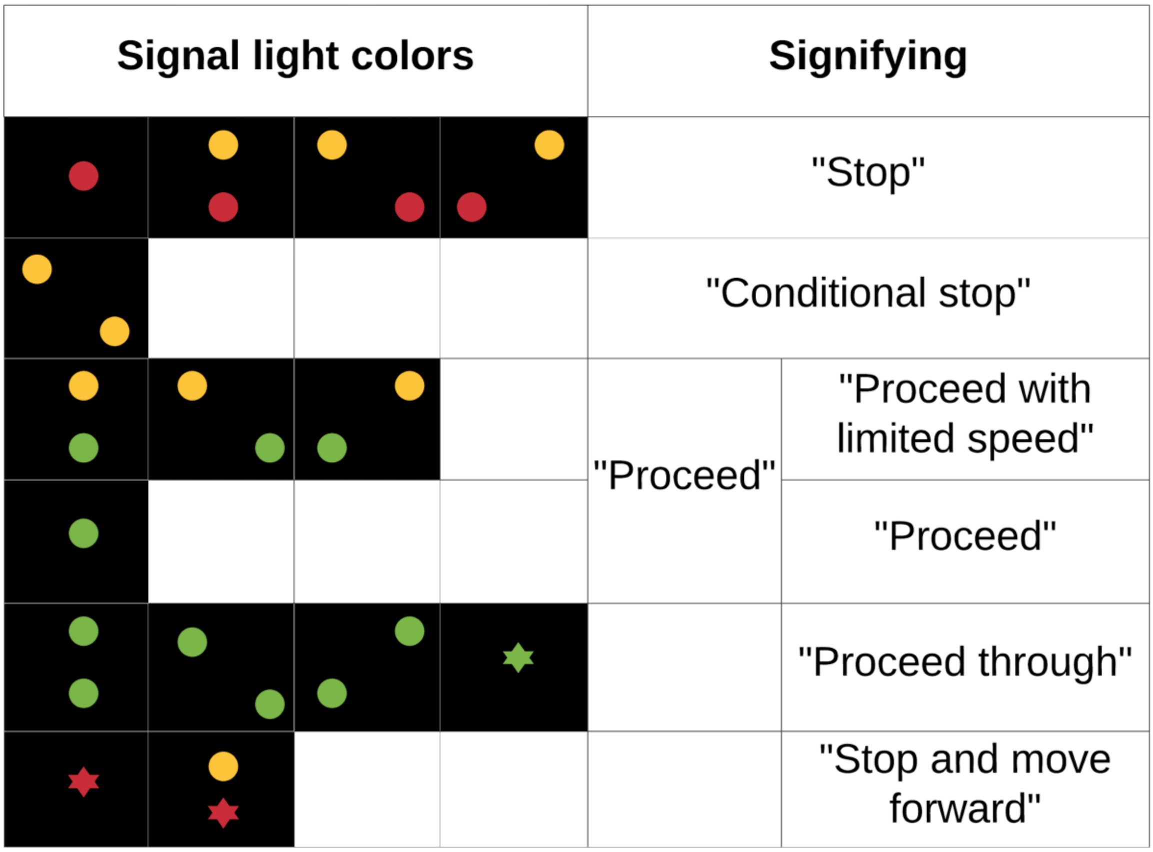


Figure 1.5 Traditional Light Signals (Translated version)[9]

Since this system has been in use since 1953, the system is fast approaching its full lifecycle. Resulting in the system failing more and more often, resulting in more frequent delays and it is also getting harder to repair. Further, this system is also not sufficient for the demands of modern railway.[10]

Figure 1.6, shows the station plan for Taulov station. It marks out the different tracks, the platform and other specifications such as the light signals. This plan is further explained in the System Definition for Traditional Signalling Chapter 6.5. The full plan is available in Appendix A along with Danish explanations about the content of the plan is in Appendix B.

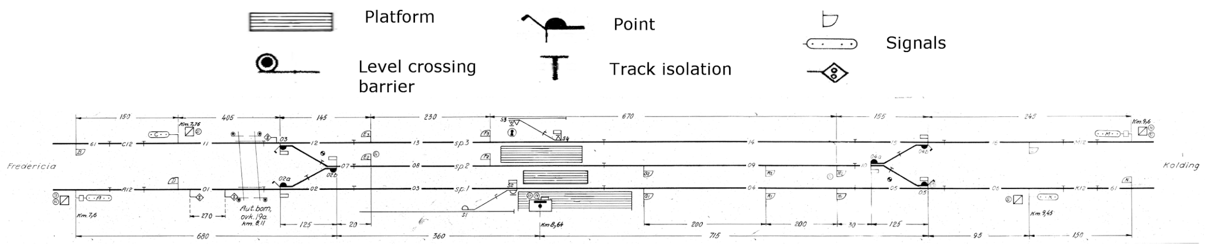


Figure 1.6 Station Plan for Traditional Signalling in Taulov (Picture from Atkins)

1.5 European Train Management System

The European Train Management System (ERTMS) is a common standard for railway traffic management, which consists of the train control system European Traffic Control System (ETCS) and radio system Global System for Mobile Communications for Railway (GSM-R). It is being made by eight UNIFE members, which are working in close cooperation with the EU, railway stakeholders and the GSM-R industry. This system is aimed to replace all the different train control systems that nations within the EU have, thereby making it easier to connect countries by trains.[11]

ETCS takes care of the signalling and train control part of the ERTMS. This is the system that constantly calculates what the allowed maximum speed is, it is further equipped with an on-board system that can take control of the train if the maximum speed limit is exceeded. On top of that the system continuously gives the train driver updated signals in an onboard display.[12]

There are three levels of ERTMS. Level 1 is an addition to an existing system, meaning that it works alongside a system that is currently in use. The communication between the train and the tracks are done through special belises, called Eurobalises, and those are located by the track sides, and are further connected to the train control centre. This means that there will be a ETCS equipment onboard, making it possible to automatically calculate and supervise what the maximum speed for the train is and further it can see where the next braking point for the train is if needed. That information gathered are then displayed to the driver on a screen dedicated for this system, also known as DMI (driver machine interface), which will be further explained later in this chapter. The system can also take over and brake the train, in case the maximum speed limit is exceeded.[13] This level is illustrated in Figure 1.7

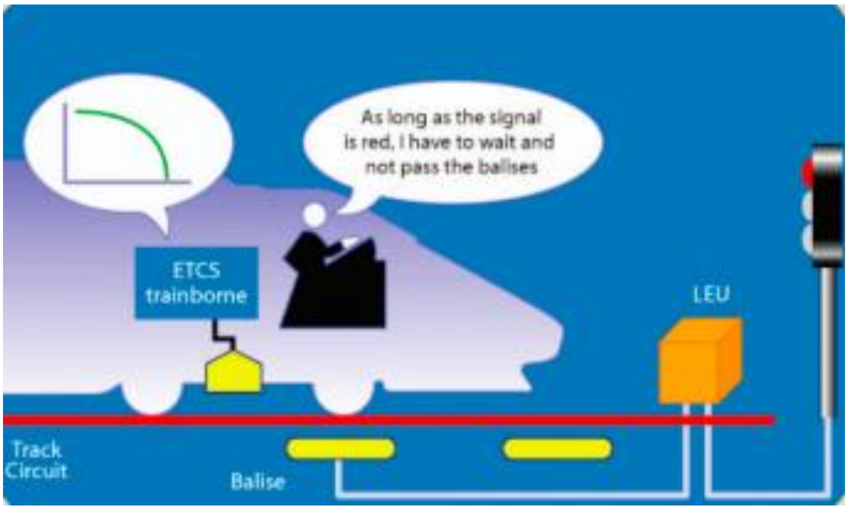


Figure 1.7 Level 1 of ERTMS [14]

When it comes to Level 2 of ERTMS, the interoperability and safety is the same as Level 1, however the landside signals are now gone, meaning that all the movement authority is communicated directly from the Radio Block centre (RBC) to an on-board unit using a radio channel (GSM-R). Then, the balises are only used to transmit the fixed messages, such as location, gradient, speed limit and etc. Those messages are then also displayed on the DMI. Thereby, the driver will be informed continuously on the line-specific data and the signals statuses on the route ahead, meaning that the train will be able to travel at either maximum or optimal speed at all times, and at the same time maintaining a safe braking distance factor. Not only that, but level 2 is expected to reduce the maintenance cost of the landside signals, and increase the efficiency of the tracks, since with higher speed and reduced headways will make it possible to have more trains on the tracks.[14] This is the level that is being implemented in Denmark.[3] This level is displayed in Figure 1.8.

Both Level 1 and 2 works with so called “fixed block”, which means that there is a specified area between two fixed points that cannot be used by two trains at the same time. This is however what differentiates level 3.

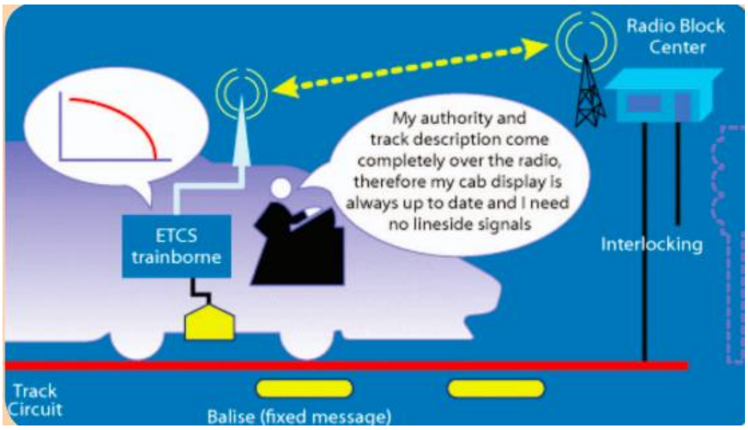


Figure 1.8 Level 1 of ERTMS [14]

For level 3, the idea is to have a moving block concept, meaning that the trains can come closer to each other, especially while travelling at lower speed. Thereby, it will eliminate the trackside train detection, along with the axle counters and track circuits.

With Level 3 a more accurate and continuous position data is supplied to the control centre directly by the train, instead of the track-based detection equipment. However, this level is still in development and has not been implemented yet.[14] [15] This level is shown in Figure 1.9.

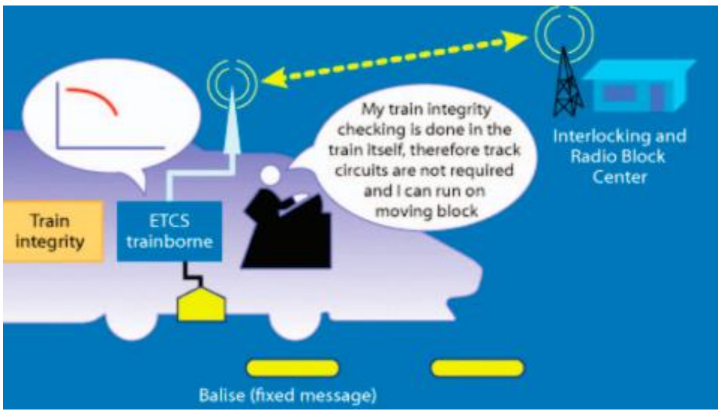


Figure 1.9 ERTMS level 3[14]

The DMI, or the in-cab display, informs the driver about various data. The display shows a speedometer that informs the driver of the current speed along with the allowed maximum speed. The track ahead is also displayed, with information about the gradient on the track ahead and when the speed limit will change. The DMI further displays other information's such as the TCS operation mode, the allowed distance the train can travel and the point when the driver needs to start braking in order to avoid the ETCS interference. The screen can be seen in Figure 1.10.[16]

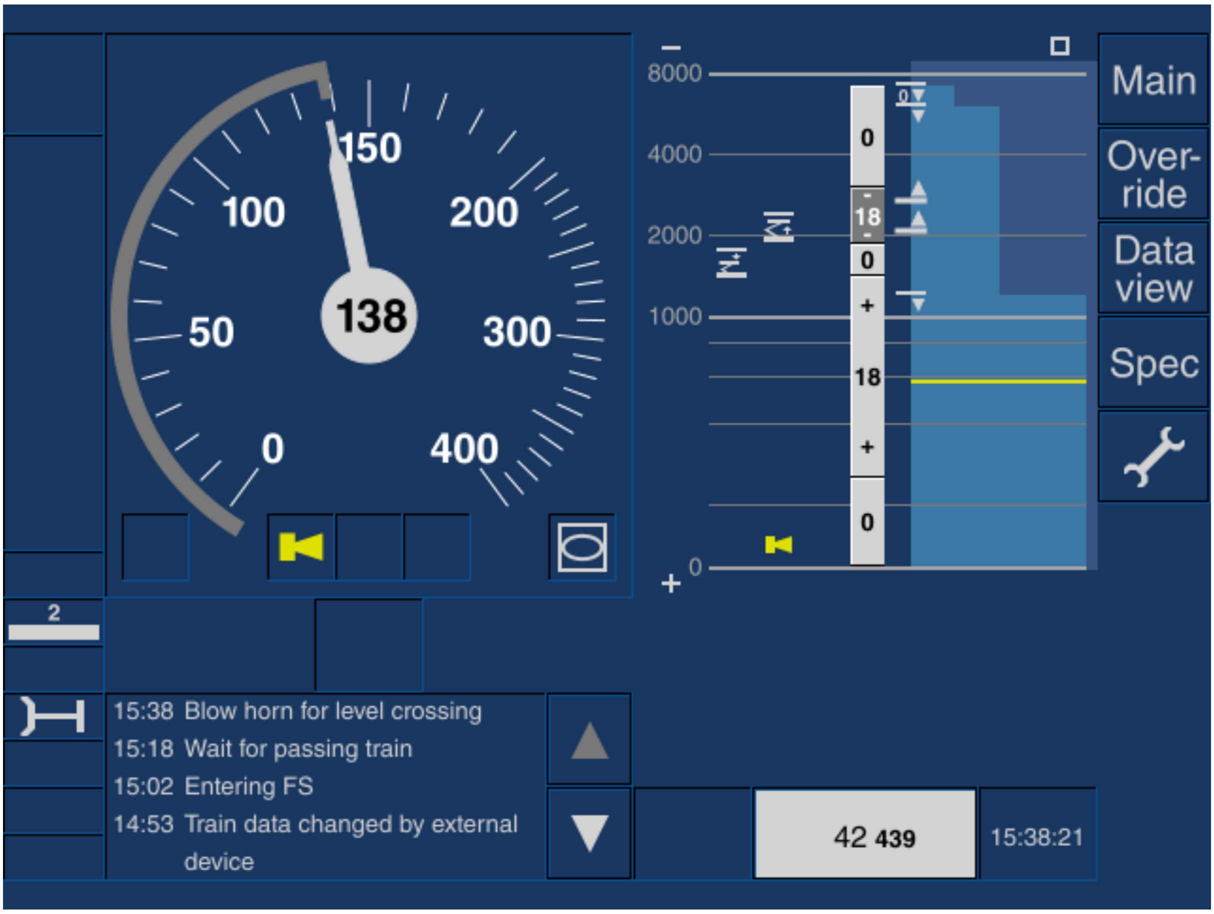


Figure 1.10 The Driver Machine Interface Display [16]

For the ERTMS the train will also have different levels of driving, such as stop and proceed with caution, drive on sight, shunting, along with having different levels of supervision from the ERTMS and ETCS system, those will however be further explained in Chapter 6.6.4, which discusses the safety measures and requirements.

The ERTMS system uses GSM-R. This is a radio system for speaking-and data communication between the train driver, traffic controller, the signal system and others. This is a wireless communication standard used in the ERTMS, which allows high quality communications at speeds up to 500 km/h, which enables the transition to high speed trains systems.[17] In 2017 it replaced the analogue radio systems previously used for railway communication.[18]

Figure 1.11 shows the station plan for Taulov station with the ERTMS. It marks out the different tracks, the platform and other elements. This plan is further explained in the System Definition for ERTMS in Chapter 6.6, along with a lager figure.

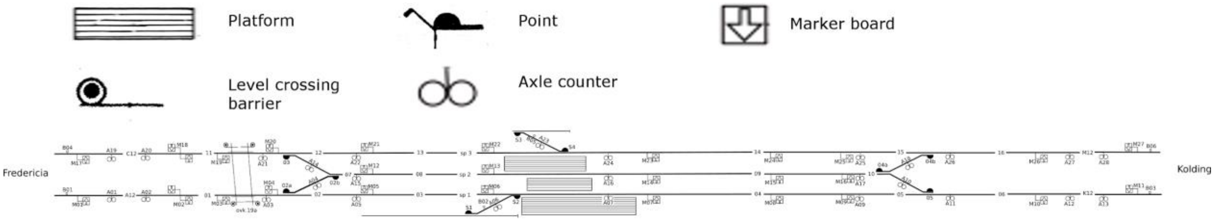


Figure 1.11 Station Plan for Traditional Signalling in Taulov (Picture from Atkins)

1.6 Stakeholders

To identify the key players, their influence and connections also in accordance with the CSM, the stakeholder analysis was conducted in order to better understand the Danish railway industry.

In the CSM stakeholders are mostly referred to as "actors," and their roles in the risk management process are found in Annex I, point 1.2.7 that establishes the main responsibility:

"Independently from the definition of the system under assessment, the proposer is responsible for ensuring that the risk management covers the system itself and the integration into the railway system as a whole."

Annex I, point 1.1.6 requires the identification of the involved actors, their responsibilities and the coordination between them:

"The first step of the risk management process shall be to identify in a document, to be drawn up by the proposer, the different actors' tasks, as well as their risk management activities. The proposer shall coordinate close collaboration between the different actors involved, according to their respective tasks, in order to manage the hazards and their associated safety measures."

Moreover, Article 5, point 3 demands that all risks introduced by the involvement of stakeholders are managed:

"The proposer shall ensure that risks introduced by suppliers and service providers, including their subcontractors, are managed. To this end, the proposer may request that suppliers and service providers, including their subcontractors, participate in the risk management process described in Annex I."

Many stakeholders may be involved in the CSM, but it is, in the end, the responsibility of the proposer to control the risks related to the significant change to the system, the application of the CSM, and to demonstrate that the change is safe.

The CSM regulation further requires that all actors (stakeholders) needed for the safety activities of the proposer are identified in the safety plan. The plan must also explain what is demanded of the stakeholders in ways of resources and responsibilities.

A suggestion for stakeholder categories needed for a CSM project could look like the stakeholder categories found in the EN 50126-1: 2017[19]:

- *"railway undertakings (railway duty holder);*
- *infrastructure managers (railway duty holder);*
- *maintainers;*
- *railway supply industry;*
- *safety authorities."*

Having the EN 50126-1 in mind, the list actors involved in the project could be:

a) Banedanmark as project proposer with the overall responsibility for documenting that all identified hazards and associated risks are contained to an acceptable level

b) Ministry of Transport, Building, and Housing.

c) Project Manager.

d) Other Infrastructure Manager or Railway Undertaking involved with the project, e.g., DSB, Arriva, Sydtrafik. Movia, freight train companies etc.

e) Supplier providing off-the-shelf products, e.g., Alstom, Ansaldo, Siemens, and Thales, etc.

f) Organization constructing to a given design, e.g., Deloitte implementing ETCS systems in DSB machines.

g) CSM Assessment body, e.g., TÜV SÜD, Ricardo Rail, etc.

h) Independent Safety Assessors, e.g., Atkins, COWI, Deloitte, Niras, etc.

i) Notified Body, e.g., TÜV SÜD, Ricardo Rail.

j) Designated Body, e.g., Ricardo Rail, Elklint Railway, Lloyd's Register, etc.

k) Danish Transport, Construction and Housing Authority under the ministry, as the Danish National Safety Authority (NSA).

l) Final product operator or maintainers, e.g., DSB, Arriva, Sydtrafik, Movia, and Banedanmark, etc.

m) Interfacing operators and maintainers such as municipal and regional authorities.

However, the list not complete. There may be many more stakeholders that must be included in the safety plan, but it shows some of the potential actors required for the CSM process. The definition of actors or stakeholders in the CSM and EN 50126-1: 2017 may be rather narrow.

For a given project one may want to consider cooperation with more than the apparent stakeholders that are officially involved in the phases of the project life cycle. In the risk management vocabulary, ISO guide 73 [20], a stakeholder is defined as:

"person or organization that can affect, be affected, or perceive themselves to be affected by a decision or activity."

This definition is quite broad and does not make a distinction between stakeholders and users, thereby allowing for the inclusion of more individuals and groups than those considered by the CSM regulation.

Additional stakeholders can, therefore, be added to the list such as:

n) the different types of system users, e.g., commuters, travellers, etc.

o) the surrounding structures, e.g., residential, public and commercial buildings

p) the users of interfacing systems, e.g., road users

q) environmentalist NGOs, e.g., Greenpeace and The Danish Society for Nature Conservation (DA: Danmarks Naturfredningsforening)

r) local and national news media sources

According to Donaldson and Preston [21], there is a divergence between stakeholders and influencers. Some actors might have influence and be affected by the project, some may simply have a stake in the outcome, and others may only have influence and not be affected by the result. The actors that only influence are classified as influencers. The media is an example of an involved party that only influences without any stake in the actual outcome of a project and are therefore not considered as a stakeholder according to Donaldson and Preston, but evidently can have an enormous impact on project activities, despite little or no legitimate claim. Power and legitimacy are separate attributes that sometimes overlap, so stakeholder identification must also accommodate these differences. Mitchell et al. [22] define power and legitimacy as primary attributes in stakeholder identification and add urgency as a factor as well.

Based on the power, urgency, and legitimacy factors Yosie and Herbst [23], classified stakeholders into four distinct categories.

Group 1. Those who are affected directly by the development.

Group 2. Those who are interested in the project, and want to become involved in the process and seek a chance to contribute.

Group 3. Those who are interested in the development of the project and may seek information.

Group 4. Those who are affected by the result but do not participate in the stakeholder process.

With these four categories, it is possible to group the stakeholders of the proposed CSM-RA project list previously shown into a affected and influence matrix, adapted from Attrup and Olsson 2008 [24], as an indicator of power and legitimacy, that can be used to prioritize how the stakeholder interaction should be done. The figure 1.12 below shows how such a matrix can potentially be instituted.

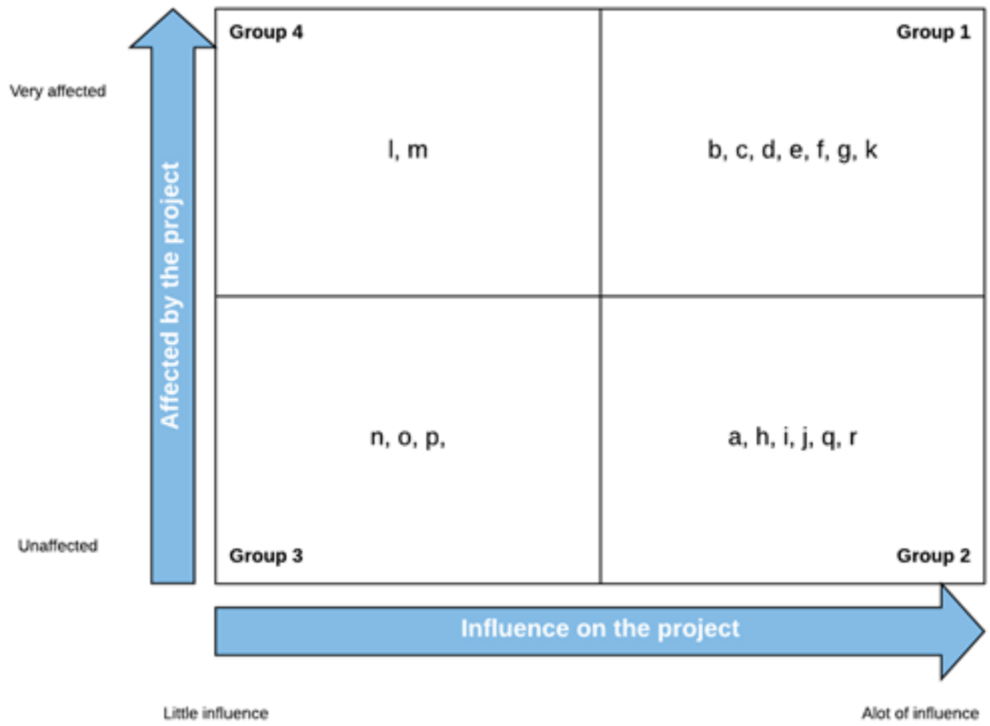


Figure 1.12 Power and Legitimacy Matrix [24]

The matrix can be expanded further with more boxes if a more detailed segmentation of stakeholders is required. By this figure, it is basically identified who has the authority to make decisions in the CSM process and whose active participation is essential for the process execution. By understanding this, it is easier to identify what type of risk communication each actor entails and how to prioritize the outgoing messages.

A communication or collaboration strategy can be developed for each group of stakeholders granting a structured consideration of the stakeholders' needs. This can be done by considering what to expect of a stakeholder, be it support or resistance, by reflecting on what the stakeholders' risk perception is of the two systems, their interest in the project and if there are any conflicts of interest among them. This can be explored by considering the benefits and disadvantages in relation to the project for each party, and what type of risk debate is most accepted by the stakeholder.

According to Renn [25], knowledge, and expertise will not always be sufficient to reassure a person of safety. He, therefore, differentiates between three levels of risk debate required depending on the complexity of the subject and the intensity of the conflict (as seen in Figure 1.13).

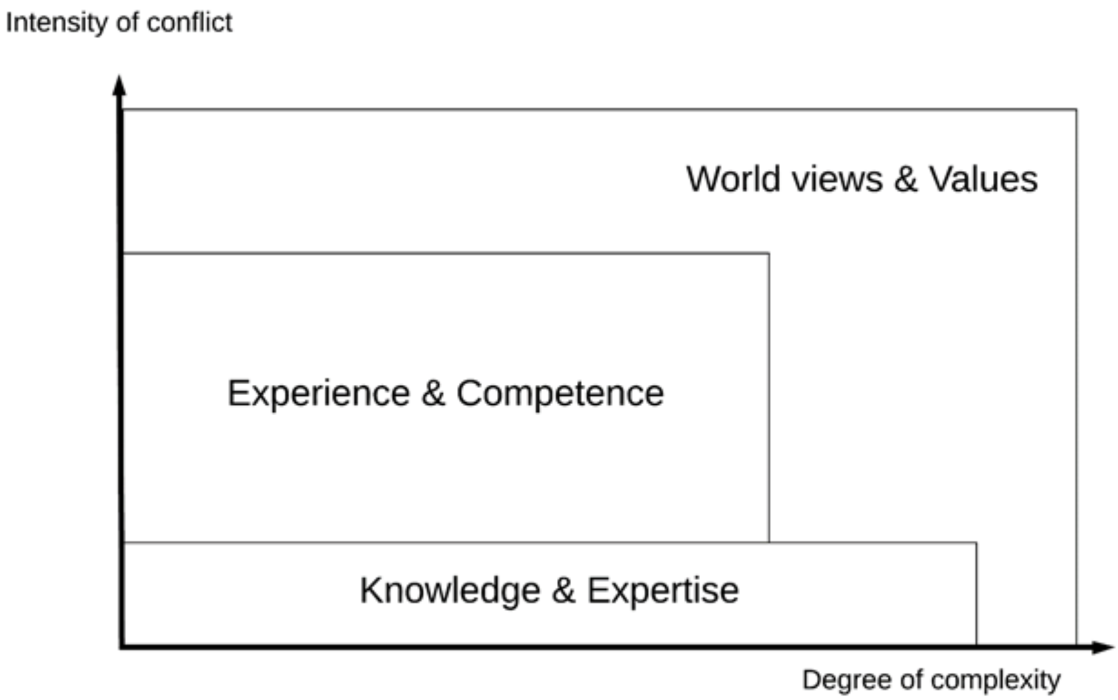


Figure 1.13 Levels of concern in risk debates adapted from Renn [25]

The first level is where arguments based on knowledge and expertise are sufficient. At this level the conflict of risk perception is low, and therefore adequate data and analysis based on this information is enough to satisfy the debate unless the complexity of risk is very high. In these cases, values and worldviews are needed in the argumentation.

For the second level, the divergence of risk perception is somewhat elevated. Here, experience and competence with the specific risk are essential for a constructive debate. However, if the degree of complexity is high, worldviews and values again play an important role in the considerations of risk. If the intensity of conflict and degree of complexity are very high, the discussion of risk will mostly if not only be accepted as a discussion of worldviews and values.

The railway is a complicated system comprised of many complex subsystems with numerous stakeholders involved. Which means that the debate of risk in the railway system can easily advance to a high intensity of conflict and a very high degree of complexity based on interests, benefits, cost, and values. While many argue that the new ERTMS' signalling system is safer than the system currently used, the cost of implementing the system has until now increased by so much [26][27][28], that some stakeholders may question the significance of the improved safety which in turn may result in a debate of values and worldviews.

The railway system is a mixture of human actions within technological parameters and therefore a sociotechnical system. In this case, it is appropriate to divide the sociotechnical system into the three groups for analysis. When assessing risk in railway projects, Atkins A/S contemplates about how the Human actors, Organizational actors, and Technical systems (abbreviated as HOT) as shown in the example below (seen in Figure 1.14) interact. The human and organizational aspect can be arranged in the HOT model by means of the stakeholder identification model, and the level of risk communication for deciding on the relevant risks using Renn's model of risk debates.

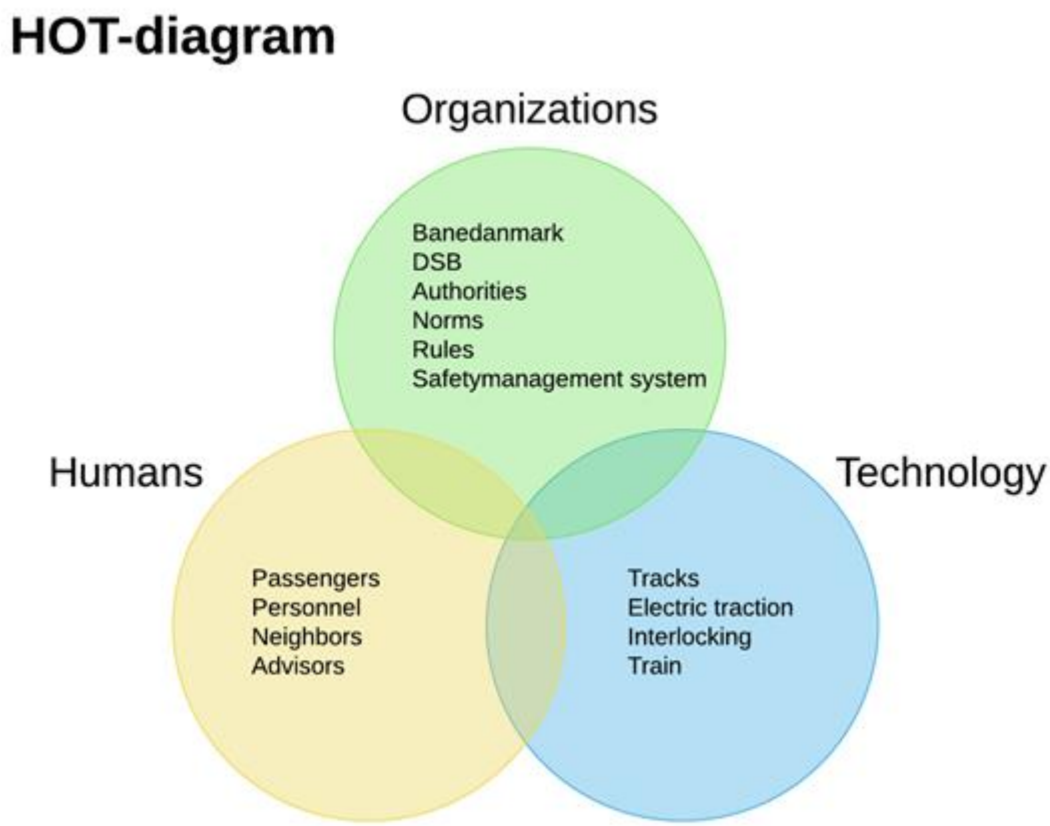


Figure 1.14 HOT Diagram (Picture from Atkins)

When identifying the hazards and assessing the risks of the railway, it is recommended to consider the HOT categories, in order to identify the human factors, the procedural factors and technical factors that may contribute to the risks and how hazards may arise when the three categories interact with each other. This project therefore aspires to use all three categories to identify how each influences the hazards.

2. Problem Formulation

As has been mentioned in the previous chapter, Denmark is aiming to be the first country to fully implement ERTMS, meaning that instead of implementing it one route at a time, during a long time period, the whole country will get this system in a shorter time period (approximately 15 years, depending on delays).

This could therefore result in dramatic changes for the personnel and people working closely with the railway industry. As of this it is important to analyse both the system that is being replaced, along with the newer and potentially improved ERTMS, and see if they are comparable. This is will show descriptively the differences and further help the actors involved to be better prepared for the changes ahead.

2.1 Research Question

The main research for this project is following:

Is is possible to compare the Traditional Signalling system and European Rail Traffic Management System?

The Traditional Signalling is still being used in some forms in some stations and the new European Rail Traffic Management System is supposed to replace the different train management system across the European Union.

The sub-questions of this project are:

- *What are the functions of these two systems?*
- *What are the hazards and safety barriers for these two systems?*

3. Delimitations

In the beginning of this project the decision was taken to only focus on Denmark and the signalling system and train management used there. This was due to the fact that Denmark is the first country to fully integrate ERTMS and replace their existing signalling system.[1]

To focus this project some limitations had to be put into place, in order to solve the problem. Therefore, only one station plan was used for the main analysis of the systems. For this project an older plan of Taulov station was chosen, as this plan is used as an example for educational purposes.

For the definition of the traditional management system, the system referred to as DSB 1953 is used, since several stations across Denmark still operate with it, usually with various upgrades. However, since the upgrades are not consistent with the stations and vary in extent and modernization, the basic system was used for the purpose of this project as it is the basic version upon which the upgrades are based. This system is referred to in this project as Traditional signalling.

As the station plan that was used is from 1965,(Appendix A) it was not possible to take the Automatic Train Control (ATC) system into account, as that system was first developed in the late 1980's. [29] In addition to this, the type of trains considered for this project were limited, as when the Taulov station was in use, only trains similar to Inter City and Lyntog were driven through the station. Therefore, metropolitan trains, such as S-Tog, and freight trains were not taken into account.

4. Project Outline

In order to solve the problem at hand, the two railway management systems were identified and compared, the Traditional Signalling system that has been in use in Denmark and the ERTMS, a European standardized train management system, based on the plan of Taulov station.

To begin with, a system definition was conducted for both of the systems, which is done in accordance with the CSM. The system definition will include system objective, functions and elements, boundaries, physical and functional interface, system environment and safety measures and assumptions that determine the risk assessment.

After having identified both systems a Hazard log Analysis was done for each system, in order to identify hazards, the causes of those and the treatment applied in order to reduce them. This analysis is also a part of the CSM, and therefore has been used as the hazard identification model.

To further analyse how the systems, deal with a hazardous scenario, a Fault Tree Analysis was used. This analysis offered another perspective into how these systems operate and displays a graphical figure of the system behaviour.

Data gathered by the system definitions and the analyses were used for a comparison which was conducted on the systems, based on their functions, hazards and barriers (Functional Diagram, Hazard Log and Fault Tree).

Conclusion was then drawn based on the information from the comparison.

5. Methodology

The information in this project was gathered from various sources including books, internet, standards and consultations. Several research analyses were used such as Stakeholder analysis, Fault Tree Analysis and Hazard Log. The structure of the project was modelled based on the Common Safety Method (CSM), which is used as standard in the railway industry within the European Union, and the project structured required by Aalborg University, as this thesis is a part of an master's program at the institute.

The project begins with introducing the current situation within the Danish railway industry, its transition to European Rail Traffic Management System, from the Traditional Signalling. Then further analysing the problem and identifying the key players.

After the introduction a definition of the two system is conducted, and then the hazards were identified. With the data gathered a comparison of the two systems was done, followed by discussion and conclusion.

5.1 Limitations

Due to the fact that ERTMS was first put into use on one route on 21st of October 2018, data regarding the efficiency of the route was limited and not available during the work of this thesis. [30] Another limitation towards the scope of this thesis was the fact that the Taulov station is not in use in the same format as the station plan that is used in this thesis. This is due to the fact, that the station layout has been changed since the drawing was made in 1965. Therefore, making it harder to get real data to further analyse the problem and to gain more insight into how the traditional system was working in the station.

As of this the focus was put into qualitative data, with functionality and hazard identification as the main focal point.

5.2 Methods Used

5.2.1.1 Common Safety Method

According to DIRECTIVE 2004/49/EC from the European Union, it is stated that the CSM should be integrated to ensure a high level of safety in the railway industry within the member states. This will help ensure a high level of safety within all the member states of the EU.[31] Within this directive further definitions and terms are established in order to have one standardised way for the whole of EU, according to the Safety Directive. In Railway Safety Directive it is further mentioned how a risk analysis should be handled within the railway industry. There it is pointed out step by step how this process should be handled and in what order it should be done in. Therefore, a system definition should be carried out in a specific way, in order to follow European Union rules and regulations, as of that other standards such as ISO 31000 cannot be used for purpose of this project.

5.2.1.2 Hazard Log

In the International electrotechnical vocabulary - part 821: Signalling and security apparatus for railways (IEC 60050-821:FDIS2016, 821-12-27), the definition of a hazard log is:

"..document in which hazards identified, decisions made, solutions adopted and their implementation status are recorded or referenced.."

In this project, the purpose of the hazard log is documentation of the hazard identification. Therefore, the decisions, solutions and implementation segments will be omitted from the log. A hazard log is commonly formed as the foundation for continuous risk management for safety. It exemplifies a model to track hazards and their conclusion. The hazard log must be revised throughout the system life cycle, whenever a change to identified hazards occurs or, a new hazard is detected. The hazard log shall contain or refer to details of:

- the aim of the hazard log
- each hazard, responsible bodies for managing the hazard, and the contributing functions or components
- probable consequences and frequencies of the order of events related to each hazard, when applicable
- the risk as a result from each hazard in quantitative or qualitative terms, where appropriate

- the chosen risk acceptance principles and in case of explicit risk estimation also the risk acceptance criteria to demonstrate the acceptability of the risk control related to the hazards
- for each hazard, the measures taken to reduce the related risks to an acceptable level or to remove the risks
- exported safety constraints

There are two types of hazard log, internal hazard logs for managing the company's internal processes and external ones. The external hazard log is an extract of the hazard log that is appropriate for transferring information between actors. Its purpose is to notify the project actors about the relevant safety aspects at the interfaces to their systems or subsystems and about hazards which cannot be contained by a single actor. In Regulation (EU) No 402/2013 Article 3 (16) the hazard record is defined as the following:

"hazard record means the document in which identified hazards, their related measures, their origin and the reference to the organisation which has to manage them are recorded and referenced"

This definition is somewhat wider and more ambiguous, but still closely related to the previous definition with the inclusion of the identified hazard, their cause, and the parties responsible for managing them.

5.2.1.3 Fault Tree Analysis

The Fault Tree Analysis is the most used reliability and risk analysis method, according to Terje Aven. In basic terms, a Fault tree is a logic diagram, that show the connections between failures of components in a system failure, which cause or contribute to an unwanted event. [32]

The Fault Tree can both be a quantitative and qualitative analysis, all depending on the analysis itself. A quantitative analysis is used when the probabilities of the failures that lead to the unwanted event are known. Then based on these probabilities, calculations can be done to know what the chances are for the main event to happen. However, a qualitative analysis can be used when the probabilities of the events and failure rates cannot be estimated, and the analysis is then used to analyse the causes of unwanted events. The benefits of this type of analysis is then to look into how the primary events are connected and how they can impact the unwanted event.[33] This type of analysis is used for the purpose of this project.

The Fault Tree is built up in a deductive way; with an unwanted event at the top with basic events, which consists of the different elements that create the basic events (e.g. component failure, human error or other failures), coming down from it. Making it a good tool to use when working with complex systems and subsystems.[32] When working on a Fault Tree Analysis a step-by step approach is used, along with the help of two questions “How can this happen?” or “What are the causes of this event?”, as those will help go through each step of the Fault Tree, by pointing out what needs to go wrong order for the unwanted event to happen.[32] The basic events are connected with gates, an And or an Or gate. An And gate means that the basic events connected to the gate all have to happen in order to move up in the fault tree, and an Or gate means that at least one of the input events need to happen in order to move up in the Fault Tree. The different gates can be seen in Figure 5.1.

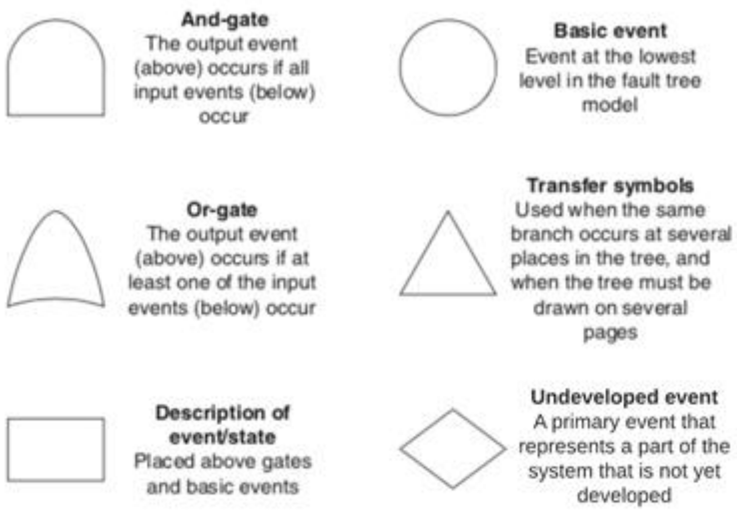


Figure 5.1 Adabted Verison of the Fault Tree And and Or Gates [32]

5.3 Validation

This project was written in collaboration with Per Stoltze, chief specialist at Atkins, who has years of experience within Danish Railway. Information gathered from his knowledge and experience was then used and cross referenced with online sources and literature.

The models used to conduct the analysis were collected through literature, lessons and standards and were conducted in accordance with their principles of use, to ensure their validity.

When using online sources, only pages assumed to be reasonably reliable were used, such as official pages of companies, official European Union pages and pages related to them, official Danish railway sites and similar. The information gathered from the online sources were cross referenced with other sources to ensure their legitimacy.

If news outlets were used, the contents of them were also searched on other pages to verify them to make sure that they were accurate.

After researching other projects with the same focus no precise matches were found. It has also been confirmed by the consultant from Atkins engineering and design company that to their knowledge no such comparison has been done to this day.

6. Systems Definition

In this chapter the two systems, Traditional Signalling and ERTMS, will be identified and defined. There will be separate chapter for each system, each including a list of system functions, elements, interfaces and safety measures.

As for the purpose of this project the same station layout is used, the same boundaries and environment are for both systems. As of that they will be described jointly in the section bellow.

The main purpose of both systems are the same, manage the trains movements, arrivals and departures and doing so in manner that is as safe as reasonably possible. Another shared goal for the systems would be efficiency, however that factor is not part of the analysis for this project.

6.1 Boundaries

To set a clear set of boundaries and extent of the system, the system will be limited by the following:
From the left, the system is limited by the set of light signals at the 7,6 km mark on the rails towards Fredericia. The light signals are included in the system.
From the right, the system is limited by the set of lights at the 9,6 km mark on the rails towards Kolding. The light signals are included in the system.
From the top, the system is limited by the fence next to the track number 3.
From the bottom, the system is limited by the fence next to the track number 1 and the station building. The building is not included on the system.

Also included in this system is a level crossing at the 8.1 km mark on the rail in the direction towards Fredericia. The level crossing included in the system is limited by the set of light signals on each side of the crossing. Both sets of light signals are included in the system.

The boundaries are shown in Figure 6.1.

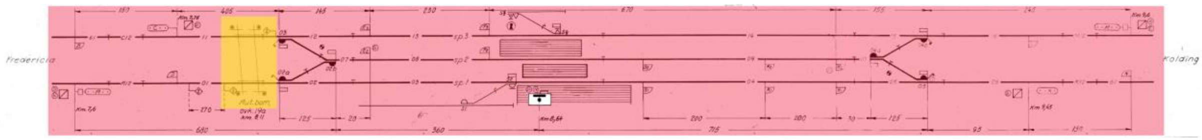


Figure 6.1 System Boundaries

6.2 System Environment

In this chapter there will be listed the environmental elements that the system operates with, influences or is influenced by. These are included to help with understanding of the systems limits, complexity and functions. Those elements are divided into two sections, physical and functional environments.

6.3 Physical Environment

The physical environment represents the elements with which the system operates on a physical level. It consists of the following elements:

<u>Trains and wagons</u>

- All trains and wagons that are on the tracks. This element includes both train engines, wagons for passengers, maintenance vehicles that operate on track for maintenance purposes and vehicles that operate on track for the purpose of shunting.

<u>Passengers</u>

- All the people that are within the borders of a system for purpose of travelling with a train or accompanying a passenger, on the train or platform.

<u>Personnel</u>

- Includes all the people employed by the railway company or its associates that are within the borders of the system for the purpose of working, such as drivers, conductors, traffic manager, maintenance and repair personnel etc.

<u>Level crossing users</u>

- All the people that are using the level crossing to cross the rails on foot, bikes, cars or other means of transportation.

<u>Unauthorised persons</u>

- All the people who are within the borders of the system, but should not be there, especially in areas that are off limits.

<u>Electrical wires</u>

- High voltage wiring that are used to supply the trains with electricity, mostly above the train tracks. They can cause damage to unauthorised persons under certain circumstances.

<u>Weather</u>

- Can influence the functioning of the system either by its influence on the system hardware or by the conditions affecting the operational conditions, especially with rain, snow, ice, strong wind etc.

6.4 Operational environment

The operational environment contains the tasks that are being conducted within the system boarders as a part of the daily routines, which are not part of the train managing system.

- Trains passing at speed
- Trains arriving, passengers alighting or boarding, trains departing.
- People and vehicles crossing the level crossing.
- Trains crossing the level crossing.
- Cargo being loaded and unloaded onto and from trains.
- People crossing from platform to platform.
- Trains shunting.
- Wagons being hooked and unhooked to and from trains and to and from other wagons.
- Maintenance works on trains and wagons.
- Maintenance on rails, points and sensors.
- Maintenance on signals (only Traditional Signalling)
- Landscaping.

6.5 Traditional Signalling

There is a large plan of the station equipped with Traditional signalling at the end of this chapter 6.5.3, named Figure 6.2.

6.5.1 System Objective

The objective of this system is to provide interlocking at Taulov station, and letting the train safely enter and leave the station without the danger of having another train or object in the way. This is further done by external light signals, that are given by a train controller, in order to communicate how the train driver can safely approach or leave the station without any obstacle in the way (or informing the driver that there might be an obstacle, but he can stop and proceed with caution).

6.5.2 Functions and Elements

There are several functions that this system has to have to be able to fulfil its objective. In this chapter these functions will be listed and described. Furthermore, there will be the listing of elements of which the system consists and the functions they participate in. Only the main elements participating in the functions will be listed, because of the complexity of the system.

6.5.2.1 Functions

Updating movement authority

Movement authority in this project means the permission to get the train in motion. It involves both shunting and driving. Updating this status is crucial for the information/permission to be as up to date as possible. In this system it is done by the train driver reading the signals and/or communicating with the traffic control operator.

Locking a route

By locking a route, it is meant that a certain part of a track is reserved for a certain train. Another train cannot be directed to the same track so there is no overlapping.

Components used:

- Control panel
- Track changing points
- Tracks and track sections
- Wires
- Relays

Setting a signal

By setting a signal, a certain combination of lights with a predefined meaning will appear on the signalling device on the trackside. This signal is used to inform the train driver of a certain situation, giving him instruction/permission on how to proceed.

Components used:

- Signals
- Wires
- Control panel

Track vacancy proving / train detection system

Several hardware is used to check and control whether a track is occupied or vacant. In other words, the hardware is checking if there is a train or wagon present on a certain part of a track.

Components used:

- Wiring
- Train sensors
- Control panel

Setting and locking points

If a track is vacant, the system allows it to be "locked" for a train, if certain conditions are fulfilled. These conditions include among others the track not being locked for another train and the train being able to fit the desired track. If these conditions are met, the system allows the points to be set in such a way that the train may access the track.

Components used:

- Changing points
- Wiring
- Control panel
- Signals

Releasing a route

By releasing a route is meant that the track is being made available for another train. There again are several conditions that must be fulfilled for a track to be "released".

Components used:

- Train sensors
- Tracks sections
- Signals
- Wiring
- Control panel

Level crossing barriers and signals control

By controlling the level crossing barriers and signals, the signal is shown for the drivers and pedestrians whether it is clear or not to cross the rails.

Components used:

- Barriers
- Signals
    - Both light and acoustic signals
- Wiring

- Control panel

Train Monitoring

Managing trains arrivals and departures. This is done by fixed schedule, irregular changes are arranged via radio.

Components used:

- Track isolations

[34][35]

6.5.2.2 Elements

Signals

All the light signalling systems are included, in the Figure 6.1 and are named in the following manner:

G_1 located at km 8,85,

R_1 located at km 9,05,

H_1 located at km 9,25,

E_2 located at km 8,31,

F_2 located at km 8,54,

G_2 located at km 8,85,

R_2 located at km 9,05,

H_2 located at km 9,25,

E_3 located at km 8,31,

F_3 located at km 8,54.

There are further 4 entrance and exit signs, marked with A, located at 7,6 km, M, located at 9.6 km (entrance signs), C, located at 7,76 km, and K, located at 9.45 km (exit signs).

They participate in the function “setting a signal”.

In the whole station there are 10 light signals.

Acoustic Signal

Used to transcend information to passengers, e.g. that a train is approaching and that the tracks should be vacant and etc. Located at the station itself and at the level crossing.

Barriers

A simple gate, that can open and closed to prevent ongoing traffic onto the tracks.

Tracks

Railways tracks, used by trains to move around (shunting and driving). They are formed by the "Track sections". In the station there are 3 tracks.

Track section

It is a part of the railway track divided into sections used by the train detection system to recognize the train section status, whether it is clear or occupied by train. In this case, there are 27 sections. Sections outside this project limits, located between train stations, can be several kilometres long.

Train sensors

Used to detect if the track section is being occupied or is available. This is done by using electrical currents.

Those sensors are:

> Sensors A12, 01, 02, 03, 04, 05, 06, and K12 are located on track 1.
>
> Sensors 07, 08, 09 and 10 are located at track 2.
>
> Sensors C12, 11, 12, 13, 14, 15, 16, and M12 are located on track 3.

Level crossing

By level crossing it is meant an intersection of a road and a railway track, which is at the same elevation as the railway track, and in this case, there is only one. Located around 8,11 km.

Track relay

An electro-mechanical switching device. Used as a part of most subsystems in the Traditional Signalling, as this system is designed heavily on relays.

Platform

An elevated area used for passengers to board the train or for the cargo to be loaded onto or out of a train.

Here there are 3 platforms. Located around 8.64 km, although spreading a few meters in each direction.

Points

Devices that can be aligned to different positions thus allowing the train to change tracks. In this station there are 8 changing points.

03 and 02a are located at 8,16 km, 02b is located at 8,28 km, 05 and 04b are located at 9,35 km, 04a is located at 9,23 km. Furthermore, there are points s1, s2, s3, and s4 used for shunting.

Wiring

Are used to connect the electrical components and signals.

Interlocking processor

Device designed to lock tracks, preventing conflicting movements.

Control Panel

Is located with the train controller in the train station, this is used to control the electrical components, e.g. signals, changing points etc. and is located at 8,64 km.

6.5.3 Physical and Functional Interfaces

6.5.3.1 6.1.4.1 Physical Interface

Signals – Track

Trains - Track

Trains - Passengers

Signals - Controls

Controls - Points

Controls - Operator

Tracks - Level crossing

Level crossing - Cars

Level crossing - People

Trains - Engine driver

Signals - Train driver

Signals - Passengers

Signals - Car drivers

Signals - People (on crossings)

Maintenance - Rails

Maintenance - Signals

Maintenance - Points

Maintenance - Controls

People (trespassing) - Rails

People (vandalism / sabotage) - Signals

People - Platform

Platform - Cargo

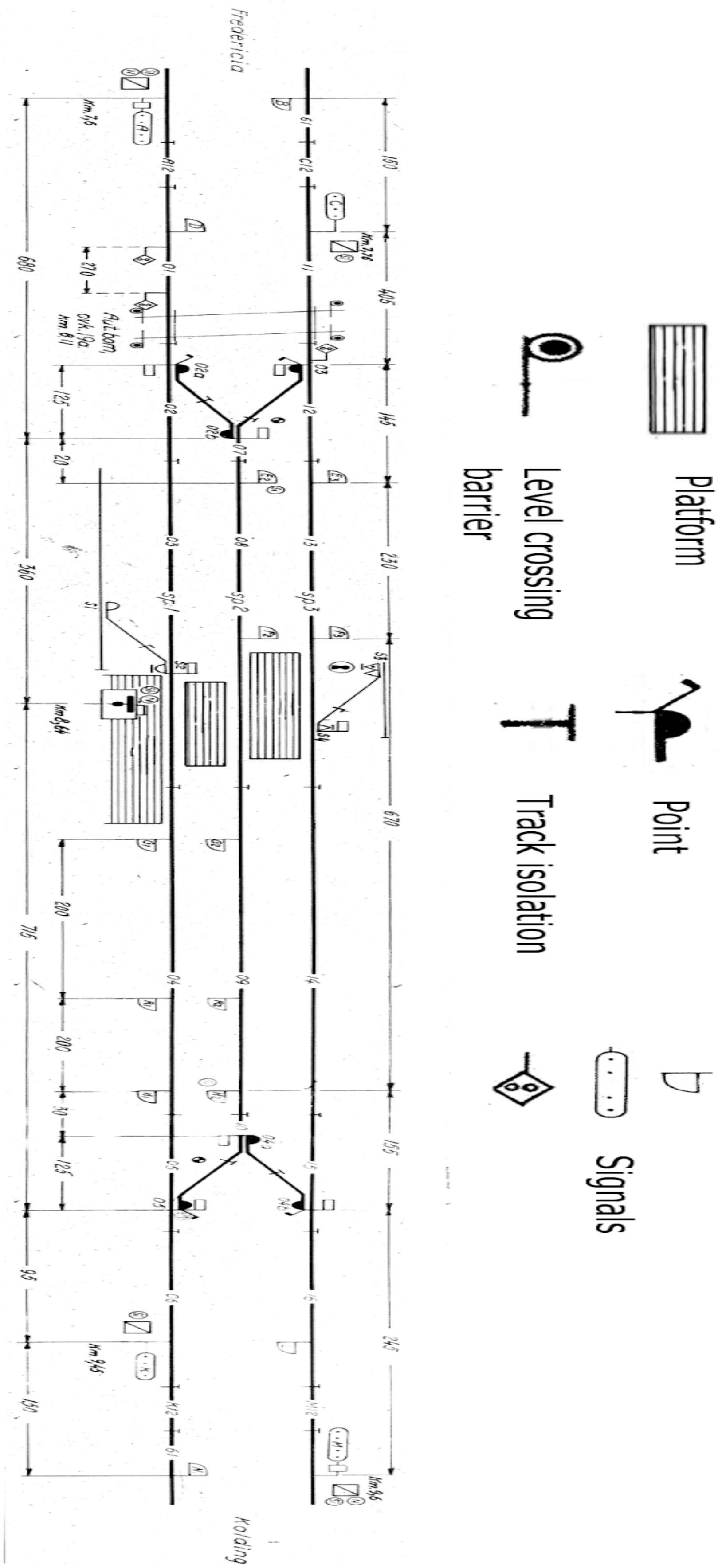


Figure 6.2 Taulov Station Plan for Traditional Signalling (Picture form Atkins)

6.5.3.2 Functional Interface

In the Figure 6.3 below, the train managing system is shown. In the boxes there are the system elements and the arrows symbolize the connections.

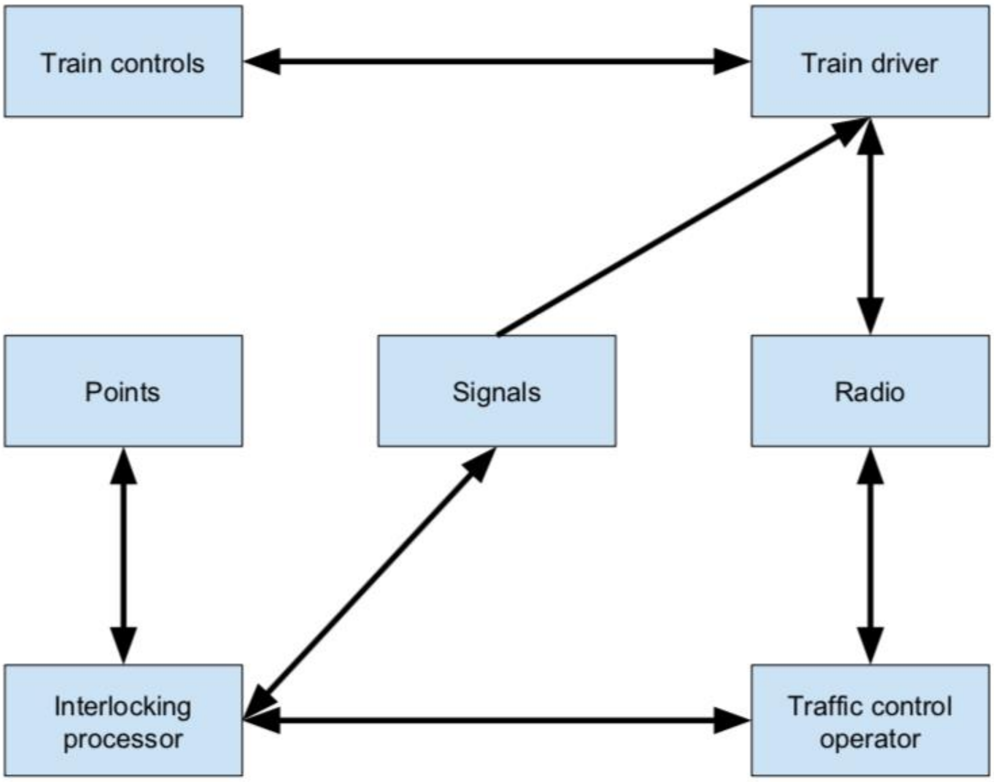


Figure 6.3 Diagram of Functional Interface for Traditional Signalling

From the diagram it is clear that there are two main elements managing the trains. One is the traffic control operator, deciding on the positions and movements of the trains, and the other is the train driver, physically operating the train in accordance with traffic control operators' instructions.

As it is shown, the main element in controlling the train is the train driver, who is in control of the train by using the train controls. The information on where the train should be, what speed it should be moving etc. are relied to him visually by the signals and verbally by the traffic control operator.

Traffic control operator is in charge of managing the trains based on previously designed schedule and of making temporary changes, if necessary.

The key controlling element is the interlocking processor, which changes the points and sets the signals accordingly, based on the traffic control operators' setting.
It is clear, that the Traditional Signalling system relies heavily on the human factor to operate.

6.5.4 Safety Measures and Requirements

The most important safety procedure, when it comes to a train journey, is the determination of a route. This means that before a train journey begins, the route needs to be specifically determined and mapped out. Making it easier for the train controller to know at what point the tracks need to be free, and at what platform the train should stop on. Then, when the train approaches the station the route can be safely locked in, meaning that the train can safely approach the right platform. In order to do so, the train controller will need to lock in the route on his control panel, which will then signal if the route is vacant and no obstacles are in the way. By having this done, it can reduce the risks of other trains being on the route (although delays can of course happen, but then they work accordingly in order to limit the risks that it can cause).

In Denmark there is a manual for railway safety procedures called Sikerhedsreglement (SR), (Danish for the Safety Regulation), which is published by Banedanmark. This manual includes explanations of different definitions, signals, the competences and responsibility of the employees and etc. This helps ensure that everyone working within the industry have the same understanding of all of the different terms and signals and they all work within the same boundary – thereby enhancing the safety and security of the train trips.[9]

It can however happen that a route is locked in, and all points are in position and locked, but for some reason it is not certain that the track route is free. Therefore, in order to keep the risk of a hazard low, but still try to keep the train on schedule it is possible for the train to go ahead in this specific route, but making sure that the tracks ahead a free, this is formally called driving on sight. Meaning that the train cannot drive fast and the train driver needs to be able to see the track in front of him, so if there are any obstacles he has the potential to stop in time. In this type of driving the max speed is 40 km/h. [9]However, in case that the train management has received information that something might not be as it should on the track, they may allow the locomotive driver to proceed with the journey but with extreme caution. They will have to inform the locomotive driver exactly what he should be expecting and approximately where he should be expecting it. In this type of scenario, the max speed may not exceed 60 km/h, although the train management might decide on a lower maximum speed. At the stations there is an additional light signal for these scenarios, this signal is called 'stop, and move forward'(sometimes referred as s.o.r.f in Danish). This signal simply means that the train needs to stop at the signal, and then slowly move forward, but at a limited speed that that makes it possible for the train to stop with short notice. [9]

In the station layout for Taulov station, there is a table that shows all the different conditions and procedures that are connected to a specific route. Among the elements it shows are the safety intervals, points, signals and their connection to the safety in running the station. This table can be seen in the Figure 6.4, and a full sized version is also available in Appendix A along with Danish explanations regarding the context of the table Appendix B. The purpose of this table is to show the conditions that need to be in place for the train to safely approach and leave the station.

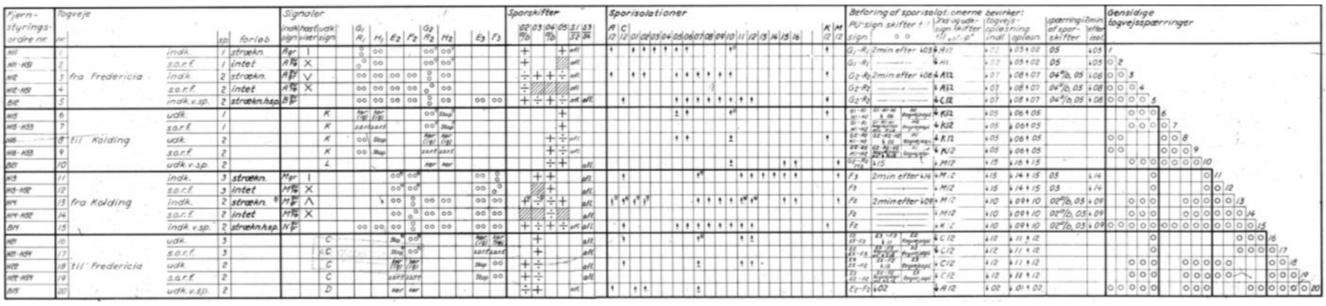


Figure 6.4 Table for Safety Conditions, Taulov Station, Traditional Signalling (Picture from Atkins)

The safety measures will further be elaborated on in the hazard log for Traditional Signalling system. As there it will be explained what barriers have been put in place to reduce the risks of a hazard.

6.6 European Railway Management System

There is a large plan of the station equipped with the ERTMS at the end of chapter 6.6.2, named Figure 6.6.

6.6.1 System objective

The objective of this system is to unify the train operations of the nations within the EU, and to lay foundation for automatic train operation. This system will further provide easier communication between train driver and train controller via signals inside the train cabin, and not with the old-fashioned track side light signals. This is further done via the GSM-R radio network, which transfers both audio - and data communication between the train driver, the train controller and the ERTMS system. Making it easier for the train driver to know e.g. his speed limits throughout the route. This will all ensure that the train can safely enter and leave the station without the danger of having another train or other object in the way.[36]

This new system will mean that potential failures in the system will be easier to locate and further decrease maintenance cost, as track side equipment such as light signals will be removed completely.[37] [14]

As a part of the ERTMS the ETCS, further ensures the safety by continuously calculating the allowed speed limit, and further ensure that the limit is not exceeded, by having the allowance of braking the train for those instances.[12] This will further increase the efficiency of train travels through the EU.

6.6.2 Functions and Elements

There are several functions that this system has to have to be able to fulfil its objective. In this chapter these functions will be listed and described. Furthermore, there will be the listing of elements of which the system consists and the functions they participate in. Only the main elements participating in the functions will be listed, because of the complexity of the system.

6.6.2.1 Functions

Updating movement authority

Movement authority in this project means the permission to get the train in motion. It involves both shunting and driving. Updating this status is crucial for the information/permission to be as up to date as possible. In the ERTMS the movement authority is updated automatically by checking the train position.

Components used

- Balise
- GSM-R equipment

Locking a route

By locking a route, it is meant that a certain part of a track is reserved for a certain train. Another train cannot be directed to the same track so there is no overlapping.

Components used:

- Interlocking processor
- Points
- RBC

Track vacancy proving

Several hardware is used to check and control whether a track is occupied or vacant. In another words the hardware is checking if there is a train/wagon present on a certain part of a track.

Components used:

- Axle counters
- Balises
- Train Monitoring System (TMS)

Setting and locking points

If a track is vacant, the system allows it to be “locked” for a train, if certain conditions are fulfilled. These conditions include among others the track not being locked for another train and the train being able to fit the desired track. If these conditions are met, the system allows the points to be set in such a way that the train may access the track.

Components used:

- Points
- Interlocking processor

Releasing a route

By releasing a route is meant that the track is being made available for another train. There again are several conditions that must be fulfilled for a track to be "released"

Components used:

- Interlocking processor
- Points
- TMS

Train Monitoring

Managing train movements, arrivals and departures. This is done by the the balises and other track side equipment which sends the information via GSM-R data.

Components used:

- Balises
- GSM-R
- Tack side equipment
- RBC
- TMS

[34][35][38]

6.6.2.2 Elements

Axle counters

Hardware equipment that is used to count the number axels passing over it, thus acquiring information whether or not the train or its part are present on certain track section. This information is then used to determine whether the track section is clear or occupied.

Tracks

Railways tracks used by trains to move around (shunting and driving). They are formed by the "Track sections". In the station there are 3 tracks.

Track section

Is a part of the railway track divided by the sections, used by the train detection system to recognize the train section status, whether it is clear or occupied by train. In this case there are 27 sections. Sections outside this project limits located between train stations can be several kilometres long.

Level crossing

By level crossing it is meant an intersection of a road and a railway track, which is at the same elevation as the railway track, and in this case there is only one. Located around 8,11 km.

Platform

An elevated area used for passengers to board the train or the cargo being loaded onto or out of a train. Here there are 3 platforms. Located around 8.64 km, although spreading a few meters in each direction.

Points

Devices that can be aligned to different positions thus allowing the train to change tracks. On this station there are 8 changing points. 03 and 02a are located at 8,16 km, 02b is located at 8,28 km, 05 and 04b are located at 9,35 km, 04a is located at 9,23 km. and moreover there are points s1, s2, s3, and s4 used for shunting.

Interlocking processor

Device designed to lock tracks, preventing conflicting movements.

Onboard train (3.4.1 in GE/GN8605 ETCS System Description), shown in Figure 6.5.

ERTMS/ETCS equipment

- European Vital Computer (EVC)
- Train Interface Unit (TIU)
- Balise Reader
- Driver Machine Interface (DMI)
- Odometry
- Balise Transmission Module (BTM)
- Juridical Recorder Unit
- Specific Transmission Module
- GSM-R + antenna

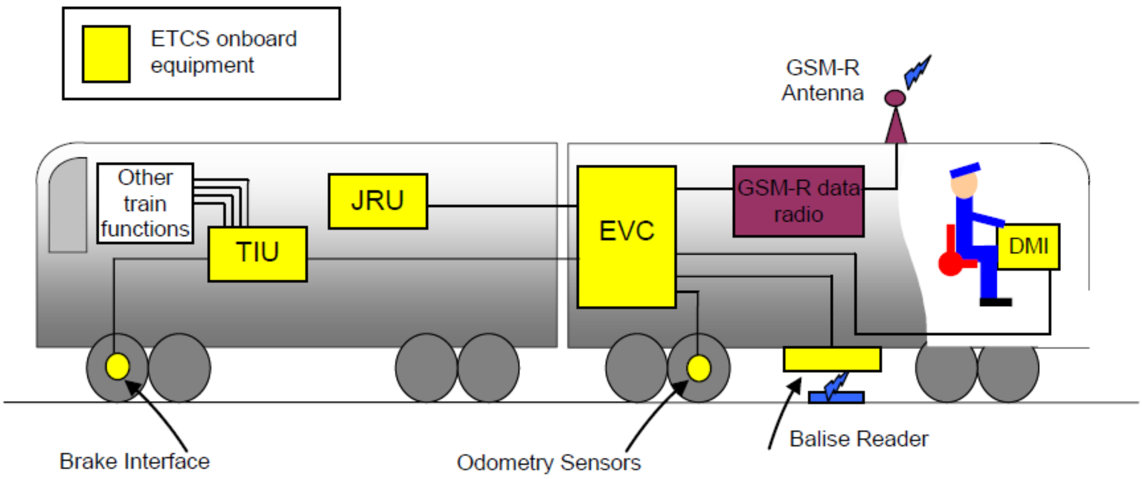


Figure 6.5 ERTMS Onboard Equipment[16]

Trackside (3.4.1 in GE/GN8605 ETCS System Description)

- Marker boards
- ERTMS parts
  - Radio block centre (RBC)
  - Base transceiver station (BTS)
  - Lineside Equipment Unit (LEU) (only with level 1) Source:
  - Train monitoring system (TMS)
  - Euroloop
  - Radio In-fill Unit
  - Balises
  - [39][40]

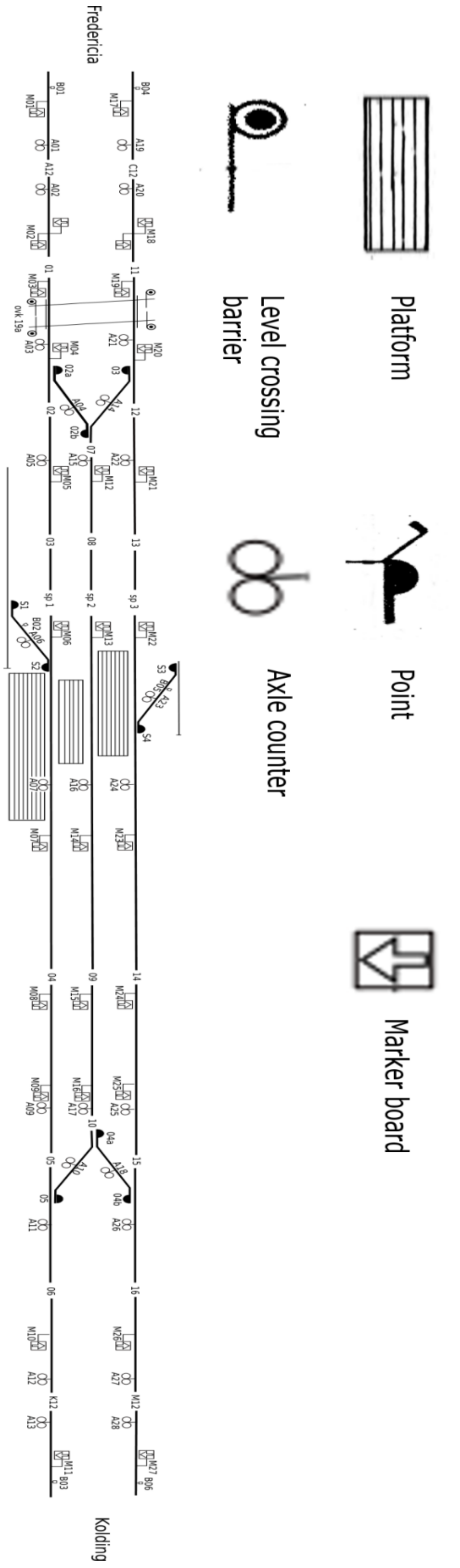


Figure 6.6 Taulov Station Plan for ERTMS (Picture form Atkins)

6.6.3 Physical and Functional Interfaces

6.6.3.1 Physical Interface

Trains - Track

Trains - Passengers

Signals - Controls

Controls - Points

Controls - Operator

Tracks - Level crossing

Level crossing - Cars

Level crossing - People

Trains - Engine driver

Signals - Passengers

Signals - Car drivers

Signals - People (on crossings)

Maintenance - Rails

Maintenance - Signals

Maintenance - Points

Maintenance - Controls

People (trespassing) - Rails

People (vandalism / sabotage) - Signals

People - Platform

Platform - Cargo

Balise – Track

Marker board – Track

Axle counter – Track

Sensors - Train

Receivers - Train

Transmitters - Train

Display - Train

Computer - Train

ETCS onboard - Train (For details see previous Chapter 6.6.2)

ETCS trackside - Track (For details see previous Chapter 6.6.2)

6.6.3.2 Functional Interface

In the Figure 6.7, the train managing system is shown. In the boxes there are the system elements and the arrows symbolize the connections. For better understanding, the complete ERTMS was simplified to show only the main elements and functions.

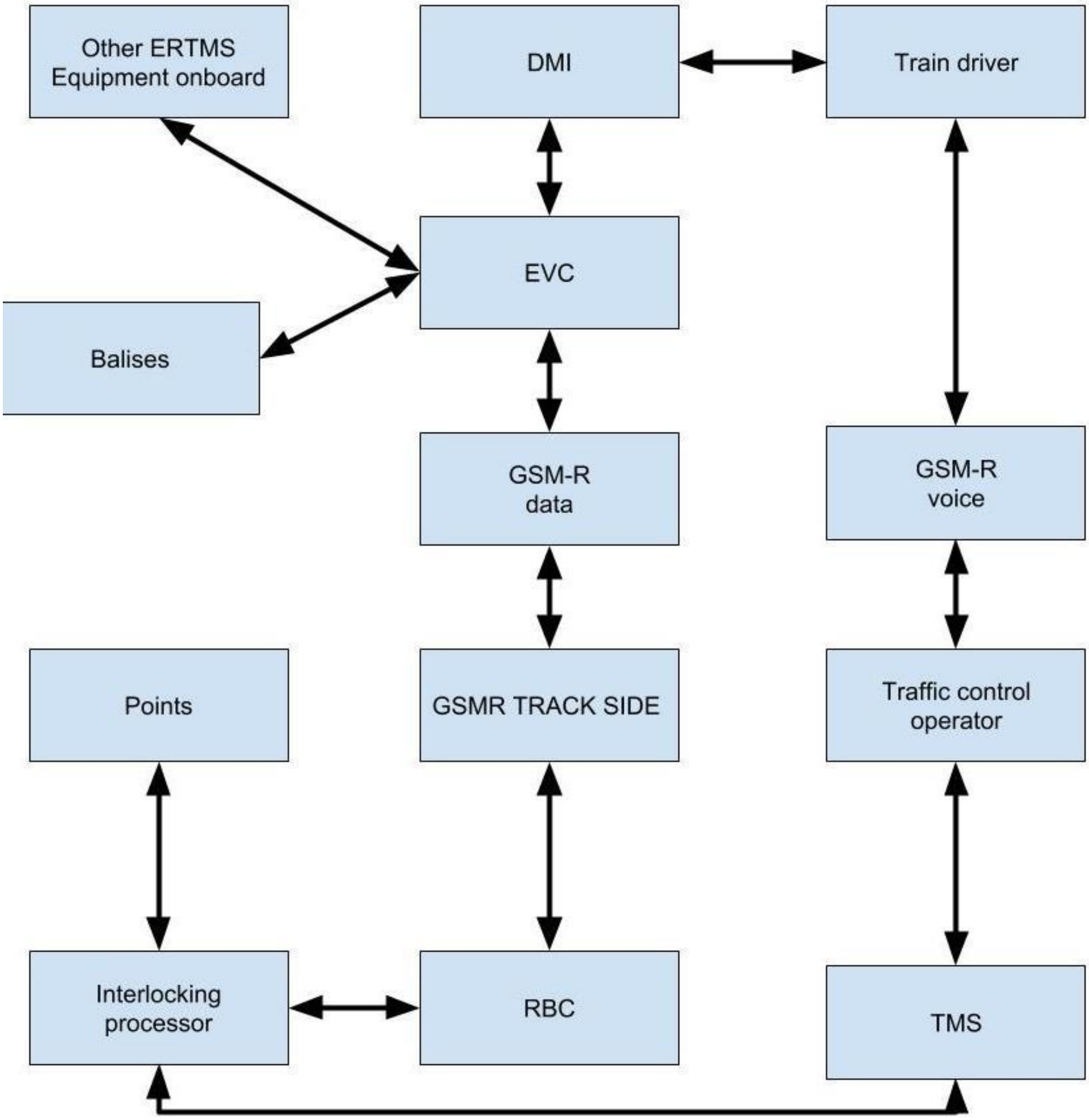


Figure 6.7 Diagram for Functional Interfaces for ERTMS

The diagram shows, that the main elements for managing the trains are train driver, traffic control operator, EVC and TMS.

The driver is controlling the train movements via the train controls (DMI), but the EVC is checking his actions, assessing the situation and updating him on the information needed for efficient running based on numerous information from the ERTMS.

To manage the trains the traffic control operator only adjusts the information in the TMS when special circumstances arise and the system will adjust.

The TMS is keeping track of the train movements and routes and planes it so there are no overlaps.

The ERTMS is constantly updating and informing the driver of the maximum speed, which results in efficiently running the train while controlling the driver for unsafe behaviour. In that sense the ERTMS is limiting the human factor from the train management.

6.6.4 Safety Measure and Requirements

As in the Traditional Signalling, it is important for the route of the train to be predetermined to ensure the safety of the train trip. According to Preben S. Pedersen who is the vice chairman of the Danish Railway Association, with the existing system (albeit it has the ATC also in hand), a train driver can be sure that when he passed a green light at a station, he will not meet another train at that track. But this is however not the case for the new ERTMS system.[41] That is where the movement authority (MA) comes into play. The MA automatically being automatically renewed by the ERTMS, based on the information received form the trackside and onboard equipment and the information received via GSM-R. When the MA is not renewed the train will stop before reaching the danger point. The danger point is a point beyond which it is not possible to guarantee safe passage. The MA is needed for the train to start its journey and to further enter new block sections during its travel, thereby replacing the track side light signals. There are however occasions when a train can drive without or with limitations to the MA, those are for example: driving on sight, with limited supervision and for shunting.[42]

There are a few operating modes of the ETCS that affect the driving of the train. Those that are considered to be relevant for this project are: full supervision, on sight driving and staff responsible, the other modes can be found in RSSB's ETCS System Description.[16]
The main ETCS mode is Full Supervision, this is only applied when the ETCS equipment on board has access to all the information it needs in order to fully supervise the train.[43] On sight driving is when the train can move ahead, even though it is not known if the track ahead is free. This is done in a way that the driver needs to travel at a speed that makes it possible for him to completely stop the train before it crashes into an obstacle. Finally, there is the staff responsible mode, which is used when the ETCS system does not have all of the information it needs to fully supervise the train. This mode is used when the train is starting its journey, as the current position is invalid or unknown, and also if the driver chooses to override the system. In this mode the ETCS system is though still monitoring the maximum speed.[43]

Furthermore, to better ensure the safety of the train a dynamic speed supervision has been implemented, that means that continuously the train is being monitored based on position and speed, then calculated based on that the braking distance. This system can further optimize the trains arriving to a desired destination in time, with the help of the target speed monitoring system, which helps to ensure better efficiency. However, if the driver overspeeds, he will get a audio warning telling him to reduce the speed and get back into the maximum permitted speed. Withal, if the driver fails to follow those warnings, the system will take over and start braking the train until it is at allowed speed. If the train extensively over steps the speed limit an emergency brake will be used.[16]

Other safety barriers include: The barriers used in the ERTMS, are as follows[16]:
Data consistency
The system is cross-referencing the data received. The data is encrypted and marked with a specific timestamp and order number.

Determination of Speed and Location
The system automatically reports system location and speed based combined information from the trackside and onboard equipment.

Determination of Most Restrictive Speed Profile
The system is monitoring the speed of the train and compares it to the location, checking for locally reduced speed etc.

Odometry Monitoring
The system is monitoring the rotation of the wheels and cross-references the data with the location data gathered from the roadside equipment.

System Health Monitoring
System is constantly monitoring the onboard and roadside equipment for failures. This system further analyses the importance of the failure, if it is something that needs immediate attention or can wait until later. (Operational Concept for ERTMS Issue 2)

Supervise Train Movements
The train can be prevented from moving in directions that is not allowed.

Track Condition Monitoring
The system can inform about the conditions on the track that might affect the train.

6.7 Assumptions the Determine the Risk Assessment

As the purpose of this project is to find if the two systems are comparable, the risk assessments are done for both systems as they should be the same in order to make a fair comparison.

For this project it is assumed for the risk assessment that:

- The CSM process is adequate for defining these systems and assessing the risk in the traditional railway system and in the ERTMS, as it is required in the The Railway Interoperability Directive
- The hazards in the railway system can be identified by the hazard log.
- The station plan of Taulov station accurately depicts the system under investigation.
- The system can be sufficiently translated into a functional block diagram.

- The causes of hazards can be visualized in a Fault Tree to determine how the system must fail for an accident to occur.
- The system components only have two states which are functioning or failing.
- The fail safes in the ERTMS are reliable.
- Each hazard has one or more causes.
- That the dynamic behaviour of the system can be explained on the function of its elements.

7. Hazard identification / Risk analysis

According to the Regulation (EU) No 402/2013 from 30th of April 2013, hazard identification is the process of finding, listing and characterizing hazards.

When making a hazard identification, four methods could be used for this case, those are geographical, functional, traffic oriented or object oriented. However, in the light of the problem at hand, functional and object-oriented methods will be used for hazard identification. This is because the functional method can focus on train detection, signalling, communication and train routes. The object-oriented method can be used to identify hazard in I-signals A and B, track change 1 and 2, track 1 and 2 and the platforms. These are all important aspects of the signalling process.

7.1 Hazard identification

As previously mentioned in Chapter 1.2.4, the Safety Directive Annex I, 1.1 identifies at least five different accidents; collision, derailment, level-crossing accidents, accidents to persons caused by rolling stock in motion, fires, with an additional category of others. When it comes to accidents related to failures within the signalling systems or the ERTMS, only four are relevant. As fire in a rolling stock is not considered to be related to signalling systems. There are however many different ways for each category to happen, as there are a few things that can go wrong, that can result in a hazard, and those are listed in the following hazard logs.

7.2 Hazard Log

In accordance with the CSM, the hazard log analysis has been conducted for each of the systems. The hazard log provides an easy understanding, with arranged lists of possible hazards to the system, their causes, consequences, classifications and hazard treatment in place. It is also useful for the purposes of the project, since the graphical interpretation is a good way to quickly compare a complex topic like this one. The possible hazards were listed with their possible causes, consequences and barriers that are in place to minimize these hazards. Possible consequences were also categorised based on the railway definitions and categories.

7.2.1 Traditional Signalling

The hazard log is made based on the system working under normal circumstances and can be seen in Table 7.1.

	Hazard Description			Hazard Classification			Hazard Treatment
Hazard	Cause of the hazard	Underlying causes for the hazard	Comments	Accident Type	Person Categories	Conssequences	Barriers
Track is not free	Route not locked	Interlocking processor	Electrical problem	Collision	Passangers	Damage to Infrastructure	Schedule
		Mechanism fail			Employees		
		Track occupied					Driving procedures
	Signal malfunction	Signal broken	Dirt/ice blocking		Level Crossing User	Damage to vehicle	Personnel
	Human error	Bad connection					Signals
		Power failure	Wiring problem		Other Person at a platform	Injuries	Safety intervals
	Vacancy proving fail	False negative/positive					
		Mechanical problem	Component worn out		Other person not at a platform	Death	Maintenance
	Train monitoring fail	Radio problem					
Level crossing not safe	Signal malfunction	Bad connection	Component worn out	Level crossing accidents (collission train-car/bike, person)	Passangers	Injuries	Level crossing signals
		Signal broken					
		Power failure				Death	Level crossing barriers
	Level crossing signal fail	Bad connection	Wiring problem		Employees		Driver
		Signal broken					Legislation
		Power failure				Damage to vehicle	Maintenance
	Level crossing barriers fail	Mechanical problem					
	Human error	Power failure			Level Crossing User	Damage to Infrastructure	
		Bad connection					
	Train monitoring fail	Radio problem					
Overspeed	Signal malfunction	Signal broken	Component worn out	Derailment, Collision	Passangers, Employees, Level crossing users, Other person at a platform, other person not at a platform	Injuries, Death	Maintenance
		Bad connection				Damage to Infrastructure	
	Human error	Ignore Signal	Wiring problem			Damage to vehicle	
People crossing track	Signal malfunction	Bad connection	Component worn out	accidents to persons caused by rolling stock in motion	Passangers,	Injuries	Maintenance
	Human error	Signal broken	Wiring problem		Other person at a platform	Death	Signs
							Signals
		Power failure			Employees	Damage to vehicle	Driver
Signal passed at danger	Vacancy proving fail	False negative/positive	Dirt/ice blocking	Collision, derailment, level-crossing accidents, accidents to persons caused by rolling stock in motion	Passangers	Injuries	Safety braking distance
		Mechanical problem	Component worn out		Employees	Death	
	Train monitoring fail	Radio problem	Wiring problem		Level Crossing User	Damage to vehicle	Maintenance
	Human error	Ignore Signal	Short circuit		Other Person at a platform		
	Failure to Stop	Lack of warning	Lack of friction		Other person not	Damage to	

Table 7.1 Hazard Log for Traditional Signalling

<u>Track is not free</u>

Situation in which there is an obstacle in a form of a train or wagon in a way of another train.

<u>Level crossing not safe</u>

Situation in which the level crossing is not free for the train to cross. This could mean that there is a car, motorcycle, bike or a pedestrian in the level crossing area while there is a train passing it.

Overspeed

Situation in which a train is moving at a speed higher than the allowed speed limit.

People crossing track

Situation in which there are people crossing the rails when there is a train driving on the rails.

Signal passed at danger

Any situation in which the train goes past a point where there is a signal that signalises "STOP".

There are several hazards present in the Traditional Signalling, but the system of barriers designed to mitigate them is in place and ensures reasonably safe operational conditions. Significant part of the safe running conditions relies on the abilities and experience of the personnel operating the system, as there are not that many "safety nets" present in the Traditional signalling. The system is also facing some reliability issues as a result of the use of analogue technology and the component fatigue.[3]

7.2.2 European Railway Traffic Management System

The hazard log is made based on the system working under normal circumstances on the ERTMS level 2 and is shown in Figure 7.2.

	Hazard Description			Hazard Classification			Hazard Treatment
Hazard	Cause of the Hazard	Underlying Causes for the Hazard	Comments	Accident Type	Person Categories	Conssequences	Barriers
Level crossing not safe	Human error	People ignoring warning signs		Level crossing accident	Level crossing user	Injuries	Level crossing signals
	Level crossing signal fail					Death	
	Level crossing barriers fail					Damage to vehicle	Level crossing barriers
						Damage to infrastructure	Legislation
						Delays	Maintenance
ERTMS failure	Component failure	Fatigue		Collision	Level crossing user	Injuries	Automatic brakes
		Bug in the system					Frequent movment authority updating
	Power failure	Weather		Derailment	Employees	Death	Constatnt system healt monitoring
		Fatigue			Passangers	Damage to vehicle	
		Power cut		Level crossing accident			Data Consitancy Checking
	Cyber attack	Train recieving incorrect information	System breach		Other person at a platform	Damage to infrastructure	Supervised Train Movements
		Train ignoring information	Firewall breakdown	Accidents to persons by rollingstock in motion	Other person not at a platform	Delays	Train Speed Supervision
		Communication cut off					Maintenance
People crossing track	Human error	People ignoring warning signs		Accidents to persons by rollingstock in motion	Employees	Injuries	
						Death	Maintenance
	Signal malfunction				Passangers	Damage to vehicle	Signs
					Other person at a platform	Delays	Signals

Table 7.2 Hazard log for the ERTMS

<u>Level crossing not safe</u>

Situation in which the level crossing is not free for the train to cross. This could mean that there is a car, motorcycle, bike or a pedestrian in the level crossing area while there is a train passing it.

<u>ERTMS failure</u>

A situation in which one or more parts of the system fails to work properly.

People crossing track

Situation in which there are people crossing the rails when there is a train driving on the rails.

The ERTMS is actually very well designed, with several built-in safety mechanisms that will cause the train to stop whenever malfunction is detected, the movement authority is not renewed within limit, or if any other unexpected circumstance arises.

The safety procedure is then initiated, the train driver contacts the traffic control operator and after going through a specific protocol, the driver takes over the control of the train and proceeds with lower level of ERTMS or without it at specified low speed. Other hazards may occur at that point, but are not included in this analysis because at that point the system is not in normal operational conditions.[16]

7.3 Fault Tree

The Fault Tree Analysis was used as addition to the CSM. The purpose being better understanding of how the systems would react in a hazardous situation and make the output easier to understand and compare. These graphical representations serves well for the purpose of this project, when comparing these two systems.

7.3.1 The Event

To better compare the two systems a scenario was devised. This scenario will help comparing the functional aspects of the two systems. A scenario involving an identical danger was presented to both systems to see how the system would react to the given situation. A Fault Tree Analysis was applied to both systems to demonstrate the systems' barriers and reveal which parts of the systems would have to fail for the scenario to end up in an accident.

The Fault Tree analysis concept was further explained in chapter 5.2.1.3.

The scenario is as follow: Two trains are on the collision course on a one-way track. They could be heading on the opposite direction, towards each other or meeting a slower or stopped train heading in the same direction. For the Traditional Signalling, it would be an unusual situation for the trains to meet head to head, because under the normal circumstances two trains should not be put on the one-way track heading towards each other at the same time. For the ERTMS however, this would be a normal practice.

This scenario was chosen for several reasons. One being that this scenario has the most serious potential consequences in both systems, as seen in the Hazard Log in previous chapter 7.2. Other reasons being that similar scenario has occurred recently in Jutland as a part of the testing of the ERTMS. According to Atkins this test was not very well conducted, as the parties involved were not properly informed and the whole test resulted in an unpleasant incident for both the railway company and drivers, thankfully as it was in a testing phase no passengers were on board.[44][45] [46]

7.3.1.1 Traditional Signalling

For the purpose of the table being easier to read and understand the assumption was made that in this scenario the driver does not notice the impending collision in time to safely brake. As shown in a Figure 7.1, there are several instances that can cause two trains to collide.

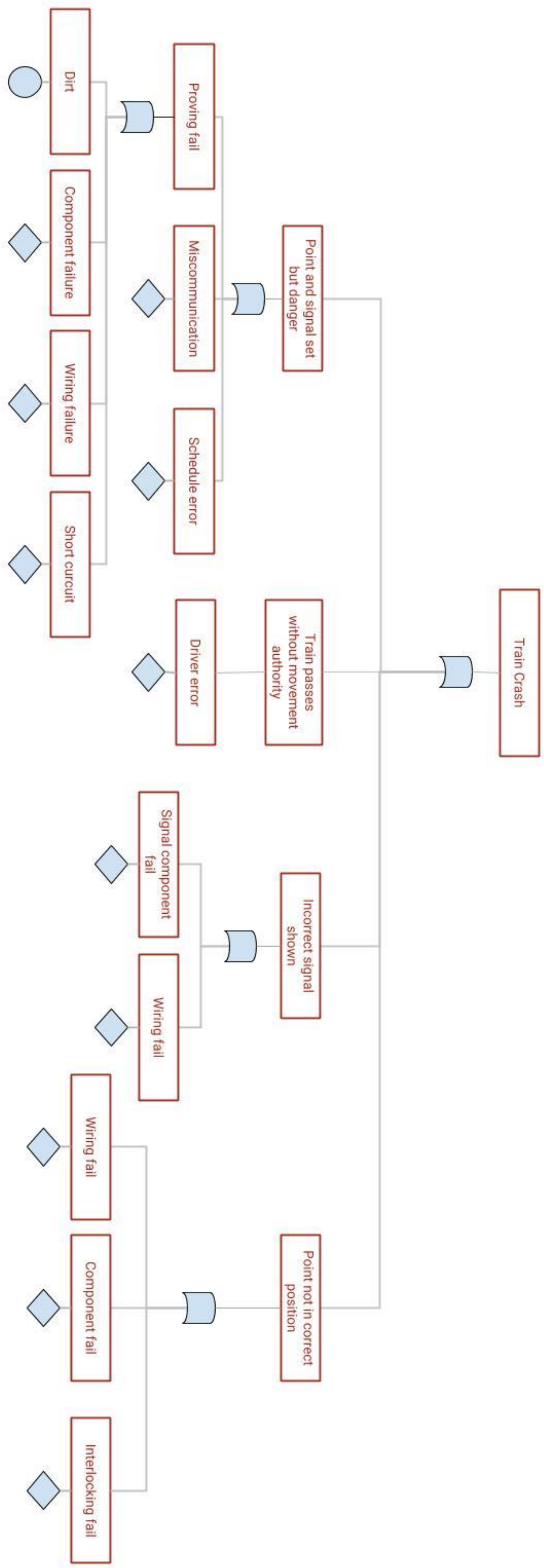


Figure 7.1 Fault Tree Analysis for Traditional Signalling

Point and signal set but danger

In this situation there is a signal and point set in a position that would send a train into a dangerous situation. That could be caused by several reasons, such as scheduling error or miscommunication, which are considered to be human error, since there is not electronic checking system in place. Another option is a proving fail occurring. That could be caused by the hardware failure. The hardware parts of the system are also somewhat sensible to weather, considering the fact that some of the parts work on the principle of conducting electric current, like the vacancy proving. Elements like snow or salt can cause false positives or negatives.

Train passes without moving authority

Situation where the train passes a point where it was supposed to stop.

Incorrect signal shown

In this situation there is an incorrect signal showing even though the initial signal was correct.

Point not in correct position

In this situation the point is not in the desired position and can send the train onto a collision route.

7.3.1.2 European Railway Traffic Management System

For the purpose of the table being easier to read and understand the same assumption was made as with the Traditional Signalling, that in this scenario the driver does not notice the impending collision in time to safely brake. Additional assumption was made, that the system constantly monitoring for errors in the system, the Health monitoring system, would fail as well. In Figure 7.2 there are several situations that could theoretically cause the train to collide with another train.

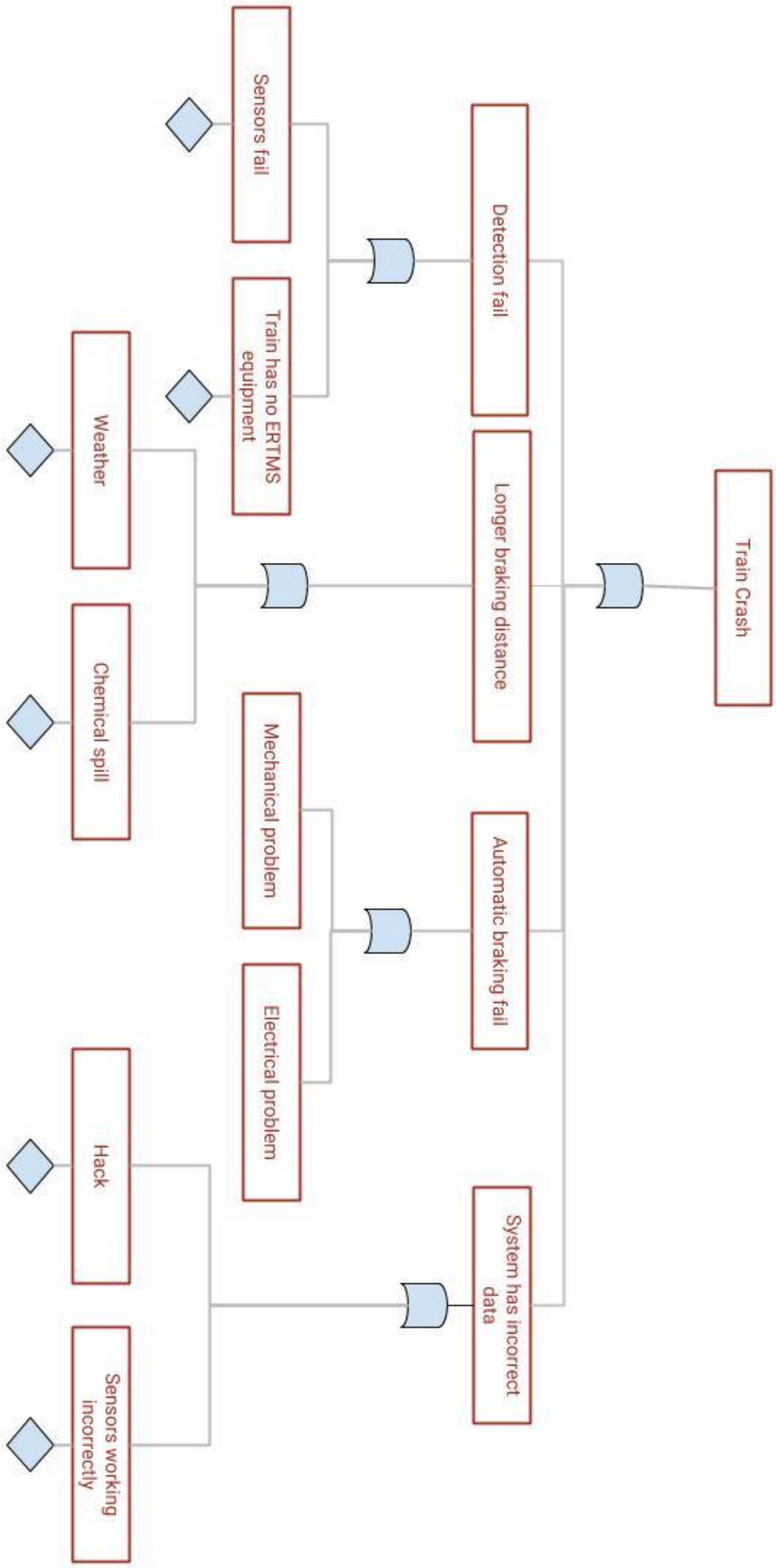


Figure 7.2 Fault Tree Analysis for ERTMS

Because of numerous safety features included in the ERTMS, it is quite unlikely that the system has incorrect data, detection fail or the automatic braking failure would occur. Keeping in mind that there would also would have to be failure of the Health Monitoring System and the driver would have to fail to notice the impending collision in time. The data received is compared with other data, and have a unique code and etc., detection fail would have to involve a train without the ERTMS equipment to be put onto a track, which would not be possible under normal circumstances (however, this could happen during the implementation phase as both types of systems need to be in use while updating the trains onboard system). Because the system has not been fully deployed yet, there are no failure statistics publicly available at the moment. When these data are available, the data could be added to this table for additional results. The longer braking distance seems to be the most likely hazard.

Detection Fail

A situation where the train would not get detected, causing other train to collide with it.

Longer Braking Distance

In this scenario the system would initiate the emergency braking, for example because of would detect two trains at the same track section, which is not allowed, but the conditions on the rails would not allow for the trains to brake in time. The braking distance set by the system design would not be enough because of the unexpected conditions.

Automatic Braking Fail

Situation where the system would fail to activate the automatic braking in case of danger, the movement authority was not renewed or other situation where the automatic braking should be applied.

System Has Incorrect Data

In this situation the system would receive incorrect data that would lead to the dangerous situation.

8. Comparison

After simply identifying the two systems, the 60-year gap between these two systems is clear. While the Traditional Signalling system is simpler in functions the newer ERTMS is more extensive and includes more features. Thus, the ERTMS system is much more extensive and complex.

To see how similar the systems are, there are several comparisons in this chapter.
A comparison of the Functional Diagrams for both of the systems was compared in order to see how differently or similarly the two systems operate.
To compare the system hazards and barriers, the Hazard Logs from both systems will be used.
To see how the two systems, deal with a specific hazardous scenario of two trains heading for a collision on a one-way track, the Fault tree analysis results will be compared.

8.1 Functional iagrams

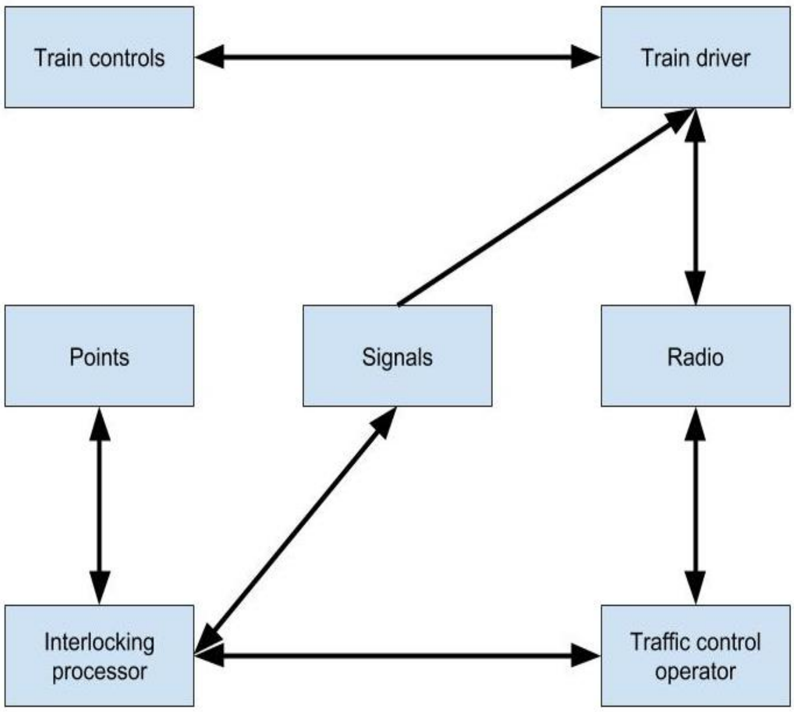


Figure 8.1Functional Diagram for Traditional Signalling

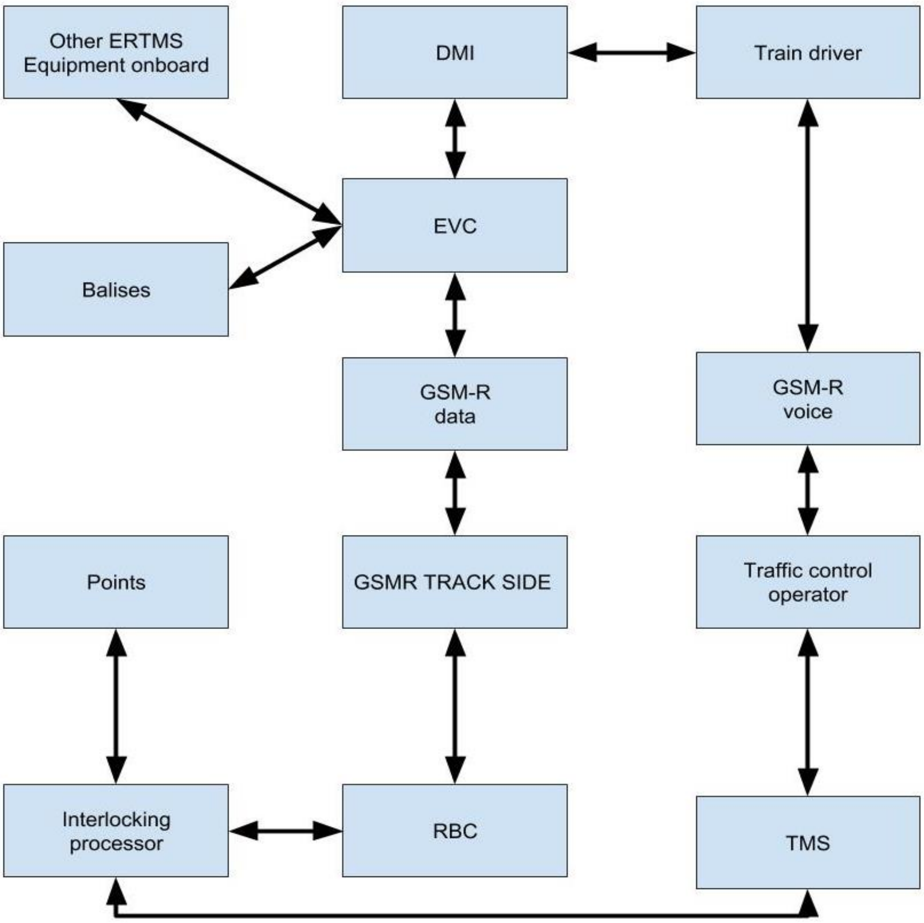


Figure 8.2 Functional Diagram for ERTMS

By comparing the functional diagrams, shown again in Figures 8.1 and 8.2, it shows that there are almost twice as many elements in the ERTMS than in the Traditional Signalling. Several safety barriers have been added and the system has grown in size and complexity.

In the Traditional signalling, the responsibility for smooth and safe running is mostly placed on the train driver and the traffic control operator. These two elements have to be highly trained and capable, because of the lack of safety barriers beyond the standard procedures and the design of the system itself. This makes the system more vulnerable when facing some unplanned changes, because the implementation of those changes would be mainly done by the traffic control operator. He would have to then forward the newly updated commands to the train driver via radio and inform other train drivers that could also be affected. Considering how such a task is demanding and complicated, there is a risk of an error or an impact on the efficiency.

The ERTMS on the other hand handles most of the organisational task, leaving the traffic control operator in a position of monitoring how the system is running, looking for possibilities of system malfunction along with dealing with tasks that are outside of the systems objective. The train driver is being given all the necessary information via the ERTMS, including the optimization of efficiency. Furthermore, there are several safety features and barriers embedded in the system, checking the operator and the driver for mistakes.

8.2 Hazard logs

When comparing the Hazard Logs for the Traditional Signalling and ERTMS it shows that only two hazards are the same in both tables. Those hazards are level crossing not safe and people crossing track. These two hazards are the two least influenceable by the systems because they involve people from outside of the system crossing through it. It also shows some different additional barriers applied in the newer system, meaning that there has been an increase in safety.

The older system is shown to have more hazards and to be more prone to mechanical failures along with human error. By adding the additional safety layers, the ERTMS eliminates the cause of a human error significantly, leaving it only in the hazards that are very difficult to manage by systems like this.

The ERTMS on the other hand is relying on the interconnection of most of the elements, giving it better control over what is happening almost in real time and very precisely, but at the same time being vulnerable to one malfunction influencing the whole system. It is however clear, that this sensibility adds to more safe running. It is clear that the new system has solved several of the hazards that were present with the older one. Even though the changes bring new hazards not present in the older system, the safety barriers included in the ERTMS, thanks to a more modern approach, should ensure better operational safety and efficiency. The system health monitoring is maybe the most powerful of the barriers in the ERTMS as it is constantly checking the system for faults. This way the fault or a malfunction can be discovered before it could cause any serious problems.

	Hazard Description			Hazard Classification			Hazard Treatment
Hazard	Cause of the hazard	Underlying causes for the hazard	Comments	Accident Type	Person Categories	Conssequences	Barriers
Track is not free	Route not locked	Interlocking processor	Electrical problem	Collission	Passangers	Damage to Infrastructure	Schedule
		Mechanism fail			Employees		
		Track occupied				Damage to vehicle	Driving procedures
	Signal malfunction	Signal broken	Dirt/ice blocking		Level Crossing User		Personnel
	Human error	Bad connection					Signals
		Power failure	Wiring problem		Other Person at a platform	Injuries	Safety intervals
	Vacancy proving fail	False negative/positive					Maintenance
		Mechanical problem	Component worn out		Other person not at a platform	Death	
	Train monitoring fail	Radio problem					
Level crossing not safe	Signal malfunction	Bad connection	Component worn out	Level crossing accidents (collission train-car/bike, person)	Passangers	Injuries	Level crossing signals
		Signal broken					
		Power failure				Death	Level crossing barriers
	Level crossing signal fail	Bad connection			Employees		Driver
		Signal broken	Wiring problem			Damage to vehicle	Legislation
		Power failure					Maintenance
	Level crossing barriers fail	Mechanical problem					
	Human error	Power failure			Level Crossing User	Damage to Infrastructure	
		Bad connection					
	Train monitoring fail	Radio problem					
Overspeed	Signal malfunction	Signal broken	Component worn out	Derailment, Collission	Passangers, Employees, Level crossing users, Other person at a platform, other person not at a platform	Injuries, Death	Maintenance
		Bad connection				Damage to Infrastructure	
	Human error	Ignore Signal	Wiring problem			Damage to vehicle	
People crossing track	Signal malfunction	Bad connection	Component worn out	accidents to persons caused by rolling stock in motion	Passangers,	Injuries	Maintenance
	Human error	Signal broken	Wiring problem		Other person at a platform	Death	Signs
							Signals
		Power failure			Employees	Damage to vehicle	Driver
Signal passed at danger	Vacancy proving fail	False negative/positive	Dirt/ice blocking	Collission, derailment, level-crossing accidents, accidents to persons caused by rolling stock in motion	Passangers	Injuries	Safety braking distance
		Mechanical problem	Component worn out		Employees	Death	
	Train monitoring fail	Radio problem	Wiring problem		Level Crossing User	Damage to vehicle	Maintenance
	Human error	Ignore Signal	Short circuit		Other Person at a platform		
	Failure to Stop	Lack of warning	Lack of friction		Other person not	Damage to	

Table 8.1 Hazard Log for Traditional Signalling

	Hazard Description			Hazard Classification			Hazard Treatment
Hazard	Cause of the Hazard	Underlying Causes for the Hazard	Comments	Accident Type	Person Categories	Conssequences	Barriers
Level crossing not safe	Human error	People ignoring warning signs		Level crossing accident	Level crossing user	Injuries	Level crossing signals
	Level crossing signal fail					Death	
	Level crossing barriers fail					Damage to vehicle	Level crossing barriers
						Damage to infrastructure	Legislation
						Delays	Maintenance
ERTMS failure	Component failure	Fatigue		Collision	Level crossing user	Injuries	Automatic brakes
		Bug in the system					Frequent movment authority updating
	Power failure	Weather		Derailment	Employees	Death	Constatnt system healt monitoring
		Fatigue			Passangers	Damage to vehicle	Data Consitancy Checking
		Power cut		Level crossing accident			
	Cyber attack	Train recieving incorrect information	System breach		Other person at a platform	Damage to infrastructure	Supervised Train Movements
		Train ignoring information	Firewall breakdown	Accidents to persons by rollingstock in motion	Other person not at a platform	Delays	Train Speed Supervision
		Communication cut off					Maintenance
People crossing track	Human error	People ignoring warning signs		Accidents to persons by rollingstock in motion	Employees	Injuries	
					Passangers	Death	Maintenance
	Signal malfunction					Damage to vehicle	Signs
					Other person at a platform	Delays	Signals

Table 8.2 Hazard Log for ERTMS

8.3 Fault Trees

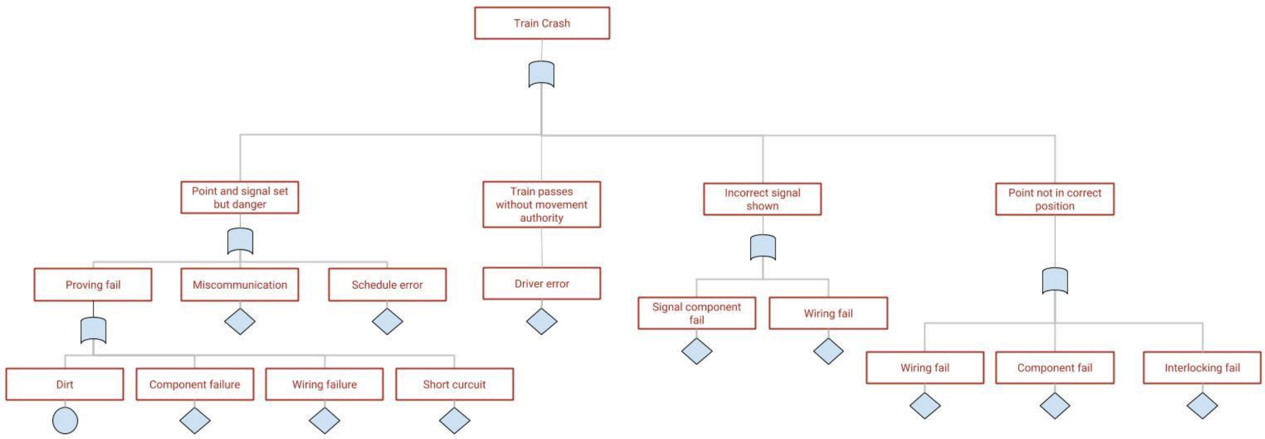


Figure 8.3 Fault Tree Analysis for Traditional Signalling

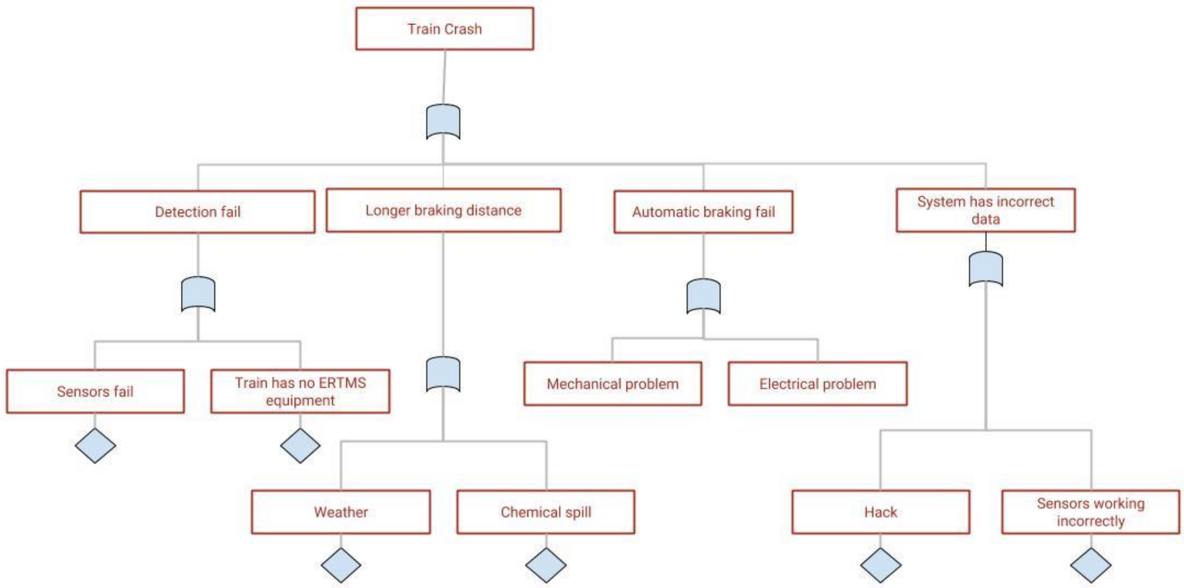


Figure 8.4 Fault Tree Analysis for ERTMS

Comparing the two fault trees for the scenario of two trains being on a collision course on a one-way track shows, that there are more possibilities for that happening in the Traditional Signalling than in the ERTMS. The Fault Trees can be seen in Figures 8.3 and 8.4.

Half of the events in the Traditional Signalling's fault tree could be caused by human error at some stage of the development of a dangerous situation. Making it more vulnerable for situations like that happening.

In the ERTMS, if eliminating the two possibilities that the system should prevent if working properly, those being detection fail and system has incorrect data, only two left are longer braking distance and brakes fail. brakes failing should be prevented by proper maintenance and therefore could be considered to be caused by human error. The longer braking distance is also an element that is difficult to influence by the system. The ERTMS has better control over the system than Traditional Signalling through the interconnection of most of its parts. It also has a mechanism that significantly lowers the possibility of human error resulting in such a serious situation like train crash, thus making it less prone to it and safer all together, thanks to its added safety features. More details about the safety features can be found in the chapter 6 Systems definitions.

8.4 Safety-I and II

8.4.1 Safety I

The Oxford Dictionary defines safety as:

"The condition of being protected from or unlikely to cause danger, risk, or injury."

This is sometimes translated to an absence of accidents or as a state whereas as few things as possible go wrong. This definition assumes that accidents transpire because of recognizable failures or errors of specific factors, be it technology, processes, or the workers and the organizations to which they are embedded. Through this assumption, humans are viewed as a liability typically because they are the most unpredictable of these factors. In this sense, the intent of hazard identification is therefore to identify the causes related to accidents and the risk assessment their probability. The safety management in this perspective is a response to a hazardous event or unacceptable risk by eliminating causes or improving mitigation measures.

This method assumes that systems work in binary ways, such as either functioning or malfunctioning and thereby seeking and examining the errors. This means that this method does not examine the human performance that almost always succeeds. This is not because people are always work according to a procedure, but because humans adjust to conditions required of the work. As systems are evolving and becoming more complex, adaptation becomes gradually more necessary to provide a satisfactory performance. It is therefore also necessary to understand how performance usually goes right, despite the uncertainties that encompass complex circumstances. Erik Hollnagel suggests that safety management should ensure that as many things as possible can go right instead of aiming to safeguard that as few things as possible can go wrong. This new approach he terms as Safety-II where the conventional practice described above is named Safety-I [47].

8.4.2 Safety-II

The safety-II approach is based on resilience engineering and has a changed definition of safety from avoiding failures to:

> *"…the ability to succeed under varying conditions, so that the number of intended and acceptable outcomes (in other words, everyday activities) is as high as possible."* [47].

By this definition, people are able to identify and overcome functional flaws by responding through normal performance variability, which provides the adaptations required to react to shifting conditions, and for this reason, things go right. People are also able to perceive and pre-emptively counter errors when systems are about to malfunction, thereby rectifying situations from becoming dangerous.

Contrary to Safety-I, Safety-II accepts that systems are incompletely understood and that changes to systems are common and sporadic. In this sense, human variability is not seen as a negative deviation from the norm but a positive adjustment that increases the resilience of systems. Therefore, performance variability is an indispensable condition for socio-technical systems unless they are extremely simple. To support this type of lateral thinking, efforts must be made in aiding to anticipate the consequences of actions, e.g., by making explicit representations of resources and restrictions of given situations. Unwanted consequences cannot be averted by removing or limiting performance variability because that would also influence the desired outcomes, however performance variability must be managed to reach an effective balance.

Both Safety-I and Safety-II can reduce undesirable effects, but the methods and measurements used are fundamentally different as shown in the Table 8.3. below.

	Safety – I	Safety - II
Definition of safety	As few things as possible go wrong	As many things as possible go right
Safety management principle	Reactive - respond when something happens	Proactive - try to anticipate developments and events
Explanation of accidents	Accidents are caused by failures and malfunctions	Things basically happen in the same way regardless of the outcome
View of the human factor	Liability	Resource

Table 8.3 Safety I & II [47]

8.4.3 Safety-I and II Application and Comparison

In risk management safety is often measured on the number of events occurred in an interval of time. The risk is then sought to mitigated by looking at the system, and in particular investigating how the human deviated from procedure, which enabled an accident to happen. However, as previously mentioned, most of the time in hazardous situations the opposite is the case. The system fails by way of human error, procedural or technical malfunction, and the inherent mitigation of a system is a human being that adapts to the situation and corrects the problem before an accident is allowed to take place.

In the Traditional Signalling system, there is a large portion of trust involved when letting humans control trains. Rules, procedures and safety measures are in place, but some actions are still left to a person's own judgement, such as speed and brake control, within specific boundaries. Drivers are accompanied by a more experienced driver until sufficient familiarity is obtained on a railway line, and only then is a driver allowed to drive on his own. Whenever the driver needs to drive the train on a line of which he is not familiar, he is accompanied by a driver who is. This leaves room for situational knowledge sharing and human interpretation of procedures on every railway line, based on experience with the procedure and the specific situation. This corresponds to the idea in safety-II of letting novices in work situations be bound by precise processes, but gradually allowing procedural boundaries to expand as experience grows. The same is true for the traffic control operator of the interlocking processor. There are actions that the interlocking processor does not allow, as shown in chapter 6.5.4, but the human traffic controller decides how the train arrives to the station based on a unity of organizational procedures, technical safety measures and system experience. These are the same three factors as previously depicted in chapter 1.6 in the HOT-diagram. If the traffic controller anticipates an unwanted situation, he has the option of informing the drivers via radio, and together they may cooperate towards a solution.

Whether this leads to an accident can be either the result of an epistemic or aleatory uncertainty but, when assessing the risk of this situation afterwards, the assessment will likely still predominantly be based on the assumption of the unpredictable human error in the organizational and mechanical system. Models such as the domino theory is one of the common theories used in safety management for mapping the causes of accidents. [48] One of the main assumptions of the first domino model was human inadequacies in mechanical systems. The model can be seen in Figure 8.6.

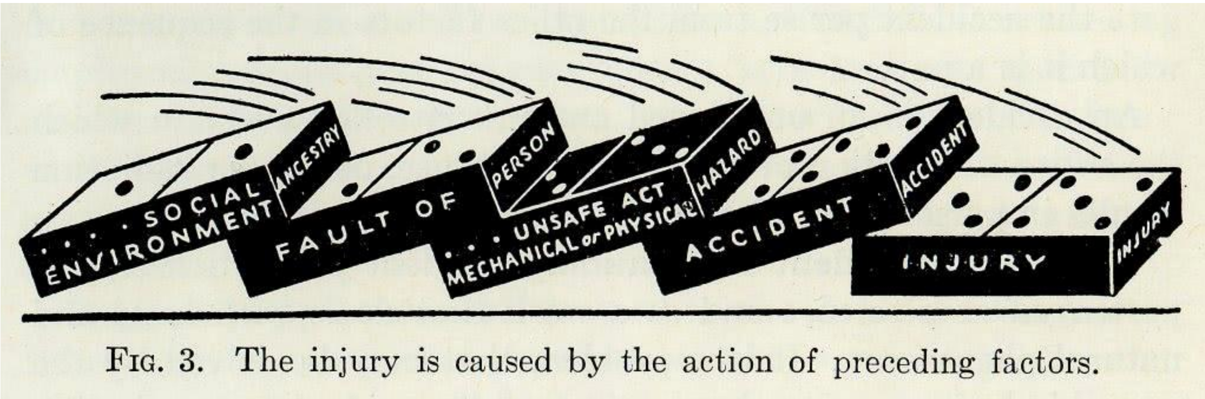


Figure 8.5 The Domino Model[49]

The Functional Diagrams of this project both for the Traditional Signalling system and the ERTMS depict how the work is imagined, but not how it is done, since it is based on official procedures and not the pragmatic processes of the everyday work. How the two processes deviate is a question for further research.

The new ERTMS system continues the old risk management tradition of mitigating human error rather than enabling human adaptation to system errors, by further limiting human action in the system. This is done by strictly, and continuously, informing the person in place of the organizational procedure required in every situation of the work shift as shown in chapter 6.6. This way it is anticipated that fewer accidents will occur. The driver receives almost all of the instructions through the DMI, which also limits his actions from deviating from the given commands. In the new system, trust is shifted away from human experience and over to the technical and procedural system. The driver no longer requires the company of experienced drivers for the journey on railway lines that are unfamiliar to him, because that role has been replaced by technical safety measures. Although, this new system can reduce some aleatory uncertainty by reducing the variability of the human and organizational processes in unfamiliar situations, the epistemic uncertainty in work as imagined compared to the work done remains an issue. Therefore, preparation of train drivers, traffic controllers and other personnel interfacing with the system to improve the human and organizational resilience is advised according to a safety-II perspective.

8.5 Sub-Conclusion

After comparing the two systems in terms of functions, hazards, barriers and in handling a hazardous situation, the age gap between them shows even more. However, both systems have similar functions and are reasonably safe to operate, even though their structures are different. Therefore, they can be considered comparable.

A summary of the systems' functions and barriers comparison can be seen in Table 8.4 in the end of the chapter.

8.5.1 Functionality

Even though both systems fulfil the main objective, that is managing trains, it is clear that the ERTMS has significantly more functions than the rather simple Traditional Signalling system. These additional functions help the ERTMS with better monitoring of the traffic, train movements, current situation and also with monitoring the state of the system itself. In the Traditional Signalling the monitoring, organizing and management was for the most part in the hands of the traffic control officer and any changes to the pre-arranged schedule would have to be resolved by him too. The ERTMS system can adapt to the changes more easily, since it is monitoring all the traffic in the area constantly and the transition of the information through the GSM-R data network is much more efficient, especially to multiple receivers.

8.5.2 Hazards and Barriers

The comparison showed that the amount of the potential hazards in the Traditional Signalling system is almost double compared to the ERTMS. Additionally, since the Traditional Signalling is relying more on the human factor, most of the hazards have a human error as a possible cause. The ERTMS mitigates these hazards by integrating several new barriers and controlling mechanisms, as can be seen in better detail in the Safety Measures and Requirements for ERTMS Chapter 6.6.4.

However, two of the hazards are the same for both systems, level crossing not safe and people crossing the track. These are the most difficult to influence, since they involve civilian people who are crossing the otherwise closed and controlled system of professionals and instructed employees. In these two hazards the Traditional Signalling may have an extra barrier in for of a train driver. Since the ERTMS is informing the driver of the necessary information via the DMI the driver may pay less attention to the situation ahead. The train driver in the Traditional Signalling has to interpret the information from the signals along the track himself, thus paying constant attention to what lies ahead. The Traditional Signalling also does not allow the trains to travel as fast as the ERTMS, which would also mean shorter braking distance.

In summary, the ERTMS proves as more safe system with less hazards and more barriers than the Traditional Signalling.

8.5.3 Hazardous Event

When comparing the Fault Tree Analysis results for the scenario of two trains approaching on a one-way track, it shows that the Traditional Signalling has more potential events leading to a train crash. Under the ERTMS it is actually very difficult to reach the situation that the two trains would collide. Since, the systems has very good barriers to prevent it from happening, the train would most likely stop, as soon as one of the many components would report a failure. This is thanks to the constant updating on the system, and its combination with the frequent updating of MA for the system is well prepared for preventing this to kind of event from happening under normal circumstances.

The Traditional Signalling is more prone to this than the ERTMS mainly, since it is not monitored as frequently, resulting in it being exposes it to the possibility of an unobserved malfunction, consequently having less barriers and relying more on human factor.

8.5.4 Summary

	System	
Functions	TS	ERTMS
Interlocking	X	X
Signalling	X	
Track vacancy proving	Analog	Digital
Axle counting		X
Train monitoring	Analog	Digital
Voice communication	X	X
Data cominucation		X
Updating movement authority	Signals	GSM-R
Safety features	TS	ERTMS
Safety delay interval	X	
Train speed supervision		X
Automatic braking		X
Data consistency monitoring		X
Train position monitoring		X
System health monitoring		X
Odometry monitoring		X
Track condition control		X

Table 8.4 Summary of the System´s Functions an Barriers

9. Discussion

One of the problems regarding ERTMS, is the fact that it is rather new, although the system has been implemented on certain tracks gradually throughout Europe, so no nations network has been changed completely to ERTMS. This has caused some problems and delays for Denmark. Since the start of the ERTMS implementation project, it has been delayed by 9 years, and the total cost has increased by 7 billion DKK, making the total cost around 20 billion DKK, thus making it the most expensive project in the history of Danish railway. [50] By the end of 2011, 2700 km were equipped with ETCS and in operation in Europe[51][52], which is only 200 km more than the whole of the Danish railway system that accounts for 2508 km as in 1st of January 2018. (According to Denmark's Statistics, BANE41)

In this project, the systems were compared based on functionality, hazards and barriers, which give an insight into the differences of the two systems. Although, it would have been interesting to further compare additional data such as reliability, efficiency, delays etc, regarding both systems. Therefore, there are no similar researches to be compared with the results of this project. It is worth to mention that it is irrelevant to use data from other countries using the ERTMS, as their signalling systems used before ERTMS might not correspond to the Danish one.

Assumptions today predict that the ERTMS will work up to 80% more efficiently and decrease the delays that have been occurring due to the previous signalling system. However, assumptions do not always meet expectations. Means that if the new ERTMS system had been further in the implementation stage into the Danish Railway System, more knowledge and data would have been gained about the actual efficiency of the system. Thus, the results from this thesis might be different in a few year’s time given that the ERTMS system will be further implemented. That would be because of data analysis and studies could then be done, which would be based on real working conditions. Additionally, it would be interesting to further research a larger section of the track than just one station.

In addition, it can be said that it is hard to compare these two systems, first of all because of the big-time gap in between the systems. As, one is from 1950’s, while the other was first made after 2000. Second of all, replacing the Traditional Signalling is simply a small part of the ERTMS. In this case it is taking a system that is located on the side of the train tracks, and not only moving it, but completely changing it into different displays in a DMI. Further, the ERTMS system is equipped with more extensive system. Helping it monitor the train speed and increase the safety, by having the possibility for the system to take over the control and make sure that the train does not overspeed, to the point of not being able to stop before hitting an obstacle.

10. Conclusion

In this project two train management systems were subjected to analysis with the aim to find if they could be comparable, what are their functions, hazards and barriers. The systems used were the Traditional Signalling system and the new European Rail Traffic Management. On the basis of the information gathered a definition was conducted for each system and then their functions were explored and further listed. Several methods were used to identify the systems' hazards and barriers. Based on the results of the system definitions and hazard identification several parameters were chosen based on which the comparison of the systems was done. The parameters were set to be functionality, hazards and barriers.

To summarize, at the basic level of the systems, these two systems are comparable, as they are both have similar functions and are safe to operate. Therefore, it can be concluded that both systems can fulfil their objective to manage trains in a reasonably safe manner. However, when it comes to the functions of the two systems, it is clear that the systems are different, which is clearly shown in the comparison of the functional diagrams. This is due to the fact that the ERTMS, is more extensive in its functions, than the simple Traditional Signalling system.

When it comes to the hazards and barriers for both systems, the ERTMS has proven to contain less hazards and more barriers for mitigation, while the Traditional Signalling system has fewer hazards, along with fewer barriers. Additionally, there is a considerable difference in the way the two systems achieve the desired state. The older Traditional Signalling depends more on the human factor, whereas the European Rail Traffic Management System has embedded many new safety features that supervise the human operators.

Unfortunately, at this point there are not enough information and data available to compare these two systems in a way of reliability, efficiency or running costs within Denmark, although the data in this project suggest that the European Rail Traffic Management System would perform significantly better than the older Traditional signalling in the reliability and efficiency. As of that, for future research it would be suggested to conduct similar study when more information is available on the European Rail Traffic Management System with more aspects added or possibly with a quantitative focus.

11. References

[1] McGhie Steffen, "Danmarks største jernbane-projekt bygger på lappeløsninger | Ingeniøren," *Ingeniøren*, 27-Mar-2017.

[2] M. S. Jensen Lasse, "GRAFIK: Sådan skal udrulningen af ERTMS forløbe | Ingeniøren," *Ingeniøren*, 23-Oct-2018.

[3] Banedanmark, "Det nye signalsystem på fjernbanen - ERTMS | Banedanmark," *Banedanmark*. [Online]. Available: https://www.bane.dk/da/Borger/Baneprojekter/Signalprogrammet/Fjernbane/Det-nye-signalsystem-paa-fjernbanen-_-ERTMS. [Accessed: 17-Dec-2018].

[4] Banedanmark, "Første strækning med det nye signalsystem i drift | Banedanmark," *Banedanmark*, 2018. [Online]. Available: https://www.bane.dk/da/Borger/Baneprojekter/Signalprogrammet/Nyheder/Foerste-straekning-i-drift-med-det-nye-signalsystem. [Accessed: 22-Oct-2019].

[5] "Jernbanens nye digitale signalsystem går i drift i Nordjylland | Ingeniøren." [Online]. Available: https://ing.dk/artikel/jernbanens-nye-digitale-signalsystem-gaar-drift-nordjylland-221263. [Accessed: 05-Nov-2018].

[6] "Uncontrolled When Printed Glossary of Signalling Terms," 2004.

[7] "The defintion accident," *Oxford Dictionaries*. [Online]. Available: https://en.oxforddictionaries.com/definition/accident. [Accessed: 10-Jan-2019].

[8] "Oversigt over sikringsanlæg - Strækning 31." [Online]. Available: http://www.blokposten.dk/sikr/oversigt/sikr-strk31.htm. [Accessed: 07-Jan-2019].

[9] Banedanmark, "SR Sikkerhedsreglement," Banedanmark, 1975.

[10] "Se hvem der skal skifte signaler for milliarder på fjernbanen | Ingeniøren." [Online]. Available: https://ing.dk/artikel/se-hvem-der-skal-skifte-signaler-milliarder-paa-fjernbanen-125159. [Accessed: 14-Nov-2018].

[11] UNIFE, "ERTMS in brief | ERTMS." [Online]. Available: http://www.ertms.net/?page_id=40. [Accessed: 04-Dec-2018].

[12] THALES, "European Train Control System (ETCS) | Thales Group." [Online]. Available: https://www.thalesgroup.com/en/european-train-control-system-etcs. [Accessed: 19-Dec-2018].

[13] "ERTMS | The European Railway Traffic Management System," *ERTMS*. [Online]. Available: http://www.ertms.net/wp-content/uploads/2018/10/3-ERTMS-Levels1.pd/. [Accessed: 04-Dec-2018].

[14] UNIFE, “ERTMS Levels,” 2017.

[15] C. Kessell, “ERTMS Level 3 – A possible way forward – Rail Engineer,” *Rail Engineer*, 2017. [Online]. Available: https://www.railengineer.uk/2017/04/25/ertms-level-3-a-possible-way-forward/. [Accessed: 08-Jan-2019].

[16] RSSB, “GE/GN8605 ETCS System Description,” 2010.

[17] “GSM-R - Det nye togradiosystem | Banedanmark,” *Banedanmark*. [Online]. Available: https://www.bane.dk/da/Borger/Baneprojekter/Signalprogrammet/Fjernbane/Nyt-udstyr-i-togene/GSM_R. [Accessed: 08-Jan-2019].

[18] McGhie Steffen, “Nu er de sidste analoge togradioer slukket | Ingeniøren,” *Ingeniøren*, 03-May-2017.

[19] European Committee for Electrotechnical Standardization, “Railway Applications – The Specification and Demonstration of Reliability , Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process.” 2018.

[20] the International Organization for Standardization, “ISO Guide 73:2009: Risk management - Vocabulary,” 2009.

[21] T. Donaldson and L. E. E. E. Preston, “The Stakeholder Theory of the Corporation : Concepts , Evidence , and Implications,” *Acad. Manag.*, vol. 20, no. 1, pp. 65–91, 1995.

[22] R. K. Mitchell, B. R. Agle, and D. J. Wood, “Toward a Theory of Stakeholder Identification and Salience : Defining the Principle of Who and What Really Counts,” *Acad. Manag. Rev.*, vol. 22, no. 4, pp. 853–886, 1997.

[23] T. F. Yosie and T. D. Herbst, “Using Stakeholder Processes in Environmental Decisionmaking,” *Ind. Health*, no. September, 1998.

[24] M. L. Attrup and J. R. Olsson, *Power i projekter og porteføljer*, 2nd ed. Jurist- og Økonomforbundets Forlag, 2008.

[25] O. Renn, “Risk Communication: Insights and Requirements for Designing Successful Communication Programs on Health and Environmental Hazards,” 2008.

[26] Steffen McGhie, “Banedanmark hemmeligholder konsulentbudget: Er steget med mindst fire milliarder,” *Ingeniøren*, 13-Aug-2018.

[27] Magnus Bredsdorff, “Kun to bud på signalsystemets plan B: Derfor steg prisen med 138 pct.,” *Ingeniøren*, 28-Nov-2018.

[28] Steffen McGhie, “Danmark ignorerede alle røde lamper for at være først med ERTMS,” *Ingeniøren*, 24-Dec-2018.

[29] "Automatic Train Control - Mobility - Siemens."

[30] McGhie Steffen, "Jernbanens nye digitale signalsystem går i drift i Nordjylland | Ingeniøren," *Ingeniøren*, 22-Oct-2018.

[31] Office of Rail and Road UK, "European railway safety legislation | Office of Rail and Road." [Online]. Available: http://orr.gov.uk/rail/health-and-safety/health-and-safety-laws/european-railway-safety-legislation. [Accessed: 03-Jan-2019].

[32] T. Aven, *Risk Analysis Assessing Uncertainties beyond Expected Values and Probabilities*. John Wiley & Sons, Ltd, 2008.

[33] DS EN, "61025: 2007 Fault tree analysis (FTA)," *Dansk Stand.*, 2007.

[34] C. N. Pyrgidis, *Railway Transportation Systems: Design Construction and Operation*. CRC press, 2018.

[35] D. et. al Hutchison, *Abstract State Machines Alloy, B, TLA, VDM, and Z*. Springer International Publishing, 2014.

[36] Krøyer Kent, "Signalsystem for 24 milliarder: Skærm i førerkabine afløser lamper ved skinner | Ingeniøren," *Ingeniøren*, 11-Dec-2008.

[37] "Første oldnordiske jernbanesignal skrottes i dag | Ingeniøren." [Online]. Available: https://ing.dk/artikel/foerste-oldnordiske-jernbanesignal-skrottes-i-dag-159235. [Accessed: 14-Nov-2018].

[38] E. H. Abdelwahed, D. Méry, C. Ordonez, and D. Hutchison, *Model and Data Engineering*, vol. 8216. 2013.

[39] MERMEC, "ERTMS/ETCS Level 1." [Online]. Available: http://www.mermecgroup.com/protect/atpatc-systems/629/ertmsetcs-level-1.php. [Accessed: 10-Jan-2019].

[40] MERMEC, "ERTMS/ETCS Level 2." [Online]. Available: http://www.mermecgroup.com/protect/atpatc-systems/630/ertmsetcs-level-2.php. [Accessed: 10-Jan-2019].

[41] McGhie Steffen, "Nye togsignaler forhindrer ikke tog på kollisionskurs | Ingeniøren," *Ingeniøren*, 29-Aug-2018.

[42] M. Palumbo, "ERTMS_ETCS_signalling_system_MaurizioPalumbo1.pdf," 2014.

[43] "ERTMS - Levels and Modes - European Commission," *European Commission*. [Online]. Available: https://ec.europa.eu/transport/modes/rail/ertms/what-is-ertms/levels_and_modes_sv. [Accessed: 07-Jan-2019].

[44] McGhie Steffen, "Tidligere DSB-sikkerhedschef: »Enhver sikkerhedschefs mareridt« | Ingeniøren," *Ingeniøren*, 31-Aug-2018.

[45] McGhie Steffen, "»Den her sag lugter langt væk af, at man ikke vil have den ud til offentligheden« | Ingeniøren," *Ingeniøren*, 02-Sep-2018.

[46] McGhie Steffen, "To tog var 177 meter fra at støde sammen under test af det nye signalsystem | Ingeniøren," *Ingeniøren*, 28-Aug-2018.

[47] E. Hollnagel, "A Tale of Two Safeties," *Nucl. Saf. Simul.*, vol. 1, no. 13, pp. 1–13, 2012.

[48] H. W. Heinrich, *Industrial Accident Prevention. A Scientific Approach.*, no. Second Edition. New York & London : McGraw-Hill Book Company, Inc., 1941.

[49] Eric Marsden, "Heinrich's domino model of accident causation," *Risk Eng.*, 2017.

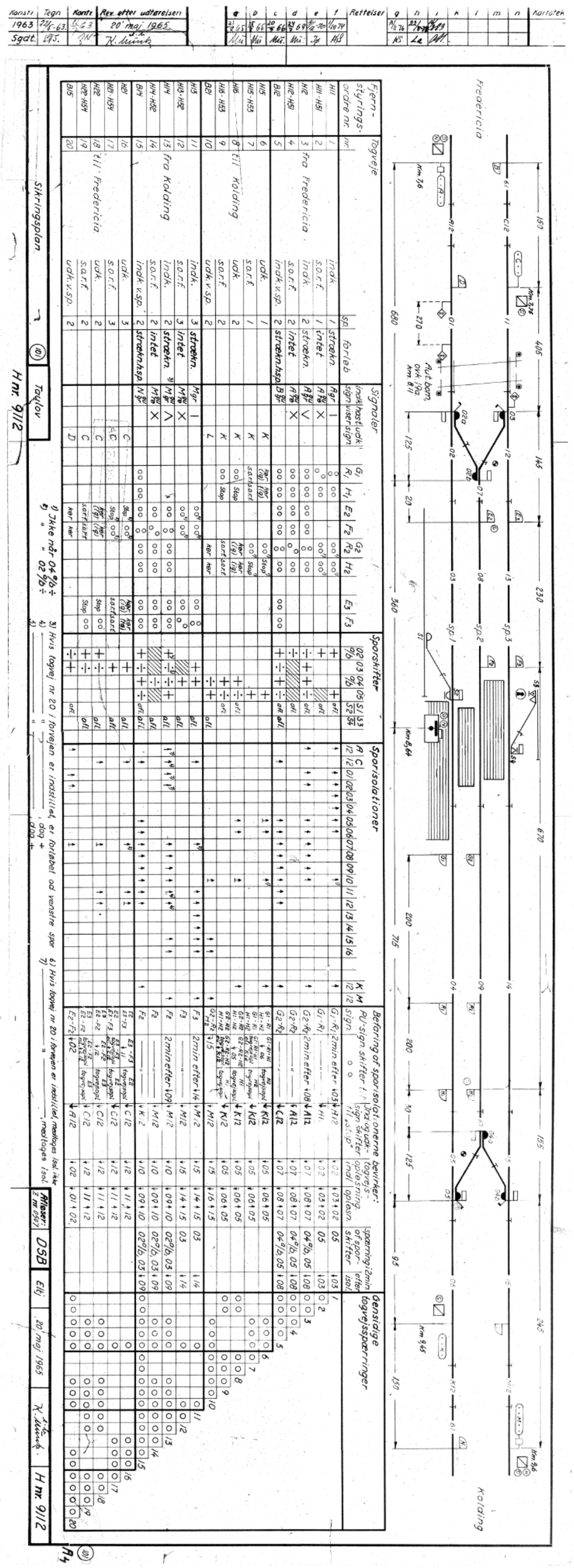
[50] McGhie Steffen, "Danmark ignorerede alle røde lamper for at være først med ERTMS | Ingeniøren," *Ingeniøren*, 24-Dec-2018.

[51] "European Rail Traffic Management System (ERTMS) - Railway Technology," *Railway Technology* . [Online]. Available: https://www.railway-technology.com/projects/european-rail-traffic-management-system-ertms/. [Accessed: 09-Jan-2019].

[52] "ERTMS Implementation - UIC - International union of railways," *UIC*, 2009. [Online]. Available: https://uic.org/ERTMS-Implementation. [Accessed: 09-Jan-2019].

Appendixes

Appendix A



Appendix B

Description of Station Plan for Traditional Signalling at Taulov Station. Explanations gained from Per Stoltze at Atkins.

Sikringsplanen viser Taulov station. Sikringsanlægget findes ikke mere. Taulov er i dag en del af sikringsanlægget i Fredericia.
Det gamle anlæg i Taulov bliver brugt til undervisning i 1953-sikringsanlæg.

Øverst er vist spor og signaler. Der er en overkørsel i Fredericia-enden.
Der er tre perroner (vist som firkanter med tætte streger).
På den nederste perron er kontrolposten vist som en hvis firkant. Den sorte streg er centralanlægget. Prikken er stationsbestyreren. Man har derfor en vis idé om hvordan stationsbestyreren ser stationen.

Der er tre togvejsspor og to henstillingsspor.

Signaler er vist. Overkørslen er forsynet med uordenssignaler (ikke overkørselssignaler).
A er et indkørselssignal (kan kendes på 4 lamper/prikker) og hastighedsviseren.
B er et PU-signal. Kan kendes på formen.
C er et udkørselssignal (kan kendes på 3 lamper/prikker)
Man kan se hvilken vej signalet vender på placeringen af signalmasten (sammenlign A og M) og ud fra at signalet står til højre for sporet.

Sporisolationer er vist som et tal. Isolationsstød mellem to sporisolationer er vist som et T

Sporskifter er vist med forskellige symboler. 03 er et helt almindelig sporskifte.
02a og 02b er to koblede sporskifter.

S1, S2, S3 og S4 er manuelle sporskifter. Efter hukommelsen er S1 og S2 magnetaflåst (Stationsbestyreren frigiver det ved at trykke på en knap. Derefter kan rangerfolkene omlægge det med håndkraft). S3 og S4 er nøgleaflåst (Stationsbestyreren frigiver det ved at udlevere en nøgle. Derefter kan rangerfolkene sætte nøglen i sporskiftedrevet og omlægge det manuelt).

Tegningen viser også nogle kilometreringer og en masse afstande (i meter).

Tabellen under tegningen viser togvejene. Der er 20.
Læg mærke til at stationsbestyreren vælger indkørsel og udkørsel separat. Det giver mulighed for at han kan lade toget vente (ved ikke at sætte en togvej), han kan vælge perron, han kan vælge om toget skal køre i høre eller venstre spor og han kan vende toget. Simpelthen ved at stykke en indkørsels- og en udkørselstogvej sammen.
Sikringsanlægget opløser selv togvejen efterhånden som toget kører gennem den togvejen. Stationsbestyreren kan ikke tilbagekalde eller opløse en togvej. (Stationsbestyreren kan lave en nødopløsning. Det får alle signaler på hele stationen til at gå på rødt i 2 minutter. Derefter opløses alle togveje. Stationsbestyreren skal skrive en forklaring i telegramjournalen. Og så skal han til at rydde op i stoppede tog og tale med vrede lokoførere).

Glem første kolonne. Den handler om fjernbetjening af sikringsanlægget.

Togvej nr 1 er fra Fredericia til indkørsel i spor 1.
Togvej nr 2 er fra Fredericia til SORF (stop og ryk frem) i spor 1. Ved SORF kører lokofører på sigt og det er ikke garanteret at sporet foran toget er frit.

Kolonnen ”Forløb” fortæller hvor sikkerhedsveje er placeret, dvs. hvor kan toget rutche hen, hvis skinner er glatte.
For togvej 1 kan toget rutche ud på strækningen mod Kolding (strækn).
For togvej 2 er der ingen sikkerhedsafstand. (i daglig tale: TUS = togvej uden sikkerhedafstand). Derfor er der heller ingen sikkerhedsvej.
For togvej 5 kører toget ad venstre spor til spor 2 og sikkerhedsvejen ligger på strækningen mod Kolding i højre spor (strækn h sp)

For togevej 1 skal indkørselssignal A vise grøn (A gr). Signalet viser grøn (kør). Hastighedsviseren viser fuld hastighed (streg).

A gu rø betyder at signal A vider gul over rød (stop) Krydset i hastighedsviseren ændrer det til SORF
A gu gr betyder at signal A viser gul over grøn (kør med nedsat hastighed). Pil ned i togvej 3 betyder 40 km/t. Pil op i togvej 13 betyder 70 km/t.

PU signal G1 og R1 viser forbikørsel tilladt (to lodrette lamper).
PU signal H1 viser forbikørsel forbudt (to vandrette lamper). Det er altså her toget skal stoppe og sikkerhedsveje ligger bag PU signal H1.
To skrå lamper betyder forsigtig forbikørsel tilladt.
Kør (ig) betyder "kør igennem" grøn lampe blinker.
Kør betyder at grøn lampe blinker
Stop betyder at rød lampe lyser
SORF betyder at rød lampe blinker.

For togvej 1 skal sporskifte 02a og 02b være i plus (dvs til kørsel af lige gren), sporskifte 05 skal være i plus (kørsel af lige gren) og sporskifte S1/S2 skal være låst.

For togvej 1 skal sporisolation A12, 01, 02 … være frie (sporrelæet skal være oppe).
05, 06 og K12 sikrer sikkerhedsvejen.
10 sikrer at der ikke er noget parkeret i spor 2 for tæt på sporskifte 05.

Og så kommer den er meget bred kolonne
For togvej 1

- PU signaler G1 og R1 skifter til to vandrette lamper (forbikørsel forbudt) 2 min efter at sporisolation 03 er blevet besat. Det der sker fordi togvej 1 opløses 2 min efter indkørsel til perron (se nedenfor). Derfor skal det blive hvor det er, indtil det får en udkørselstogvej.
- Indkørselssignal A skifter til stop, når sporisolation A12 er blevet besat. Toget er nu på vej forbi signalet. Vi skal have sat signalet på rødt inden togets bagene kører forbi signalet, så vi er sikker på at der kun kommer ét tog ind på stationen.
- Togvejs opløsning indledes når isolation 02 bliver besat og gennemføres når sporisolation 03 er besat og 02 er fri. Vi har konstateret er toget er ankommet og at det kører i den rigtig retning, så kan togvejen opløses.

- Sporskifte 05 frigives 2 min efter at isolation 03 bliver besat. Sporskifte 05 ligger i sikkerhedsvejen, så efter 2 min kan vi være sikre på at toget enten er standset eller rutchet. (Sporskifter har normalt SMUTO (sikring mod utidig omstilling), så hvis toget er rutchet og holder i sporskiftet, så vil besættelsen af isolation 05 overrule frigivelsen af sporskiftet)

Den sidste kolonne viser spærringer mellem (fjendtlige) togveje. En prik viser at sikringsanlægget ikke tillader at begge togeveje vælges.

- Prikken mellem togvej 1 og 2 forhindrer et meningsløst valg (spor 1 er garanteret frit og spor 1 er muligvis ikke frit).
- Prikken mellem togvej 3 og 13 forhindrer en frontal kollision i spor 2.
- Prikken mellem togvej 6 og 8 forhindrer en flankekollision i sporskifte 5.