Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Engineering
Department of Civil and Environmental Engineering

Marius Wold Albert

Investigation of complex accidents in the digitalised railway sector

A case study to investigate accidents involving the European Rail Traffic Management System (ERTMS)

Master's thesis in Road and Railway Engineering
Supervisor: Elias Kaasa and Mary Ann Lundteigen
May 2019

NTNU
Norwegian University of
Science and Technology

Marius Wold Albert

Investigation of complex accidents in the digitalised railway sector

A case study to investigate accidents involving the European Rail Traffic Management System (ERTMS)

Master's thesis in Road and Railway Engineering
Supervisor: Elias Kaasa and Mary Ann Lundteigen
May 2019

Norwegian University of Science and Technology
Faculty of Engineering
Department of Civil and Environmental Engineering

NTNU
Norwegian University of
Science and Technology

Preface

I have always been fascinated by accident investigation, and the quest to find out why accidents happen. In 2001 I finished my bachelor studies and started working as a consultant within the field of analysing accident and incident trends. Eight years later I got a job at the Accident Investigation Board Norway (AIBN), in the railway department. After nearly 10 years in the AIBN I am still intrigued by how accidents are able to find a way through good safety management systems, with all the best intentions.

In 2009 I attended my first educational training course at the Norwegian University of Science and Technology (NTNU). This was done at the Centre for Continuing Education and Professional Development, as a part time study for students in full-time employment. After seven completed courses in 2018, this thesis is the final step to obtaining a master degree. This has been a flexible part-time study that enabled me to combine family, work and study.

This study has been a great opportunity to get updated on the latest literature within accident investigation, and it has also slightly changed my view on how to investigate accidents. The work with the study has also created a better connection to the scientific university environment, and it is expected that this can be of mutual benefit for both the AIBN and NTNU. I believe the study also can be beneficial to other fellow investigators who are challenged by complex accidents.

I would like to thank my manager, Kurt A. Olsen, who has encouraged and supported me through the studies, and good colleagues at work for useful feedback and discussions. Thanks to my supervisors at NTNU, Professor Elisa Kassa and Mary Ann Lundteigen, for good follow-up and advice along the way. A special thanks to Terje Sivertsen at Bane NOR, his engagement and contributions has been beyond what is expected from a supervisor. Furthermore, I would like to thank everyone I have been in contact with at Bane NOR and the Rail Accident Investigation Branch (RAIB) for input, contributions and discussions.

Finally, a big thanks to my family, who patiently supported me during the studies.

Summary

The objective is to study how complex accidents involving the railway signalling system European Rail Traffic Management System (ERTMS) systematically can be analysed and investigated. The study addresses whether accident investigators may continue to use the established accident models, or do they need something new. The study is based on literature review, meetings and discussions with supervisors, AIBN colleagues, the Rail Accident Investigation Branch (RAIB), Bane NOR etc.

The literature in the thesis can roughly be divided in two parts, where the first part is general literature on the railway system and accident investigation methods. The second part is literature evaluating selected methods and the Systems-Theoretic Accident Model and Processes (STAMP) in particular.

The Accident Investigation Board Norway (AIBN) published the AIBN-method in 2017 which is a framework and analysis process for systematic investigations. In this thesis, the STAMP based CAST-method (Causal Analysis based on Systems Theory) is studied and compared to the AIBN-method, in order to evaluate the benefit of using CAST as a systemic approach within the AIBN framework. A case example from the RAIB interim report on the loss of temporary speed restriction on the Cambrian ERTMS line has been used to demonstrate the AIBN- and CAST-methods. In addition formal methods have been evaluated as a tool for software investigation.

The result of this study shows that the demonstrated methods can be used to investigate and analyse ERTMS accidents. The CAST-method adds value to the framework of the AIBN-method, and formal method is a possible tool for specialised investigation of software. For the control-structure part of the CAST-method the thesis has introduced more elements to visualise the actors and hazards to improve the graphical output. A flowchart and a series of questions is proposed for guidance in the use of formal methods during accident investigation.

It is recommended to include guidance material on the CAST-method and the formal method approach as possible tools in the framework of the AIBN-method.

Sammendrag

Målet er å undersøke hvordan komplekse ulykker som involverer jernbanesignalsystemet European Rail Traffic Management System (ERTMS) systematisk kan analyseres og undersøkes. Studien omhandler hvorvidt ulykkesundersøkere kan fortsette å bruke de etablerte ulykkesmodellene, eller om de trenger noe nytt. Studien er basert på litteratur gjennomgang, møter og diskusjoner med veiledere, SHT kolleger, Rail Accident Investigation Branch (RAIB) etc.

Litteraturen i avhandlingen kan grovt deles i to deler, hvor den første delen er generell litteratur om jernbanesystemet og ulykkesundersøkelsesmetoder. Den andre delen er litteratur som evaluerer utvalgte metoder og spesielt Systems-Theoretic Accident Model and Processes (STAMP).

Havarikommisjonen publiserte SHT-metoden i 2017, som er et sikkerhetsfaglig rammeverk og analyseprosess for systematiske undersøkelser. Den STAMP-baserte CAST-metoden (Causal Analysis based on Systems Theory) studeres og sammenlignes med SHT-metoden, for å vurdere fordelene ved å bruke CAST, som en systemisk tilnærming innenfor SHT-rammen. Et eksempel fra RAIBs midlertidige rapport om tap av midlertidige hastighetsrestriksjoner på en ERTMS strekning på Cambrian linjen i Storbritannia er brukt til å demonstrere SHT- og CAST-metodene. I tillegg har formelle metoder blitt vurdert som et verktøy for programvareundersøkelse.

Resultatet av denne studien viser at metodene kan brukes til å undersøke og analysere ulykker som involverer ERTMS. CAST-metoden forbedrer den systemiske beskrivelsen i SHT-metoden, og formelle metoder er et mulig verktøy for analyse av programvare. I utarbeidelsen av kontrollstrukturen i CAST-metoden har studien innført flere elementer for å visualisere aktører og sikkerhetsproblemer, og dermed forbedret den grafiske beskrivelsen. Et flytskjema med syv spørsmål er foreslått som veiledning i bruken av formelle metoder ved ulykkesundersøkelse.

Det anbefales å inkludere veiledningsmateriale om CAST-metoden og veiledningen for bruk av formelle metoder som mulige verktøy innenfor rammen av SHT-metoden.

Table of Content

List of figures

Abbreviations

Abbreviation	Explanation
AIBN	Accident Investigation Board Norway
ATC	Automatic Train Control
ATO	Automatic Train Operation
ATP	Automatic Train Protection
CAST	Causal Analysis based on Systems Theory
COR	Common Occurrence Reporting
DMI	Driver Machine Interface
DOE	Department of Energy
DoT	Department of Transport
ERA	European Union Agency for Railways
ERAIL	European Railway Accident Information Links
ERTMS	European Rail Traffic Management System
ESReDA	European Safety, Reliability & Data Association
ETCS	European Train Control System
EU	European Union
EU	Den europeiske union
FRAM	Functional Resonance Analysis Method
GEST	GEstion des Signalisations Temporaires
GSM-R	Global System for Mobile Communications – Railways
HFACS	Human Factors Analysis And Classification System
IoT	Internet of Things
ISA	Independent Safety Assessor
JSSSH	Joint Software Systems Safety Handbook
LGVEE	Ligne à Grande Vitesse Est européenne
MA	Movement Authority
MIT	Massachusetts Institute of Technology
NIB	National Investigation Bodies
OBU	On board Unit

ORR	Office of Road and Rail
PSASS	Partnership for Systems Approaches to Safety and Security
PSR	Permanent Speed Restrictions
RAIB	Rail Accident Investigation Branch
RAMS	Reliability, Availability, Maintainability and Safety
RBC	Radio Block Center
ROSS	Risiko- og sårbarhetsstudier (Reliability and Safety Studies)
RSD	Railway Safety Directive
SD	Samferdselsdepartementet
SERA	Single European Railway Area
SIL	Safety Integrity Level
SKI	Swedish Nuclear Power Inspectorate
SNCF	Société nationale des chemins de fer français
SRS	System Requirement Specification
STAMP	Systems-Theoretic Accident Model and Processes
STPA	Systems-Theoretic Process Analysis
TMS	Traffic Management System
TSI	Technical specifications for interoperability
TSR	Temporary Speed Restrictions
WON	Weekly Operating Notice

1 Introduction and problem

This chapter presents the background for the study, the problem set out to study, the objective of the study, and an outline of how the text is structured.

1.1 Background for the study

I have worked almost 10 year’s investigating rail accidents, and 8 years previously in the field of collecting and analysing accidents and incidents. Especially one investigation made me realise how challenging and complex a railway signalling system can be [1]. After the investigation I felt the need to learn more in order to be better prepared if a similar investigation should be conducted. Complex accidents has also been a discussion in some of the network meetings where national accidents investigation bodies are sharing experience. Other countries, especially those who have started to implement European rail traffic management system (ERTMS), do see the need for more information and some guidance on how an accident where ERTMS is involved could be investigated.

The rail sector is part of a comprehensive digitisation process, including technology being moved out of the track and into the trains. The goal is more standardisation and opportunities to cross borders across Europe. The introduction of the new digital signalling system ERTMS is one of the largest digitalisation projects in Norway, and the national infrastructure manager will invest more than NOK 20 billion over the next ten years [2]. Digitalisation technology is also utilised to prevent accidents, make maintenance smarter, and improve information for both travellers and train companies. The technology entails new opportunities for "Internet of things", sensors, "big data" and machine learning. Recorders on board, call recordings and logs from traffic management systems have for a long time been the main source of digital information in accident investigations. Over the last few years, there have been more digital information available, such as the assembly of a number of surveillance cameras and more detailed diagnostic data on trains and locomotives.

Digitalisation brings about major changes in the rail sector on technical equipment and operational tasks. This implies more use of software and means that the railway becomes more complex and high-tech. These changes challenge old methods of accident investigation and risk models, and there are research claims that new approaches are needed [3] [4] [5]. In this thesis the main focus is on how a complex system such as ERTMS can be analysed during an accident investigation process.

1.2 Objective

The objective is to study how complex accidents involving the railway signalling system European Rail Traffic Management System (ERTMS) systematically can be analysed and investigated. The study addresses whether accident investigators may continue to use the established accident models, or if they need something new.

Accident investigation within the railway domain is well established in Europe in accordance with the Railway Safety Directive 2004/49 [6]. The railway sector is challenged to adapt to new technology and changing demands for organisational structure and efficiency. This generates more complex accidents and is challenging the national investigation boards. The introduction of the ERTMS system is one of the largest projects in the European railway sector, and many safety critical tasks are controlled by software.

1.3 Problem formulation

The first part of the objective is to study ERTMS in the context of accident investigation, and complex systems. Because software is an important part of the ERTMS system, formal methods has been suggested as a possible specialised software investigation tool. This thesis uses the framework of the Accident Investigation Board Norway (AIBN) method as an established accident model, and possible improvements to the AIBN-method is studied.

The research questions to answer has been formulated in the following way:

How will the introduction of ERTMS affect the way accidents are investigated?
The introduction of ERTMS means that software will play an important role in the future investigation of rail accidents. Previous installations and operations are replaced by computer systems that can perform the tasks more effectively and at a lower cost. Going from a national signalling system with limited area of use to a European system gives an opportunity to share

experience on a larger scale. This might also make it harder to investigate when the product might be developed in a different country, and there might be challenges such as language and business secrets. The investigation must establish whether the software had a vital role in the accident or not. One issue is to investigate if the software behaved as expected, and how to narrow down the scope to the relevant part of the software. Stating it is a software error will not give a good learning experience, and is not an accepted result for improving safety. Another important issue is to investigate if current methods for accidents investigation are capable of handling the complexity of the ERTMS signalling system.

Is investigation of ERTMS any different from any other investigation involving a complex system controlled by software?

Software is used to control complex operations in order to provide safe routes for the trains. Computer based signalling systems have been around for decades, and is not completely new to the railway sector. The large scale of the ERTMS system increases the complexity of the system and introduces more actors and systems to relate and comply to. It is a challenge to identify the potential failure modes and predict their possible consequences in a in a complex system involving software. Software by itself poses no danger, but within the system the software is operating it can create a potential for hazards [7]. It is therefore important to consider software safety as a part of the system safety process and use a systematic approach when investigating accidents.

To what extent can formal methods be used as a tool in reviewing ERTMS events?

The CENELEC standards are an important set of requirements for the development of ERTMS, and they highly recommend the use of formal methods. Formal methods were established in the 1980s to analyse the functions of software. This is normally used in software safety demonstrations, and generally involves formulating specifications, designs or program code in a formal, mathematical notation. Then, verification is carried out through formal, logical reasoning about statements formulated in this notation. These statements will typically express expected safety features of the analysed system. Formal methods can also be used to specify functional requirements to detect ambiguities, lack of completeness, and internal contradictions in the specification. In addition to evaluating the utility of such methods in ERTMS investigations, it must also be considered how extensive this type of analysis is and what competence is needed to perform it.

How can the AIBN-method be further developed to provide better support for the investigation of complex railway accidents?

The AIBN-method is the Norwegian Accident Investigation Board's framework and analysis process for investigating accidents. The method can be compared to a toolbox where the investigators are guided on how to perform the investigation and what methods (tools) are recommended to use. The method do however not give a comprehensive guidance and tool suggestion for complex investigations and how to investigate software. This thesis seeks to find methods and guidance to how complex railway investigations and software may be improved in the AIBN-method.

1.4 Scope of work

This master thesis studies how a complex accident involving the railway signalling system ERTMS systematically can be investigated by using established methods for accident investigation. The AIBN-method is the Norwegian Accident Investigation Boards framework for how accident investigation shall be carried out. The AIBN-method do not give a comprehensive and detailed guidance on how to investigate complex accidents, and refers to systemic methods as a possible method. In order to test and demonstrate a possible systemic method to include in the AIBN-method, the STAMP theory and CAST-method is selected. A demonstration of a real case example involving ERTMS is applied to the AIBN-method and the CAST-method. The two methods will be compared and an evaluation of the introduction of the CAST-method to the AIBN-method will be done. In addition formal methods used as a special investigation tool for ERTMS software is also studied. This is done in order to evaluate the possible application of its use in accident investigation, where it must be demonstrated whether the software contains errors or not.

1.5 Outline of the report

The IMRaD structure is the basis for the outline of the thesis, and corresponds to the report in the following way:

- **I**ntroduction – chapter 1-2
- **M**aterial and method – chapter 3-4
- **R**esults – chapter 5

- **a**nd
- **D**iscussion – chapter 6

The introduction is presenting the problem, and the research questions set out to study. European railway signalling systems and associated regulations are briefly explained, with focus on accident investigation and relevant literature on the field.

In the material and method chapter the use of formal methods as a specialised method for software investigation is studied, and a flow chart for investigating software is proposed. The AIBN-method and the CAST-method is explained, and is the theoretical foundation for the application of the methods in the following chapter.

Chapter 5 is demonstrating how the case example can be investigated by using the AIBN-method and the CAST-method. The case example is analysed through the proposed steps of each method.

The discussion chapter revisits the research questions and explains and interprets the results of the study. The differences in the methods demonstrated in chapter 5 is discussed and compared, and also how other studies relates to the findings in this study. Finally the relevance of the study and future research is discussed before the conclusion is given.

1.6 Limitations

This study is conducted as part of the Professional Master's program in Road and Railways at the department of Civil and Environmental Engineering at NTNU, and the theme is investigation of complex railway accidents. The subject has an overlap with the RAMS group at NTNU, and for that reason, one more supervisor was provided from the RAMS group.

This study compares two types of methods for accident investigation, the AIBN-method and CAST. I have known and used the AIBN-method since 2016, while the CAST method is new to me. The AIBN-method is developed at my workplace, and this can make parts of the study subjective. Another issue that was detected during the thesis work is that working with one method also affected the information input on the other method. For example the sequence of events in the AIBN-method could be used in the CAST-method, and systemic findings from the CAST-method could be used in the AIBN-method. This may have affected the methods to have a better result than if the study had been performed separately by different persons in isolation. This is not necessarily a problem, as it may also demonstrate that using both methods can give a better result.

This study also aims to find a suitable approach on how software can be investigated in the railway signalling domain. One of the main purposes with the thesis is to guide investigators on how to approach software in an investigation. For an accident investigator with a background within software engineering, this thesis might be perceived as a bit simple regarding formal methods and software investigation.

The case study in this thesis was an active investigation by the RAIB. The case was selected because it was the first official investigation of an ERTMS signalling system by a national investigation body. This has made it challenging to retrieve information for the case example and discuss the content with supervisors, because the final report from the RAIB had not been published at the time the thesis was written. For elements that has been analysed to demonstrate the use of the method, it should be noted that I have made some small assumptions. These assumptions may not be correct. Therefor it is important to stress that the official investigation result is presented by the RAIB in their final report, and may not be in line with the results of this thesis.

Even though I am working as an accident investigator in the Accident Investigation Board Norway, this thesis has not had access to all the resources a full investigation has. Normally an investigation by AIBN will be a project where several investigators work together, and the involvement by external experts will be used in a larger extent. The outcome of an official AIBN investigation will be expected to go into more details than the output in the analysis of this thesis.

2 The European railway system

This chapter gives a short description of the European railway system, signalling systems including ERTMS and relevant regulation and standards.

The European railway is a fragmented transport network where each country historically has built the railway according to its own proprietary solutions [8]. This originates from the wars in the 1800s when the railway was developed, and interoperability was not an issue. Interoperability is defined as the ability of making systems and organisations work together (inter-operate). This has made it difficult to cross borders, and the railway has a disadvantage compared to automotive, aviation and marine transport. To be able to run a train it must fit the track gauge, and be able to communicate with the signalling system and train dispatchers. Most modern trains run on electricity and also need to be compatible with the power system. The standard track gauge for high-speed railway is 1435 mm and used by most member states, with the exception of Finland. There are several different power system in Europe, and more than twenty different types of signalling systems that complicates the interoperability on the European railway.

The introduction of The European Union Agency for Railways (ERA) in 2004 was a means to harmonise the railway. ERA has developed the Technical Specifications for Interoperability (TSIs) in order to define technical and operational standards in Europe. This thesis has a special focus on the single European signalling and control system, called European Rail Traffic Management System (ERTMS).

2.1 Railway signalling system

The main purpose of a signalling system is to keep the trains safe and not come in conflict with other trains on the track or vehicles at level crossings. The first signalling systems in the late 1830s in England consisted of manual hand signals, and further developed to semaphores and signalling posts. The later development of the signalling system consisted of Automatic train protection (ATP), Automatic train control (ATC) and Automatic Train Operation (ATO). These systems can intervene if the train driver fails to apply the brakes, or exceed the speed limit. The ATO system is capable of fully automate train operations, and can operate without a human driver input. In Europe most railways are running on older signalling systems with some form of ATP or ATC. The development of these railway signalling systems has historically been done in each country, and the systems are not compatible with each other.

2.1.1 European Rail Traffic Management System (ERTMS)

The European Rail Traffic Management System (ERTMS) is a major industrial program with the aim to gradually replace and harmonise the different national signalling systems in Europe. The background and the ERTMS system is described in the next chapters.

2.1.1.1 History

In 1989, the EU launched a study of the signalling issues in Europe, and in 1993 the EU issued the Interoperability Directive to define the Technical Interoperability Specifications (TSI) [8]. A decision to make ERTMS a key part of rail interoperability in Europe was made in 1996, and became the standard of all high-speed lines. In 1998 the main European signalling companies created the UNISIG to help develop the system specification. The first ERTMS specification was issued in 2000, and contained requirements for an interoperable railway control, command and signalling system in Europe. In 2004 the European Railway Agency (ERA) was established and given the ERTMS system authority to manage the specifications.

In 2005 the problematic connection and integration of the European rail network was expressed in the following way in a communication between the Commission of the European Communities to the European Parliament and the Council [9]:

> *"Technical barriers to trade and to interoperability – the ability of trains to run on any section of the network – are continuing to hamstring competitiveness in the railway industry.*
>
> *Today, for example, there are more than twenty signalling and speed control systems operating at the same time in Europe. The Thalys, linking Paris and Brussels in particular, has to be equipped with seven different signalling and speed control systems, entailing extra cost and increased breakdown risk and rendering drivers' jobs more complicated as they have to familiarise themselves with each system. These technical barriers are hampering the development of rail transport at the European level, while road transport is free to develop without such barriers."*

The communication stated that the long service life of signalling systems is an obstacle to a rapid deployment of ETSC, and with a renewal rate of 2.5% per year the majority of locomotives built in 2025 will still be fitted with national systems. The communication also points to financial resources as an important motivation to speed up the deployment of ERTMS for the first infrastructure managers and railway undertakings. To facilitate the deployment of ERTMS the European coordinator was appointed to ease the implementation and pinpoint problems to be solved. In 2014 the European ERTMS coordinator issued a breakthrough program [10] to boost the implementation of ERTMS in Europe. The history of ERTMS until 2016 is shown in figure 1.

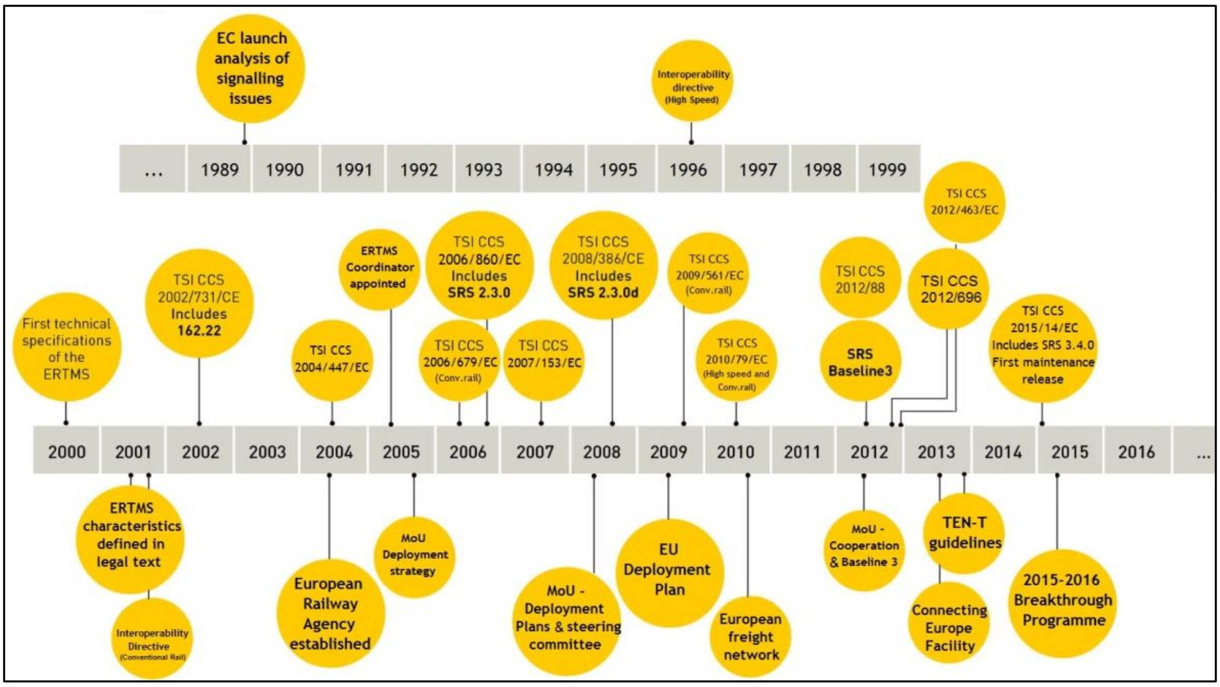

EC launch analysis of signalling issues
Interoperability directive (High Speed)
...
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
TSI CCS 2012/463/EC
ERTMS Coordinator appointed
TSI CCS 2006/860/EC Includes SRS 2.3.0
TSI CCS 2008/386/CE Includes SRS 2.3.0d
TSI CCS 2009/561/EC (Conv.rail)
TSI CCS 2012/88
TSI CCS 2012/696
TSI CCS 2002/731/CE Includes 162.22
First technical specifications of the ERTMS
TSI CCS 2004/447/EC
TSI CCS 2006/679/EC (Conv.rail)
TSI CCS 2007/153/EC
TSI CCS 2010/79/EC (High speed and Conv.rail)
SRS Baseline3
TSI CCS 2015/14/EC Includes SRS 3.4.0 First maintenance release
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
...
ERTMS characteristics defined in legal text
Interoperability Directive (Conventional Rail)
European Railway Agency established
MoU Deployment strategy
MoU - Deployment Plans & steering committee
EU Deployment Plan
European freight network
MoU - Cooperation & Baseline 3
TEN-T guidelines
Connecting Europe Facility
2015-2016 Breakthrough Programme

Figure 1: History of ERTMS. Source: European Commission.

Although significant results had been achieved the last 10 years, and ERTMS is the accepted system by all member states, the implementation was slower than expected. The main argument for not implementing ERTMS was the high cost, lack of expertise and delay of specifications. Some states also argued their existing signalling system had not reached the end of its life cycle due to investments in maintenance and updates.

By 2017 a major step was achieved by the release of ERTMS Baseline 3 set of specification, and the UNISIG members renewed signed commitment to follow the adoption of Baseline 3 for a swift and stable deployment of ERTMS. The EU Commission published the ERTMS Deployment Action Plan in 2017 [11], which will be followed up by the ERTMS Stakeholder Platform Coordination Subgroup. The Member States were also asked to draw up national implementation plans [12], and update them at least every 5 years.

The status of ERTMS is expressed in the ERTMS Deployment Action Plan [11]:

> *At the end of 2017 almost 4.500 kilometres of Core Network Corridors lines will be operational with ERTMS and almost 7.000 vehicles are equipped or contracted today with ETCS in the EU, a substantial part of which has been supported by EU funding. Nearly the totality of the Italian and Spanish high-speed networks are supervised and protected by ERTMS; so are significant parts of the Swiss, Dutch and Belgian networks. Trains operate in commercial service at 320 km/h with ETCS. ETCS controls freight trains on conventional lines, and on dedicated routes (e.g. Betuwe line). The longest alpine tunnel is operated exclusively with ERTMS. The system is in service in suburban lines with commuter traffic (e.g. Madrid).*

The deployment plan has set a high goal and it expects that by 2030 almost 51.000 kilometres of railway lines in Europe will have ERTMS, and figure 2 show the target for ERTMS deployment,

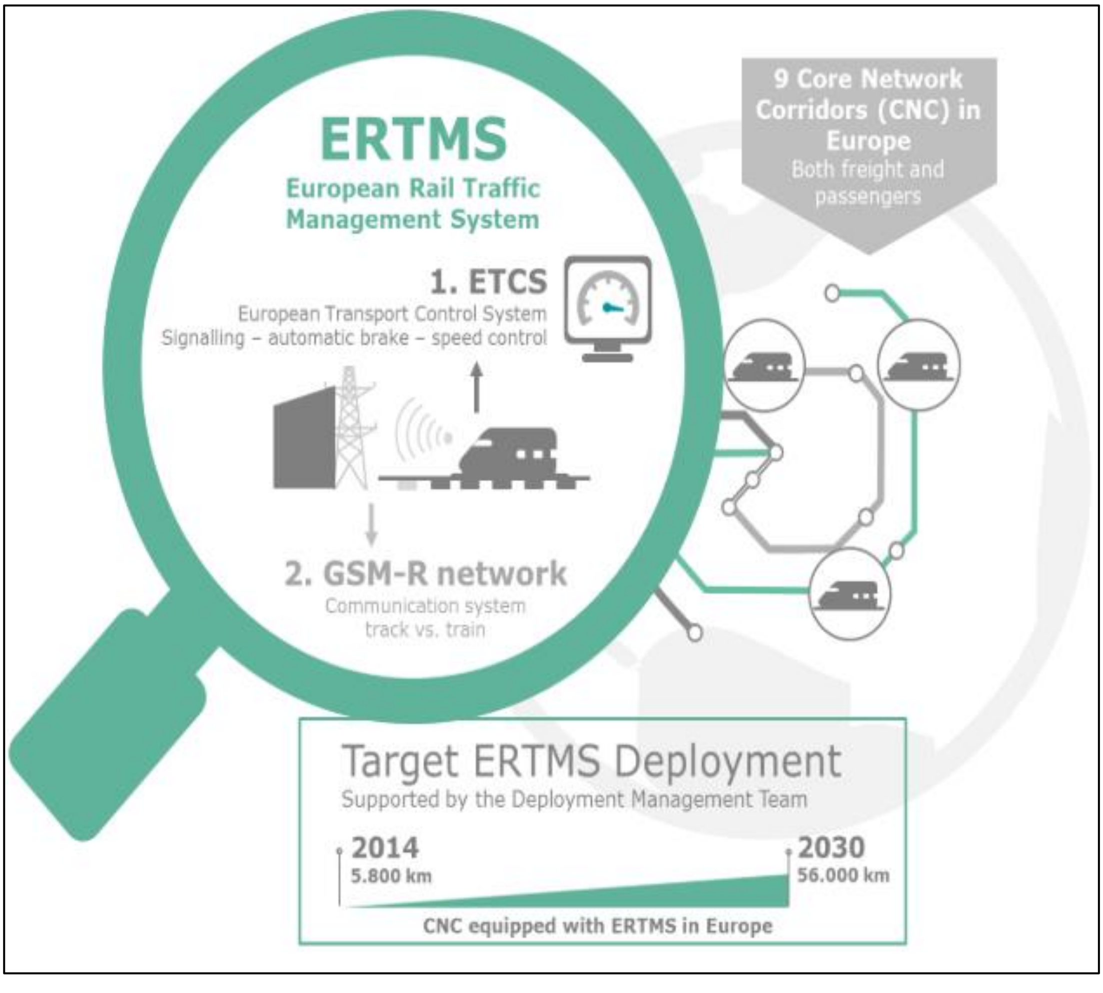

ERTMS
European Rail Traffic Management System
1. ETCS
European Transport Control System
Signalling – automatic brake – speed control
2. GSM-R network
Communication system
track vs. train
9 Core Network Corridors (CNC) in Europe
Both freight and passengers
Target ERTMS Deployment
Supported by the Deployment Management Team
2014
5.800 km
2030
56.000 km
CNC equipped with ERTMS in Europe

Figure 2: ERTMS deployment target. Source: European Commission.

2.1.1.2 The ERTMS system

ERTMS consist mainly of two systems, European Train Control System (ETCS) and Global System for Mobile Communications – Railways (GSM-R) [13]. ETCS is supervising train movements and continuously monitoring the driver, and if necessary the emergency brakes will be activated. The GSM-R is the European radio communication standard for railway operations. GSM-R is based on the GSM radio technology and uses exclusive frequency bands to communicate between the train and traffic control centres. Figure 3 shows the main components in the ERTMS level 2 which is selected for the Norwegian railway.

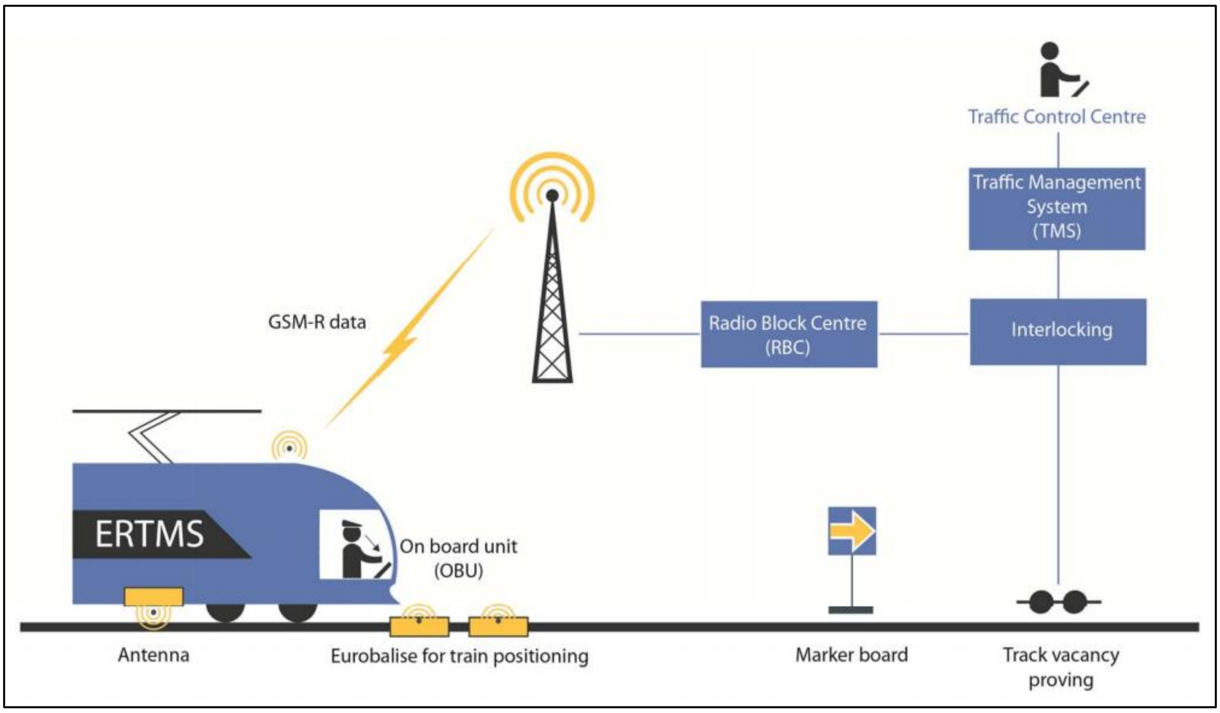


Figure 3: ERTMS level 2 is selected for the Norwegian railway. Source: Bane NOR.

The main components in the ERTMS system are:

- GSM-R, the European radio communication standard for railway operations
- Radio Block Center (RBC), the infrastructure part of the ETCS. Centralised computer that receives train positions and sends movement authorities based on information from the interlocking.
- Interlocking makes sure the trains can move safe and that incompatible train routes are not simultaneously established. The interlocking is not a part of ERTMS components, but necessary in almost all ERTMS structures.

- On board Unit (OBU), the train part of the ETCS. There are several onboard components to make sure the train operates safely, and providing the driver with information and control functions.
- Eurobalise is a device on the track that sends the train information about position, speed limits, gradients, etc.
- Train Management System (TMS), software solution for train traffic management.
- Traffic control center, monitor and control train traffic and handling of unforeseen events.

ERTMS has different modes for managing the different situations of the trackside and in-cab equipment [14].

- Level 1 is a continuous supervision of train movement, but does not have a continuous communication between the train and trackside (figure 4). Lineside signals and train detection equipment are required to substitute the missing communication, and is outside the scope of ERTMS.

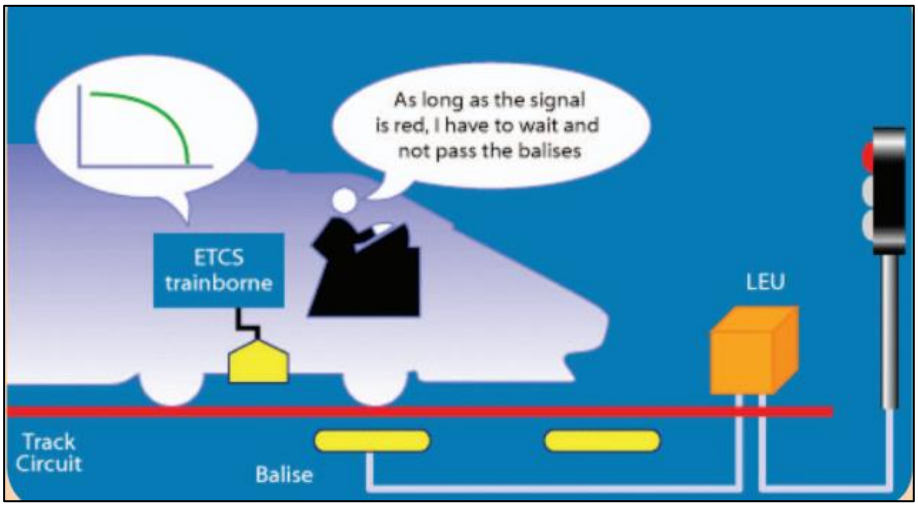

As long as the signal is red, I have to wait and not pass the balises
ETCS trainborne
LEU
Track Circuit
Balise

Figure 4: ERTMS Level 1: Source: ERTMS.net.

- Level 2 is both continuous supervision of train movement and continuous communication between the train and trackside (figure 5). Lineside signals are optional, and train detection is done by equipment outside the scope of ERTMS.

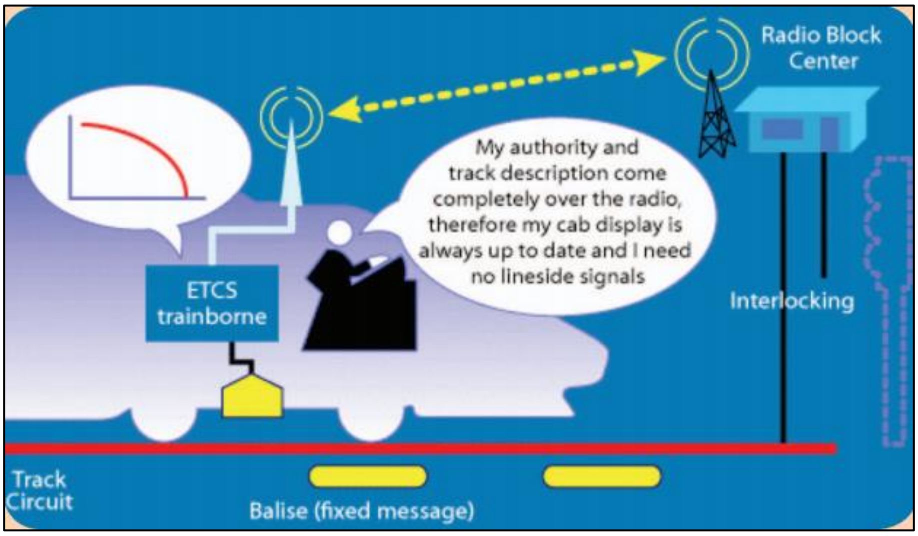

Radio Block Center
My authority and track description come completely over the radio, therefore my cab display is always up to date and I need no lineside signals
ETCS trainborne
Interlocking
Track Circuit
Balise (fixed message)

Figure 5: ERTMS Level 2: Source: ERTMS.net.

- Level 3 introduces a "moving block" technology (Figure 6). This technology will increase the capacity as it adapts to the braking performance of the train. The fixed block system has to take into account the train with the worst braking performance, and creates an unnecessary large block for trains with effective brakes. This is the main ERTMS mode which do not require lineside signals, the train location and integrity is managed within the scope of ERTMS requirements. The integrity of the train, i.e. the control of all wagons being connected and not accidentally split, is supervised by the train.

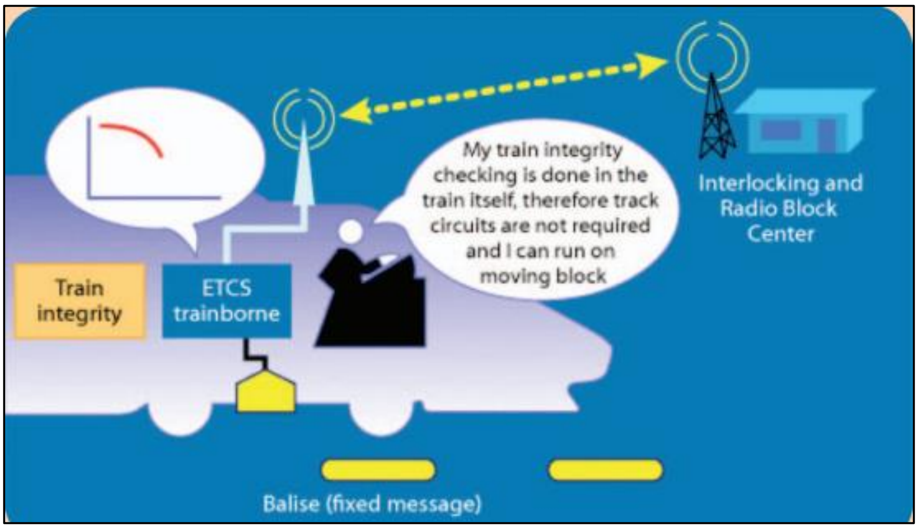

My train integrity checking is done in the train itself, therefore track circuits are not required and I can run on moving block
Interlocking and Radio Block Center
Train integrity
ETCS trainborne
Balise (fixed message)

Figure 6: ERTMS Level 3: Source: ERTMS.net.

- There are also other levels for specific situations such as train equipped with ETCS running on non-equip lines, called Level 0. For trains equipped with ETCS running on lines with class B systems there is a STM level, where the ETCS acts as an interface between the driver and the national system.

2.2 Regulations and specifications

One issue that need to be established during the investigation of a system, is to find out what regulations and specifications the system should comply with. In this thesis the focus is on ERTMS, and the requirements for computer based signalling systems is described. This process will be similar if the investigation is handling a different domain than rail signalling.

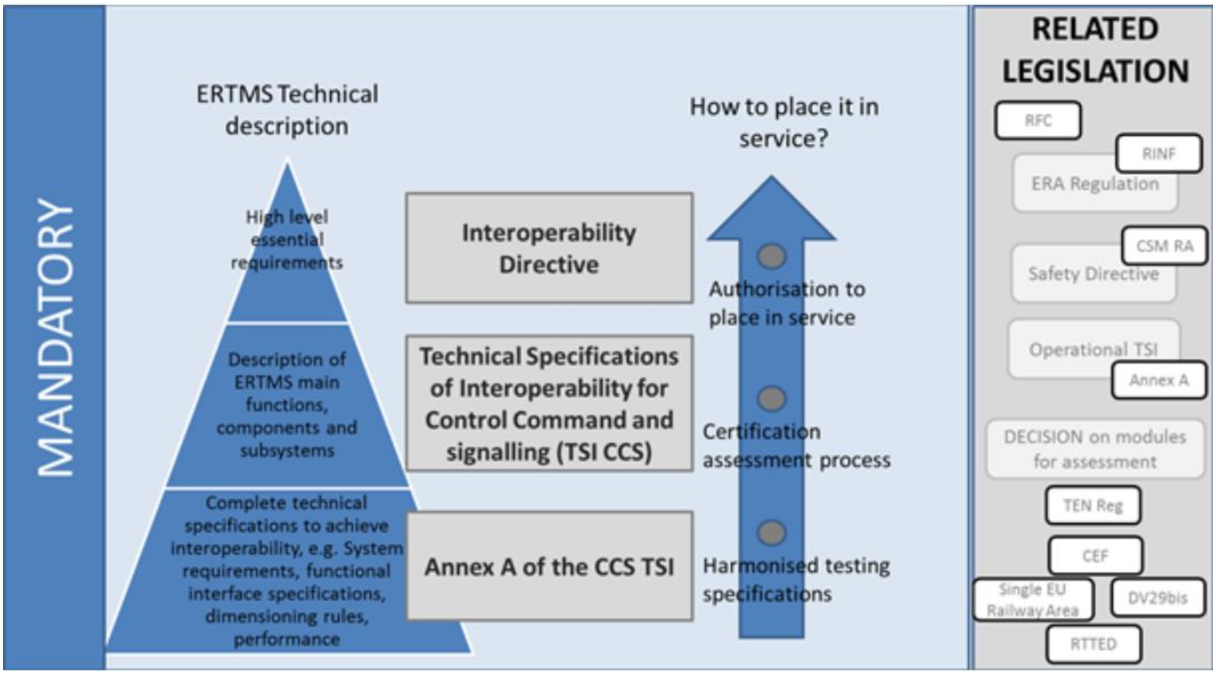

MANDATORY
ERTMS Technical description
High level essential requirements
Description of ERTMS main functions, components and subsystems
Complete technical specifications to achieve interoperability, e.g. System requirements, functional interface specifications, dimensioning rules, performance
Interoperability Directive
Technical Specifications of Interoperability for Control Command and signalling (TSI CCS)
Annex A of the CCS TSI
How to place it in service?
Authorisation to place in service
Certification assessment process
Harmonised testing specifications
RELATED LEGISLATION
RFC
RINF
ERA Regulation
CSM RA
Safety Directive
Operational TSI
Annex A
DECISION on modules for assessment
TEN Reg
CEF
Single EU Railway Area
DV29bis
RTTED

Figure 7: legislation directly related to ERTMS. Source: European Commission.

Figure 7 show the European legislation [15] mandatory and related to ERTMS, where the interoperability directive is at the high level and the annex of TSI (Technical Specifications for Interoperability) is at a more detailed level. In order to know what legislation is relevant it is important that the description of the accident gives enough information to look for the corresponding requirement. One finding could also be that there are no requirements for the problem in the accident.

The Interoperability Directive (2008/57/EC) [16] contains high level requirements for conditions such as design, construction, upgrading etc. to be met in order to be interoperable within the European rail system. The main goal for the directive is to make sure TSI's are applied across Europe, and establishing a common verification and validation process for infrastructure and rolling stock. There is also focus on putting interoperability constituents onto the marked in order to harmonise rail components. The procedure for putting ERTMS systems into service has been further explained in the EEC recommendation 2014/897/EC [17].

Technical Specifications for Interoperability specifies the legal basis and the definition of the essential operational and technical requirements for a subsystem to be interoperable. Each functional or structural subsystem forming the railway system in Europe is defined in the Directive 2016/797 [18]. For each subsystem or part of subsystem there need to be specific technical specifications that define the constituents and interfaces for compatibility and accessibility. The Technical Specifications of Interoperability for Control Command and Signalling (TSI CCS) Commission Regulation (EU) 2016/919 [19] contains the overall description of ERTMS functions, components and subsystems. Annex A of the TSI CCS contains list of technical specifications for ERTMS interfaces, dimensioning rules and performance. Each technical specifications is called SUBSET, and given a number. The main subset for all the detailed specifications for ERTMS is called SUBSET-026 and is the System Requirement Specification (SRS).

2.2.1 Standards

TSIs may make references to European standards or specifications, and that will make the reference mandatory. The only officially recognised standards by the European Commission are developed by European Standards Organisations (ESOs) [20]. The ESOs consists of the European Committee for Electrotechnical Standardisation (CENELEC), its sister organisations the European Committee for Standardisation (CEN) and the European Telecommunications Standards Institute (ETSI). ESOs are a regional body of the international counterparts such as IEC (the International Electrotechnical Commission), ISO (the International Organisation for Standardisation) and ITU-T (the International Telecommunication Union, telecommunication standardisation sector).

The mandatory standards for ERTMS are known as EN50126 [21], EN50128 [22] and EN50129 [23]. These standards are based on the IEC 61508 standard for functional safety of electrical/electronic/programmable electronic (E/E/PE) safety related systems.

EN50126 is an overall standard that describes how the Reliability, Availability, Maintainability and Safety (RAMS) process should be performed. This standard applies to all railway systems and describes the steps that must be followed follow from start to end of service. The product life cycle is represented in the shape of the letter “V”, and figure 8 show the different life cycle phases.

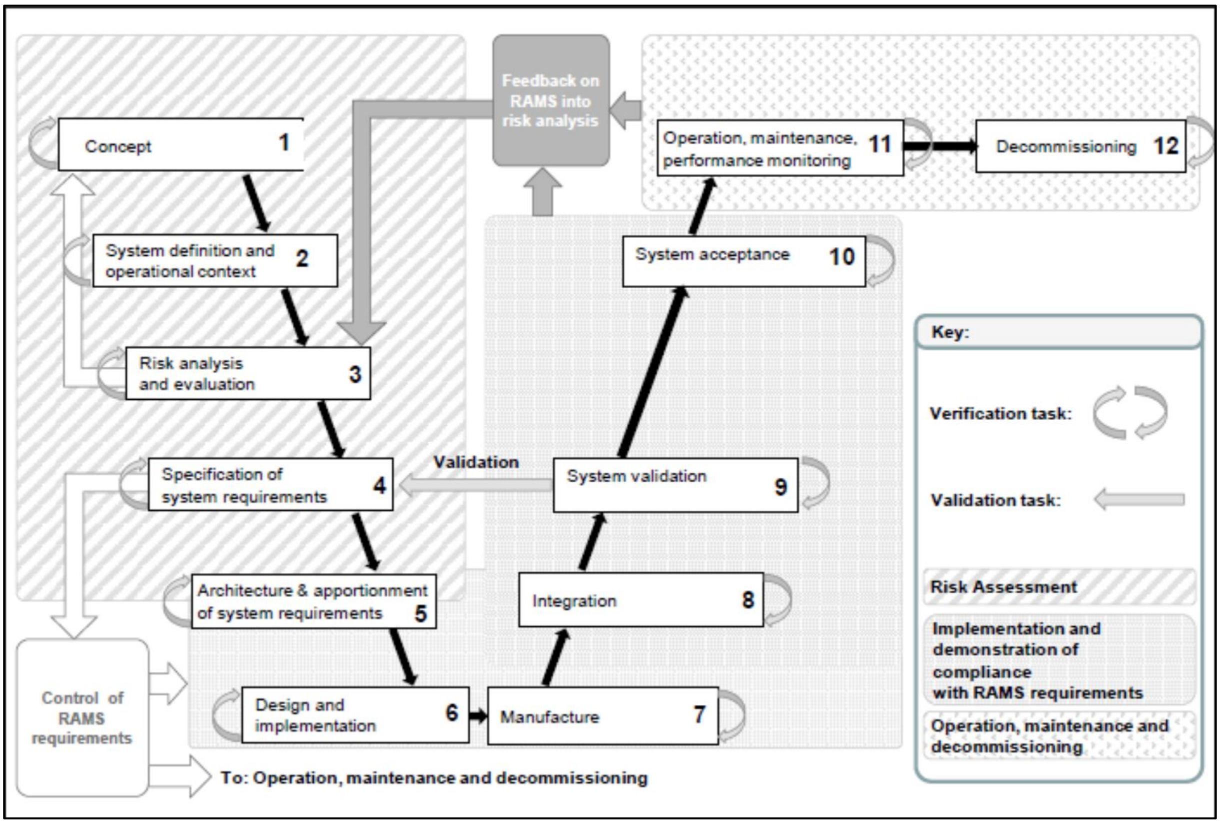

Feedback on RAMS into risk analysis
Concept 1
System definition and operational context 2
Risk analysis and evaluation 3
Specification of system requirements 4
Architecture & apportionment of system requirements 5
Design and implementation 6
Manufacture 7
Integration 8
System validation 9
System acceptance 10
Operation, maintenance, performance monitoring 11
Decommissioning 12
Validation
Control of RAMS requirements
To: Operation, maintenance and decommissioning
Key:
Verification task:
Validation task:
Risk Assessment
Implementation and demonstration of compliance with RAMS requirements
Operation, maintenance and decommissioning

Figure 8: The V-cycle representation. Source EN 50126.

EN50128 describes the process and technical requirement for software in a railway control signalling system. The standard focus on safety implications and interactions between different systems. This is a relevant standard when an ERTMS software system is under investigation, and the functional steps in figure 9 are similar to the proposed investigation technique suggested later in the thesis (figure 28).

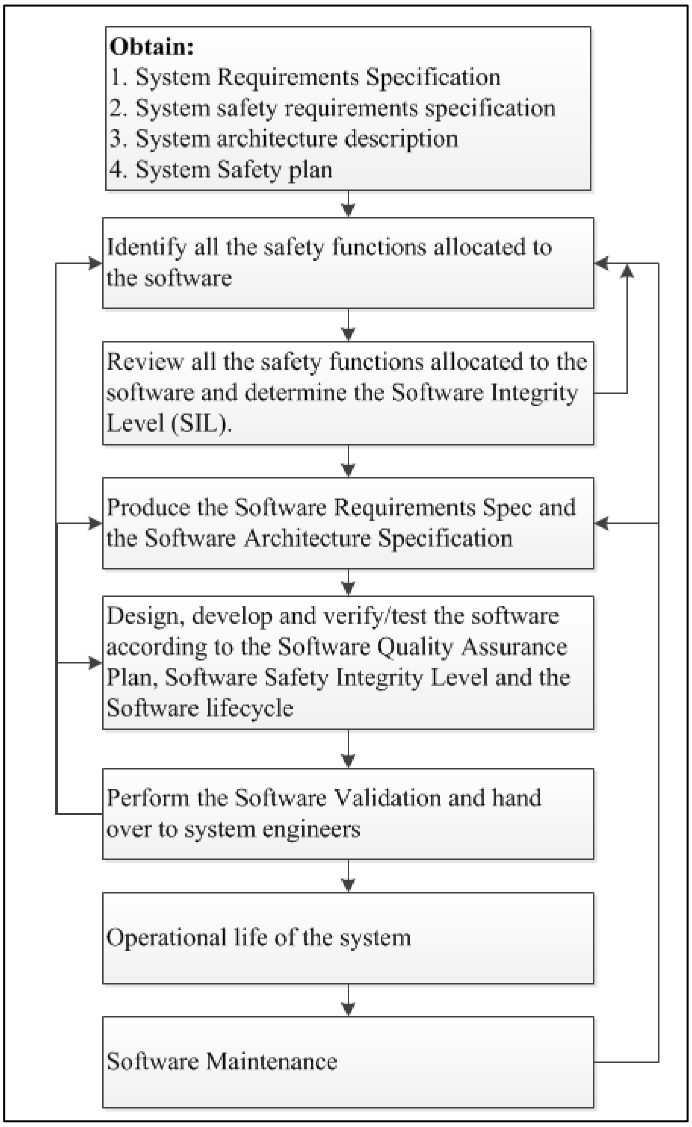

Obtain:
1. System Requirements Specification
2. System safety requirements specification
3. System architecture description
4. System Safety plan
Identify all the safety functions allocated to the software
Review all the safety functions allocated to the software and determine the Software Integrity Level (SIL).
Produce the Software Requirements Spec and the Software Architecture Specification
Design, develop and verify/test the software according to the Software Quality Assurance Plan, Software Safety Integrity Level and the Software lifecycle
Perform the Software Validation and hand over to system engineers
Operational life of the system
Software Maintenance

Figure 9: Functional steps in the application of EN 50128. Source: EN 50128.

EN50129 describes the overall lifecycle requirement of signalling systems, subsystems and equipment.

2.3 Railway accidents in Europe

The European Union Agency for Railways (ERA) collects, analyses and publishes railway safety information for the member states. ERA was set up in 2004 and is governed by European Public law. ERA's mandate is to create a Single European Railway Area (SERA). ERA is based in France and is working towards making trains safer, and able to easier cross national borders. The main activities are creating a harmonised approach to safety, removing technical barriers, and promoting simplified access to the European rail sector. The Railway Safety Directive

(RSD) was brought into force in 2004 and is a regulatory framework for railway safety. Member states are required to report safety indicators in accordance with the definitions in the RSD.

The 2018 Report on Railway Safety and Interoperability in the EU by the European Union Agency for Railways is a publication of safety indicators [24]. The report contains safety information from 30 countries, 28 EU member states and two Schengen countries. On average over the period 2012-2016 there has been around 1950 significant railway accidents each year. These accidents have on average resulted in 1050 fatalities and 850 serious injuries each year. The number of accidents, fatalities and serious injuries are decreasing over time, and is an indication of the increased safety. This result must also been seen in light of increased traffic, and more activity than in the previous years.

Since 2006 an average of 195 accidents and incidents per year have been investigated by National Investigation Bodies (NIB) in line with the requirement of the RSD. Unlike the decrease of accidents over time, the number of investigations varies each year. The report states it is necessary with further research to reveal what the variations are related to. The unpredictable nature of accidents, size of the investigation and available resources of the NIB’s should be relevant factors in the variations.

Comparing Europe to the worldwide railway safety and other transport modes show that railway safety is among the safest transport forms in Europe. Airline transport is ranked as the safest public transport mode, while Bus and Maritime transport has a higher risk of fatality. Comparing the risk of fatality of public transport and personal car transport, the risk of car transport is 10-20 times higher.

2.4 Accident investigation body

The Railway Safety Directive [6] chapter *V* and annex *V* contains the general requirements for safety investigation of railway accidents and incidents in Europe. The main goal is to prevent new accidents and further improve the safety. The investigations shall be performed by an independent National Investigation Body (NIB), to minimise the conflict of interest. The main steps and principals for conducting an investigation is stated in the RSD, and related guidance material. These principals and guidance material is at a high-level, and do not provide the necessary details that are set out to study in this thesis.

The maturity and size of the investigation bodies in Europe varies, and the approach and method to accident investigation are different. ERA has formed a network for the NIB's to share information and common practices. One important focus area is developing common investigation methods and adapt to the development of technical and scientific progress.

NIBs are obliged to send information to ERA one week after the decision to open an investigation, and a copy of the final report. The information is registered in the database European Rail Accident Information Links [25]. In addition the NIBs must send in an annual report regarding the investigations carried out and safety recommendations.

3 Material

In this chapter it is explained how the research and thesis was conducted, and material on research and literature on accident investigation and experiences.

3.1 Research approach

The process of writing the master thesis is visualised in figure 10. A prestudy report was prepared before the master thesis project, with the aim to develop the research questions to be answered [26]. It is perceived as very useful to have carried out the prestudy before the master's thesis, as several issues and clarifications was already done and the start-up went easier. The aim has been to find possible methods to help the investigation of complex railway accidents. The introduction of the European railway signalling system ERTMS allows a larger user group to benefit from guidance on the theme.

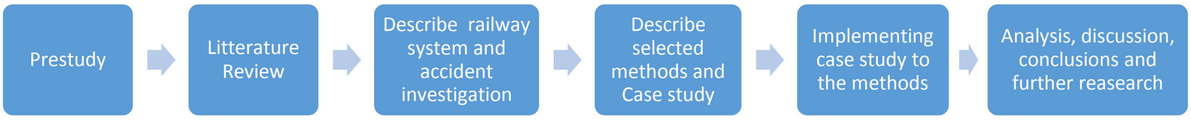

Prestudy
Litterature Review
Describe railway system and accident investigation
Describe selected methods and Case study
Implementing case study to the methods
Analysis, discussion, conclusions and further reasearch

Figure 10: The process of preparing the Master's thesis.

Information was collected through literature searches, Internet, meetings and communications with supervisors, method experts and the RAIB. The basis for describing the European railway system, ERTMS signalling system and railway accident investigation is mainly found on webpages provided by the European Commission, ERA and Bane NOR SF. The literature search for accident investigation methods is mainly carried out using the search service ORIA at NTNU. A large part of the relevant literature was also found by searching the Bibliography of books, reports and articles that was relevant for the theme. The publications by Hollnagel and Speziali (2008), Quresih (2008) and Rausand (2011) was very good sources for relevant information and further reading. The main references for the selected methods in this thesis has been the description of the AIBN-method [27], Nancy Leveson Engineering a Safer World [7], Leveson and Thomas STPA Handbook [28] and the material published at the MIT webpage PSASS [29].

The case study was selected on the basis that it was the first official ERTMS case investigated by an Accident Investigation Board (AIB), in this case the RAIB in the UK. However this was challenging because the investigation was not finished at the time the thesis was written, and only an interim report was published by the RAIB. The RAIB has however provided information in a two day meeting at the RAIB office at Farnborough, and communication via e-mail and phone.

For the study of formal methods Terje Sivertsen at Bane NOR has been the main source of information, and provided references, notes and guidance on how formal methods can be used in an accident investigation in numerous meetings and e-mails.

At the end of the thesis the application of AIBN-method was discussed with the project manager of the AIBN-method, Ingvild K. Ytrehus senior advisor at AIBN. The application of CAST was discussed with Hyungju Kim, an associate Professor at the University of South-Eastern Norway, who has experience using CAST during his previous work at ROSS Gemini centre.

Finally the supervisors were given a draft report of the thesis to comment, before the final version was submitted.

3.2 Literature on accident investigation methods

In 1931 Heinrich published the Domino Model, and it was one of the first accident models that had a big influence on the later development of accidents models. In the beginning of industrial safety the focus was on unsafe conditions, such as unprotected moving parts in factories and dangerous equipment. After these accidents had been substantially reduced, the focus also emphasised unsafe acts and human error. In 1976 Bird and Lofthus included management decisions to the Domino Model as a factor, and in 1997 Reason introduced the Swiss cheese model based on the Domino Model [7].

The American sociologist Perrow published in 1984 a book called Normal Accidents [30], which characterised the complexity of the technological environment that the society is founded on. The complexity of modern systems is still increasing, and has unfortunately been proved by several serious accidents, such as Three Mile Island (TMI) accident in 1979, Chernobyl 1986, Columbia disaster 2003 and the Überlingen mid-air collision among many others. Figure 11 shows the increased complexity and safety focus in accident investigation since the 1970s.

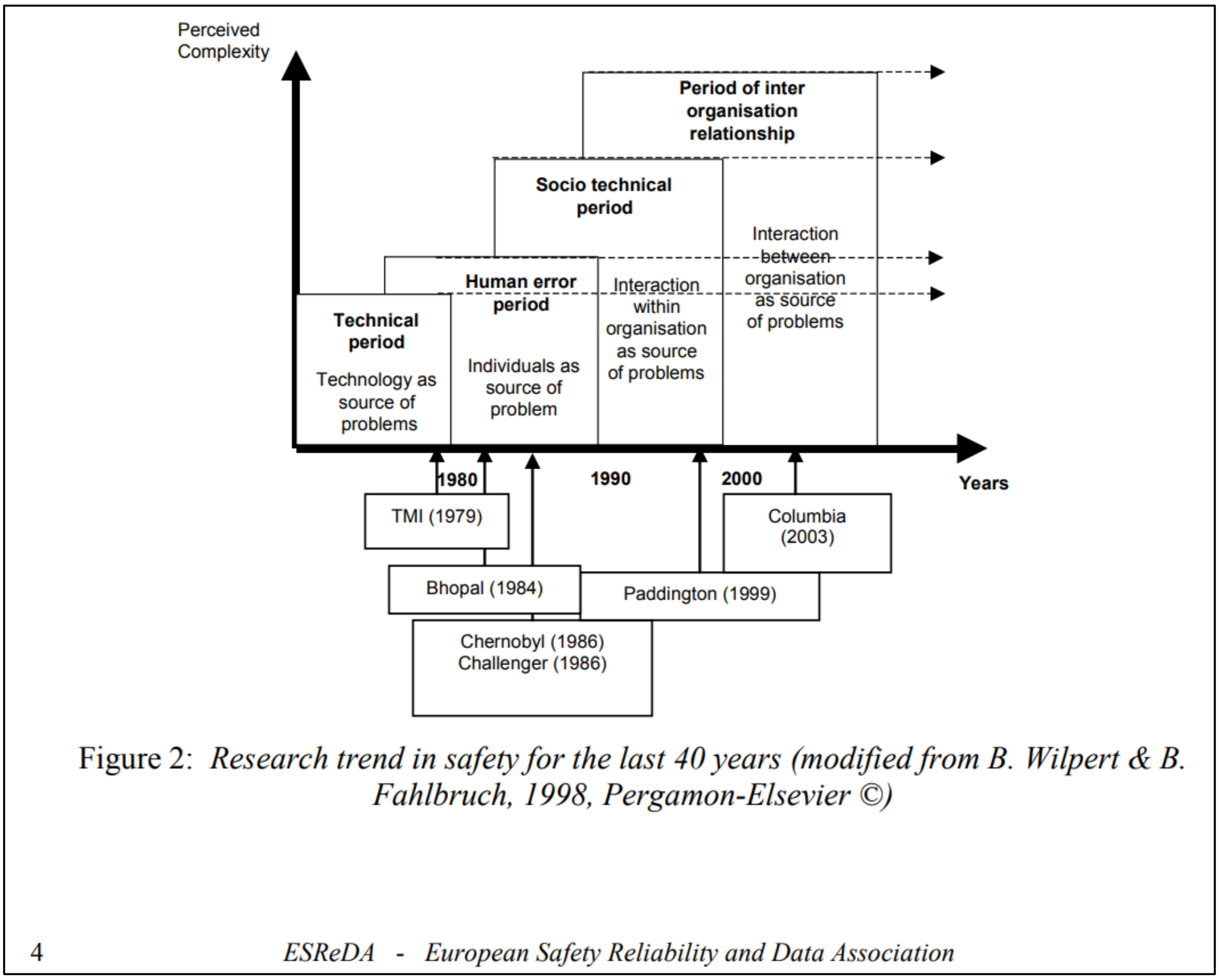

Perceived Complexity
Period of inter organisation relationship
Socio technical period
Interaction between organisation as source of problems
Human error period
Interaction within organisation as source of problems
Technical period
Technology as source of problems
Individuals as source of problem
1980
1990
2000
Years
TMI (1979)
Columbia (2003)
Bhopal (1984)
Paddington (1999)
Chernobyl (1986)
Challenger (1986)

Figure 2: *Research trend in safety for the last 40 years (modified from B. Wilpert & B. Fahlbruch, 1998, Pergamon-Elsevier ©)*

4 *ESReDA - European Safety Reliability and Data Association*

Figure 11: Research trend in safety for the last 40 years. Source: ESReDA.

In 1997 Rasmussen published the article "Risk management in a dynamic society: a modelling problem" [31]. He proposed a framework for modelling risk management in complex sociotechnical systems. In the article he claims that causal models (sequential chain-of-events), are inadequate to study failures and accidents in highly adaptable sociotechnical systems. The framework has two parts where the first is the structure of the industry, and the second the dynamic. The Dynamic of the system can modify and cause changes to structure and behaviour over time. Figure 12 shows Rasmussens example of various levels in a sociotechnical systems and the factors that can affect the different levels (environmental stressors). Rasmussen states that risk management is a control problem where accidents can happen due to loss of control of physical processes. In order to analyse a work domain's safety the boundaries of safe operations, and dynamic forces that may cause the operations to drift beyond those boundaries must be identified. He also claims that several catastrophic accidents has not happened because of coincidence or human error, but as a result of organisational migration towards an unsafe state due to pressure of cost-effectiveness in an aggressive, competitive environment.

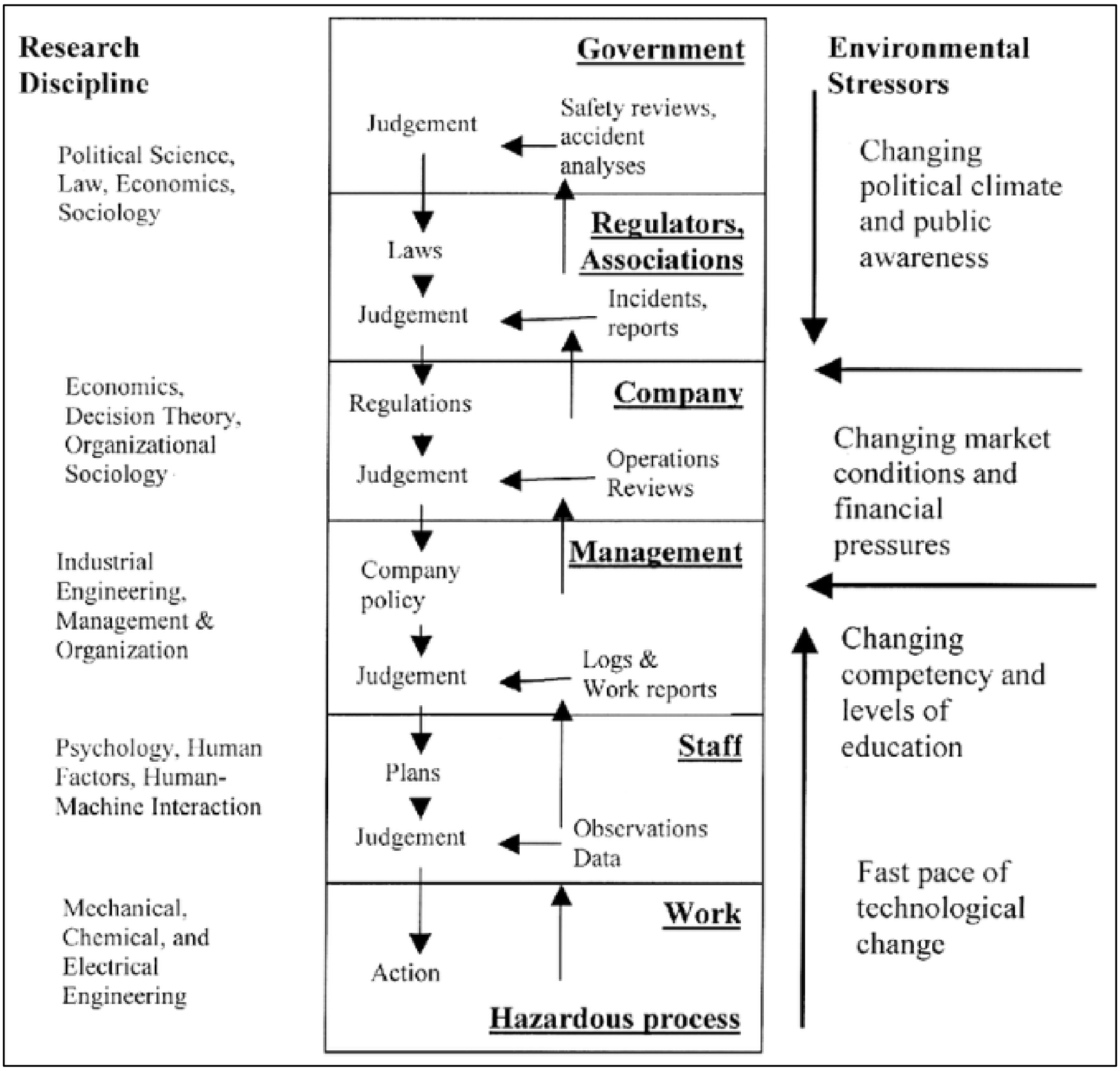
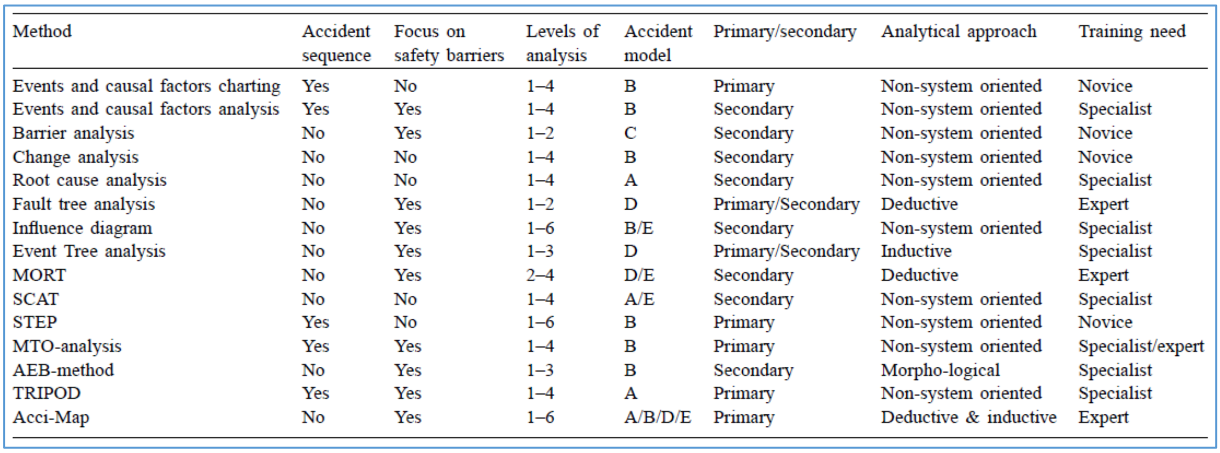

Research Discipline
Political Science, Law, Economics, Sociology
Economics, Decision Theory, Organizational Sociology
Industrial Engineering, Management & Organization
Psychology, Human Factors, Human-Machine Interaction
Mechanical, Chemical, and Electrical Engineering
Government
Judgement
Safety reviews, accident analyses
Regulators, Associations
Laws
Judgement
Incidents, reports
Company
Regulations
Judgement
Operations Reviews
Management
Company policy
Judgement
Logs & Work reports
Staff
Plans
Judgement
Observations Data
Work
Action
Hazardous process
Environmental Stressors
Changing political climate and public awareness
Changing market conditions and financial pressures
Changing competency and levels of education
Fast pace of technological change

Figure 12: The socio-technical system in risk management Source: Rasmussen, 1997.

Sklet published an article in 2004 [32] where he compared selected methods for accident investigation. The article presents a short description of some recognised and commonly used methods for accident investigation, and compares the methods based on selected characteristics (Figure 13). Sklet recommends that a combination of analytical techniques ought to be used in complex investigations, and that the investigation team have good knowledge about the different investigation methods. His work gives a good overview of commonly used methods until 2004, and may help investigators choose a suitable method for their investigation.



Method	Accident sequence	Focus on safety barriers	Levels of analysis	Accident model	Primary/secondary	Analytical approach	Training need
Events and causal factors charting	Yes	No	1–4	B	Primary	Non-system oriented	Novice
Events and causal factors analysis	Yes	Yes	1–4	B	Secondary	Non-system oriented	Specialist
Barrier analysis	No	Yes	1–2	C	Secondary	Non-system oriented	Novice
Change analysis	No	No	1–4	B	Secondary	Non-system oriented	Novice
Root cause analysis	No	No	1–4	A	Secondary	Non-system oriented	Specialist
Fault tree analysis	No	Yes	1–2	D	Primary/Secondary	Deductive	Expert
Influence diagram	No	Yes	1–6	B/E	Secondary	Non-system oriented	Specialist
Event Tree analysis	No	Yes	1–3	D	Primary/Secondary	Inductive	Specialist
MORT	No	Yes	2–4	D/E	Secondary	Deductive	Expert
SCAT	No	No	1–4	A/E	Secondary	Non-system oriented	Specialist
STEP	Yes	No	1–6	B	Primary	Non-system oriented	Novice
MTO-analysis	Yes	Yes	1–4	B	Primary	Non-system oriented	Specialist/expert
AEB-method	No	Yes	1–3	B	Secondary	Morpho-logical	Specialist
TRIPOD	Yes	Yes	1–4	A	Primary	Non-system oriented	Specialist
Acci-Map	No	Yes	1–6	A/B/D/E	Primary	Deductive & inductive	Expert

Figure 13: Characteristics of different accident investigation methods Source: Snorre Sklet.

Nancy G. Leveson is a professor of Aeronautics and Astronautics at Massachusetts Institute of Technology (MIT), and an expert in system and software safety. In 2004 she introduced a new accident model based on system theory, called Systems-Theoretic Accident Model and Processes (STAMP) [33]. In the article the need for a new model is prescribed due to the complexity of new technology that the old models are not able to cope with. The system thinking and theory is based on ideas developed after World War II, and are based on System Safety introduced by aerospace engineers such as C.O. Miller, Jerome Lederer and Willie Hammer among others. Jens Rasmussen's work has also had a great influence on the foundation of STAMP. The main application was complex systems such as aerospace, military aircraft and ballistic missile systems.

In STAMP safety is defined as a continuous control task where the identification of constraints, such as design and operations, is the key factor in managing safety. The focus on preventing component failure events is less apparent, and accidents are seen as a result of inadequate control of safety constraints at the system level. The levels of the socio-technical structure of a system is described by how each level exercises control over emergent properties, see figure

14. In order to have control it is not sufficient to only give an order or input, but also make sure the feedback is sufficient to maintain safety as performance changes over time. Feedback is an important mechanism to be able to detect and incorporate changes and adaptions in a system.

Leveson claims the event chain model, which most accidents models are based on, has important limitations as the inadequate control is only indirectly reflected by events. As an example the event chain may regard component failure as the cause of the accident, while STAMP will regard inadequate control of the safety constraints for the component as the main cause. In STAMP the safety control structure must be determined to explain why the control and feedback failed and the event occurred. Other important aspects in STAMP is to understand dysfunctional interactions, the context of the decisions taken and the reason for flawed control actions. Leveson describes an approach to accident analysis based on STAMP, called Causal Analysis based on STAMP (CAST) in the book Engineering a safer world, published in 2011 [7]. This approach is described and used to compare models with the AIBN-method later in this thesis.

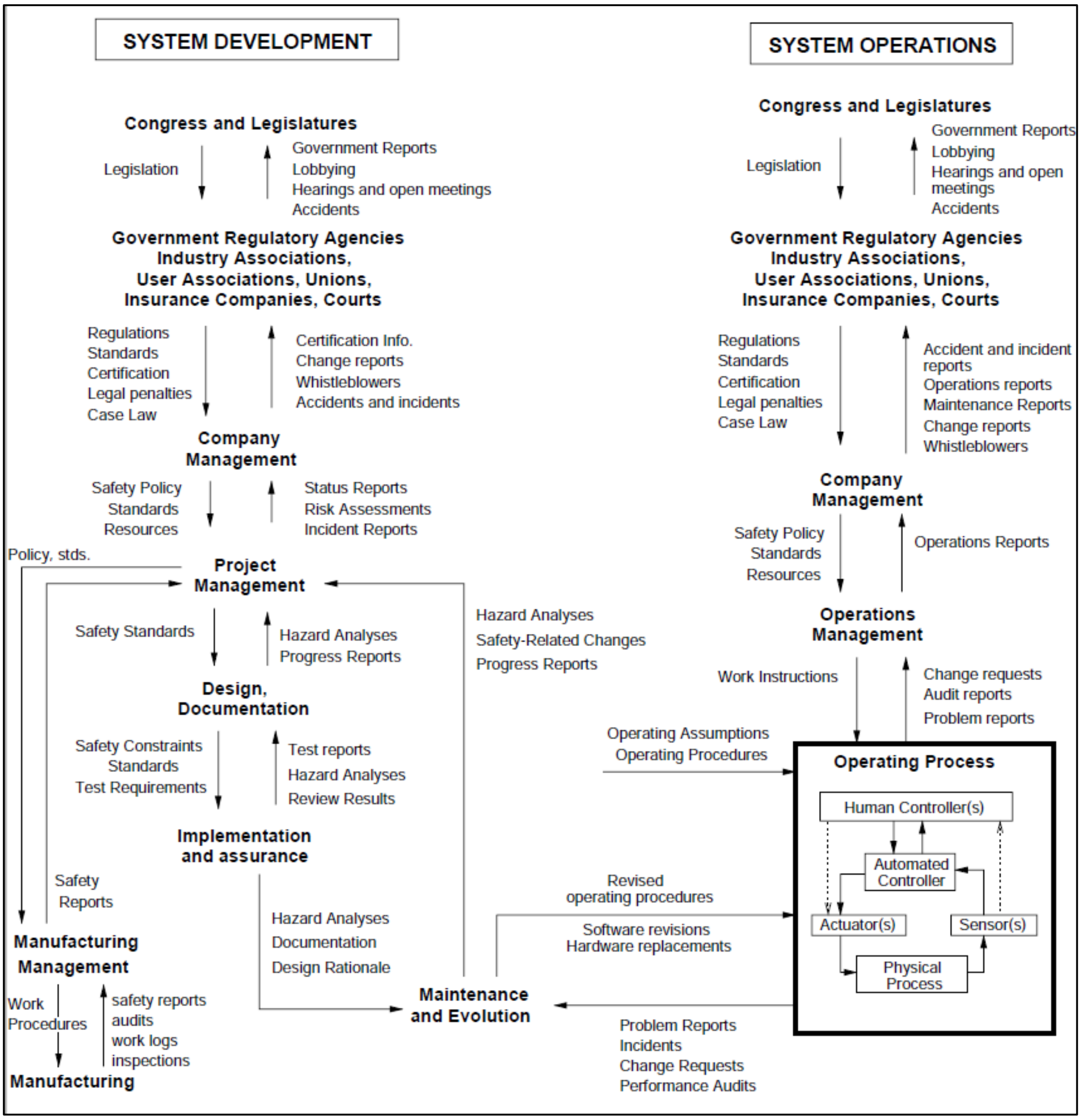


Figure 14: Example on sociotechnical safety control structure safety-critical industry. Source: Nancy Leveson.

Hollnagel and Speziali published a report in 2008, ordered by the Swedish Nuclear Power Inspectorate, on the development of methods for accident investigations [3]. The study includes a "State of the Art" and describes methods of accident investigation. The study addresses seven selected methods and places these into Perrow's (1984) diagram describing accidents in socio-technical systems in four dimensions. The diagram shows how closely connected the systems are (coupling) and how complex (description) the systems are considered to be. The study updated Perrow's original chart describing the linkage and complexity of selected industries, and assessed the scope of application for the seven survey methods (figure 15). The study acknowledges that not all accidents within an industry are necessarily the same, and that it is necessary to choose an appropriate method based on the dimension of the accident. The study lists six questions that can be used to characterise the accident and thus choose the appropriate method. The report makes a remark that it must be expected that by five or ten years the described methods will have been partly obsolete because the nature of socio-technical systems change, and therefore accidents tend to change also.

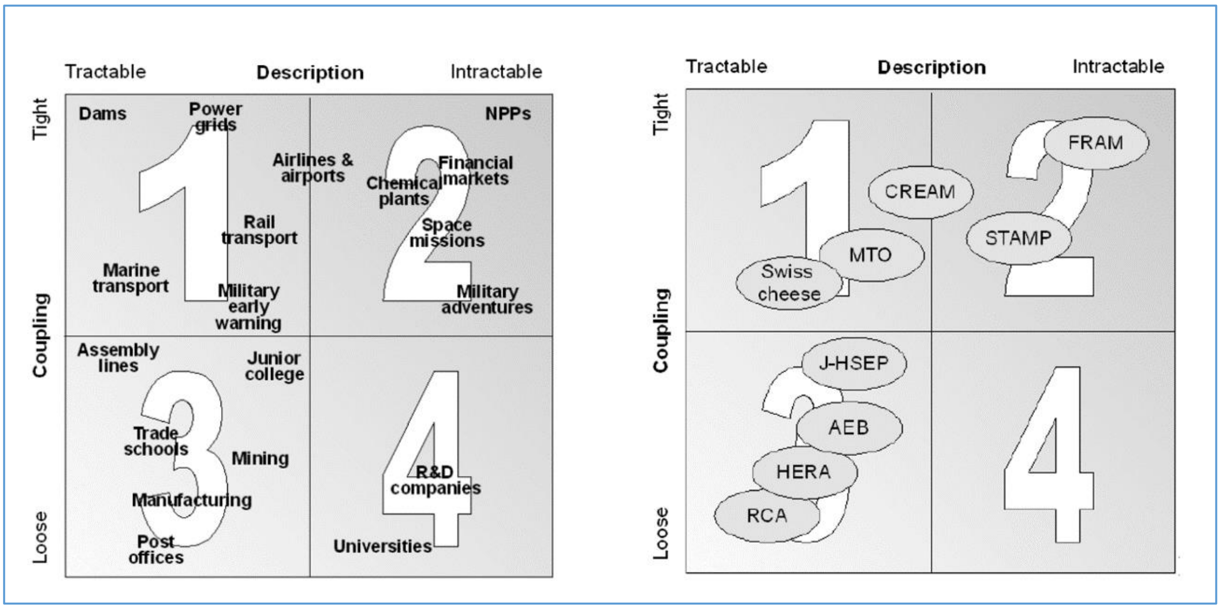


Figure 15: Complexity Chart and Accident Investigation Methods. Source: Hollnagel and Speziali 2008.

The Australian Defence Science and Technology Organisation published a report by Qureshi in 2008 with a review of accident modelling approaches for complex critical sociotechnical systems [34]. The report gives a review of traditional accident models and their limitation on accident causality of modern complex systems. New approaches to safety and accidents based on systems theory are discussed in order to understand complex systems. Research in formal methods for modelling complex system accidents are also discussed, and the significant contribution by organisational sociologists is highlighted. For analysis of complex systems the report recommends models based on system theory, and a need for more research to understand the many dimensions of safety and modelling sociotechnical system accidents.

Rausand published a textbook in 2011 [35] mainly for university courses in risk analysis and risk assessment. The book describes different methods and acts as a guide for practical risk assessments. He makes a link between how accidents occur and the influence it has on the approach to risk analysis. His book includes a chapter describing accident models and accident causation that gives a good overview on state of the art and references at the time the book was published.

A comparison of the system-based accident analysis methods Accimap, HFACS and STAMP was published in 2011 by Salmon, Cornelissen and Trotter [36]. The article presents a case-study of a school outdoor walking activity that claimed six lives, due to drowning. The aim of the paper was to compare and recommend the most suited method as there is a lack of guidance material to support the selection of one method over the other. In the conclusion the authors recommend a modified version of the Accimap method. However the article also states that the selection of accident method is more likely to be based on theoretical preference than anything else. For single accident investigation the Accimap and STAMP seems to be the most suited, while for multiple accident studies the HFACS seems to be more powerful.

The importance of software in accidents is highlighted in Hardy’s publications [37] in 2012 and his book published 2012 [38]. He summarises hundreds of accident reports, and demonstrates that many organisations do not incorporate software effectively in the system safety process. He uses these lessons learned to promote a questioning approach to help improve software safety. Examples of such questions are also demonstrated in his paper presented at the Australian System Safety Conference at Brisbane in 2012 [37]. His publications is a good source for accident investigators and risk analysers who wants to read about previous accident experiences.

Underwood and Waterson published in 2012 a critical review of three systemic accident analysis models; STAMP, FRAM and Accimap [5]. They claim that the system approach is promoted in the research literature as the conceptual preferred method for analysing socio-technical system accidents. Although the literature advocate systemic analysis models, it is not widely used in the industry. Reputable international researchers such as Leplat, Salmon, Hollnagel, Leveson, Rasmussen, Lindberg etc. are of the opinion that investigation of accidents must be viewed in a system perspective as a whole. In isolation, it is not sufficient to merely consider the accident based on, for example, component failure, human error or software failure. The system approach involves looking at the integration between technical and social elements and how they interact in the environment in which they exist. The purpose is to be able to assess which control mechanisms exist in the system as a whole, and consider where they have failed in an accident. This is referred to as the biggest paradigm shift in research on methods of accident investigation in recent times. The critical review claims that the systemic approach in accident investigation is used to a small extent in industry. The key factors to why it is not widely used in the industry are related to model validation, usability, analyst bias and the implication of not apportioning blame for an accident.

Underwood and Waterson published a report in 2013 called "Accident Analysis Models and Methods: Guidance for Safety professionals" [39]. The report is based on accident analysis literature review and interviews with 42 safety experts. The first part of the report explains different accident analysis methods and factors influencing an individual's selection of these methods. The second part of the report presents methods currently used in the industry, and experience from the Australian Transport Safety Bureau and Dutch Transport Safety Board is described. In order to select a suitable technique the report lists a number of questions to guide the investigator to take a more informed decision. The report also has an appendix with useful sources of accident analysis information to give a general coverage of the most "popular/ recognised" methods and techniques.

Underwood, et.al. published an article in 2015 where they performed a small-scale, field-based evaluation of STAMP funded by Loughborough University. Six practitioners within accident investigation took part in a workshop at Cranfield University, where they used STMAP and evaluated the method in a questionnaire. The research has limitation such as the small group of participants, but it was suggested that the methods usability and graphical output was highlighted as in need of improvement. Also the study states that learning about STAMP and its application is not a quick process, and the participants needed multiple attempts to achieve a sufficient level of understanding.

In 2015 Stoop and Benner published a paper where they questioned what STAMP-based analyst expect from safety investigations [40]. The paper examines the information CAST requires, its sources, and describes a series of 12 potential threats to the quality of the analyses. One important prerequisite in the paper is that it views CAST analysis that are based on input from accident investigation reports. The authors claim that CAST does not specify an accident investigation process, but only a way to document and analyse the result of such a process. The main conclusion is that CAST analysts should be wary of the variations among investigation report methods, and the effect it might have on the CAST analysis. The causal data in investigation reports may be problematic due to the investigations relationship to juridical connotations of proof, truth, reasonable doubt and liability.

3.3 Experience on investigation ERTMS accidents

In this thesis a complex investigation is related to software controlled signalling system on the railway, in particular the ERTMS signalling system. This narrows the scope in order to explore a possible approach for investigating this type of accidents and incidents. At the time this thesis was written only an interim report concerning ERTMS had been published by an Accident Investigation Body (AIB), and official reports on ERTMS investigations is very limited. However, ERTMS can be compared to other modern signalling systems, and experience from former accident investigation is available.

The official NIB investigation at the time this thesis is written is an interim report published by the Rail Accident Investigation Branch (RAIB) in the UK [41]. The investigation concerns the loss of Temporary Speed Restrictions (TSR) after a restart of a server. The missing TSR was not detected by the safety critical software, nor by the first train drivers to go through the TSR locations after the restart. The missing TSR was discovered the next day after a train driver reported that he did not see the TSR in his driver panel (DMI). This is the selected case example, and it is used to demonstrate the methods in chapter Application of the methods5.

In November 2013, Bane NOR (formerly Jernbaneverket) established a pilot project for trial operation of ERTMS on the eastern line between Rakkestad and Sarpsborg. Several internal investigations of unwanted events affecting ERTMS have been carried out. The experience from these surveys shows that it can be difficult to obtain relevant information from logs, and to obtain personnel with the right expertise. Bane NOR says the events can be compared to traditional SPAD (Signal Passed at Danger) events, where a driver pass a red light without permission. During the pilot trial period several incidents has also occurred due to a lack of understanding how the technical system works, confusing both the dispatchers and drivers.

3.4 Accident similar to the ERTMS case example

Airong Dong's master thesis [42] and Dajiang Suo's paper [43] is analysing the "7.23" Yong-Tai-Wen Railway Accident which killed 40 people and injured 120 in China. The accident occurred as a consequence of a train receiving wrong side signalling information, and colliding into the rear of another train. The wrong side signalling information was a result of erroneous data from a track circuit that was not captured by the exception handling by the software. This lead to a "green" signal and allowed a speed of more than 100 km/h for the rear train. The green signal was indicating the track section was clear for the rear train, when the reality was another train traveling at 18 km/h at the same track. The signalling system in China is called Chinese Train Control System (CTCS), and has several similarities to the European Train Control System (ETCS). Also the 7.23 accident has similarities to the case example, the Cambrian Line loss of speed restriction, used in this thesis. Both Dong and Suo used the STAMP theory to analyse the accident, and claim they found more inadequate controls and questions the official investigation had not answered. Unlike a European accident report the official Chinese investigation report [44] used many pages to assign responsibility and suggest punishment to the responsible people.

4 Methods

In this section the selected methods are described and explained for the later chapter where the methods are applied.

4.1 The AIBN method - framework and analysis process

In this chapter the theory for the AIBN-method is presented for each of the seven stages. This is later exemplified in chapter 5.2, where the case example is demonstrated using the AIBN-method. Because the method is relatively new and there is little literature describing the AIBN-method, a great deal of the material is reproduced in this thesis to explain and demonstrate the method.

The Accident Investigation Board Norway (AIBN) has developed the AIBN-method which describes how investigations of accidents in transport are to be conducted by the AIBN [27].

This is a safety framework and analysis process for systematic investigations. It is not a fixed process, but a toolbox investigators can use for selecting the most appropriate method or analysis for the current investigation. The document is based on safety literature and different methods and theories related to accident investigation. Frameworks from the United States [45], Canada [46] and Australia [47] have been the basis for the AIBN-method. The framework was first published in 2017, describing what AIBN considers best practice for systematic investigations.

Accident investigation can be divided in three overlapping phases as shown in figure 16.

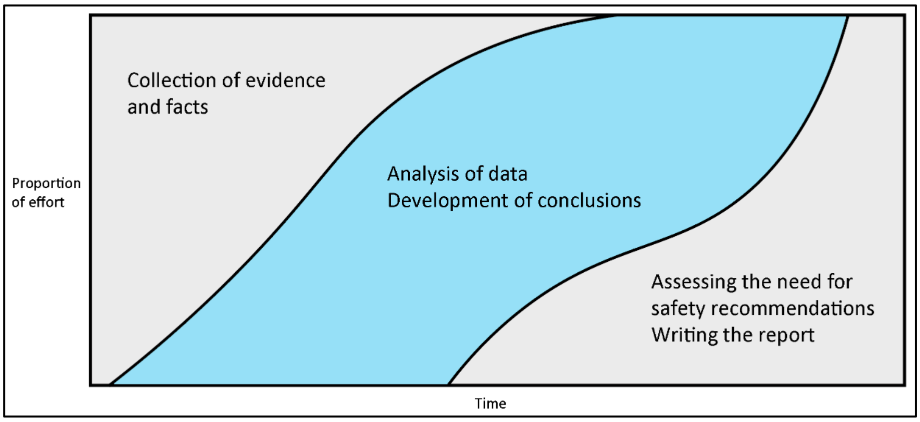


Figure 16: The three phases of an accident investigation. Source: DOE, 1999.

The AIBN also collects facts and evidence, but this is not covered in this thesis. Accident investigators at AIBN are given special training at Cranfield University on how to collect evidence and facts. This is a very important phase, and it can be challenging to know what evidence and facts that are important in the start of the investigation.

The analysis process is divided into seven stages and describes the course of life in an accident investigation, the whole process in shown graphically in figure 17. Stage 1-3 describe the process to find out what happened, stage 4-5 are the process of finding out why it happened and stage 6-7 are about how to prevent new accidents. Each stage is explained in the next chapters. The analysis process is iterative, and it may be necessary to go back and reconsider or make changes to earlier stages.

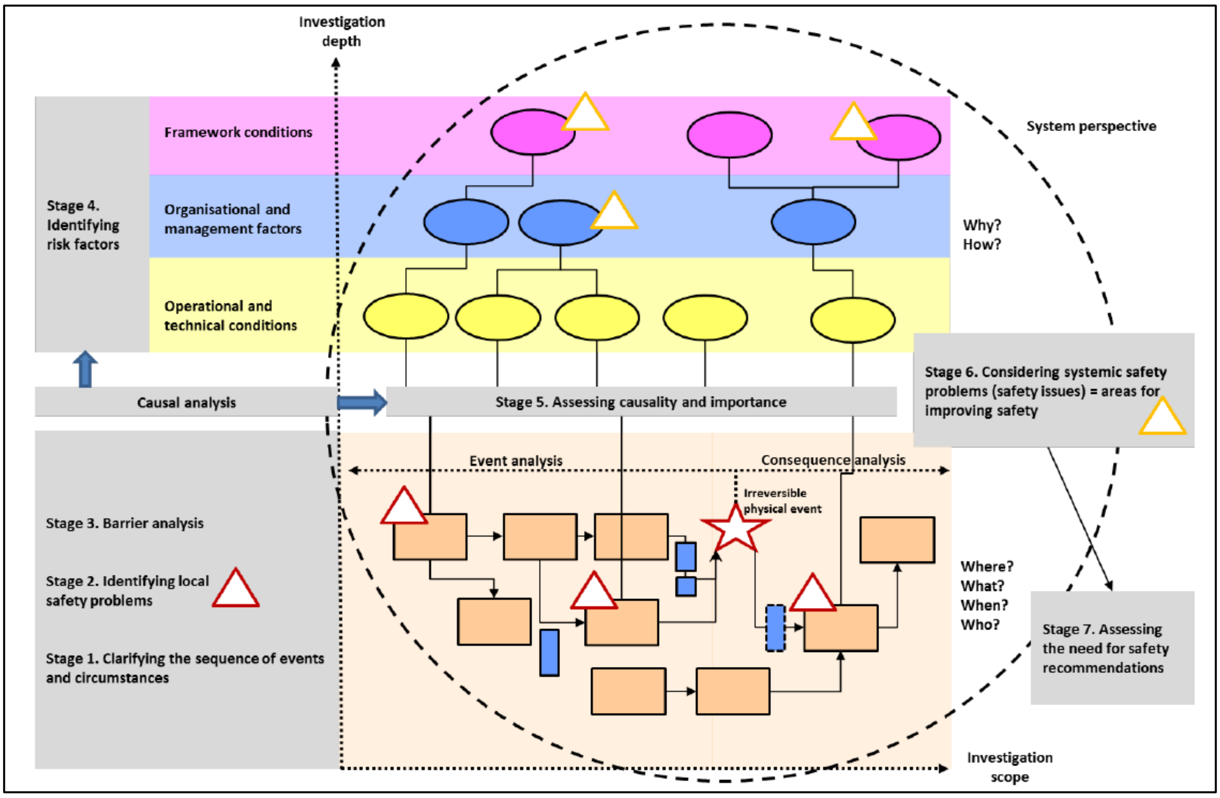

Investigation depth
Framework conditions
System perspective
Stage 4. Identifying risk factors
Organisational and management factors
Why? How?
Operational and technical conditions
Stage 6. Considering systemic safety problems (safety issues) = areas for improving safety
Causal analysis
Stage 5. Assessing causality and importance
Event analysis
Consequence analysis
Irreversible physical event
Stage 3. Barrier analysis
Stage 2. Identifying local safety problems
Where? What? When? Who?
Stage 7. Assessing the need for safety recommendations
Stage 1. Clarifying the sequence of events and circumstances
Investigation scope

Figure 17: The AIBN's analysis process for systematic investigations. Source: AIBN-method.

4.1.1 Stage 1: Clarifying the sequence of events and circumstances

The first step of the analysis process is to make sure the sequence of events are clear and that relevant circumstances are included. In some investigations this can be straight forward to understand, but in other cases it might be several theories that can explain the sequence of events that must be investigated. In the experience of using the AIBN-method so far the STEP method (Hendrick and Benner, 1987) has proven to be useful. STEP is helpful in order to structure actions, events and relationship between them. This will also challenge the investigation to uncover deficiencies, uncertainty and the need for further information.

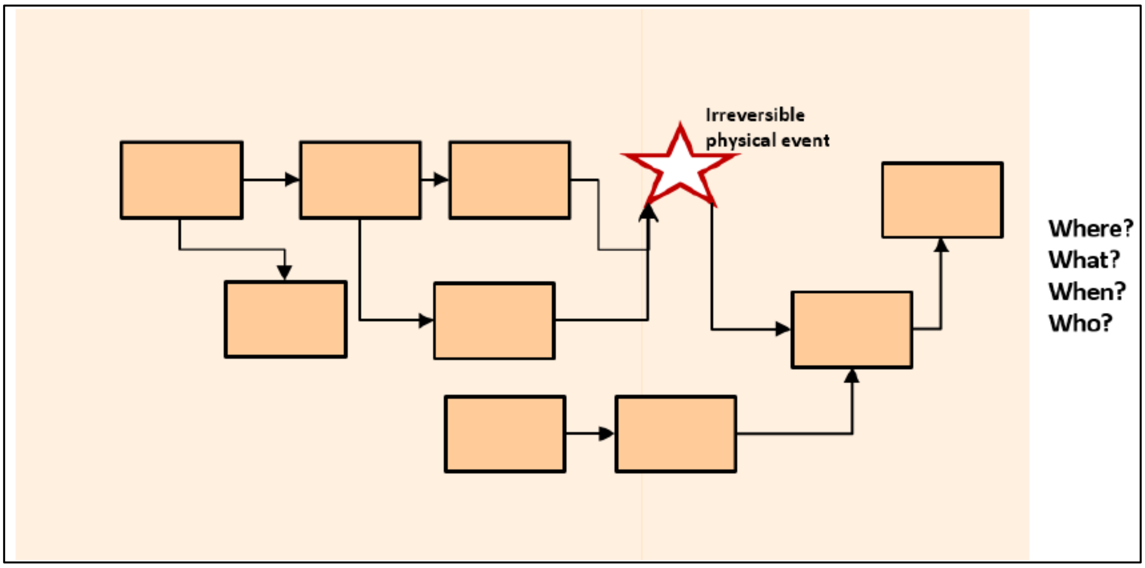


Figure 18: Stage 1. Clarifying the sequence of events and circumstances. Source: AIBN-method.

The time of the accident is defined as an irreversible, physical event. In rail transport examples can be derailment, collision or fire and is marked by a star in figure 18. For each stage the AIBN-method gives a summary on the most important factors in the analysis.

> *Stage 1. The sequence of events and the circumstances surrounding the accident must be sufficiently clarified to understand and describe what happened, where and when the events occurred and who was involved. This stage should also have clarified how an ideal transport process or work operation was meant to proceed. Any uncertainty and alternative interpretations of the sequence of events should have been assessed at this stage.*

Summary from the AIBN-method on stage 1. Source: AIBN-method.

4.1.2 Stage 2: Identifying local safety problems

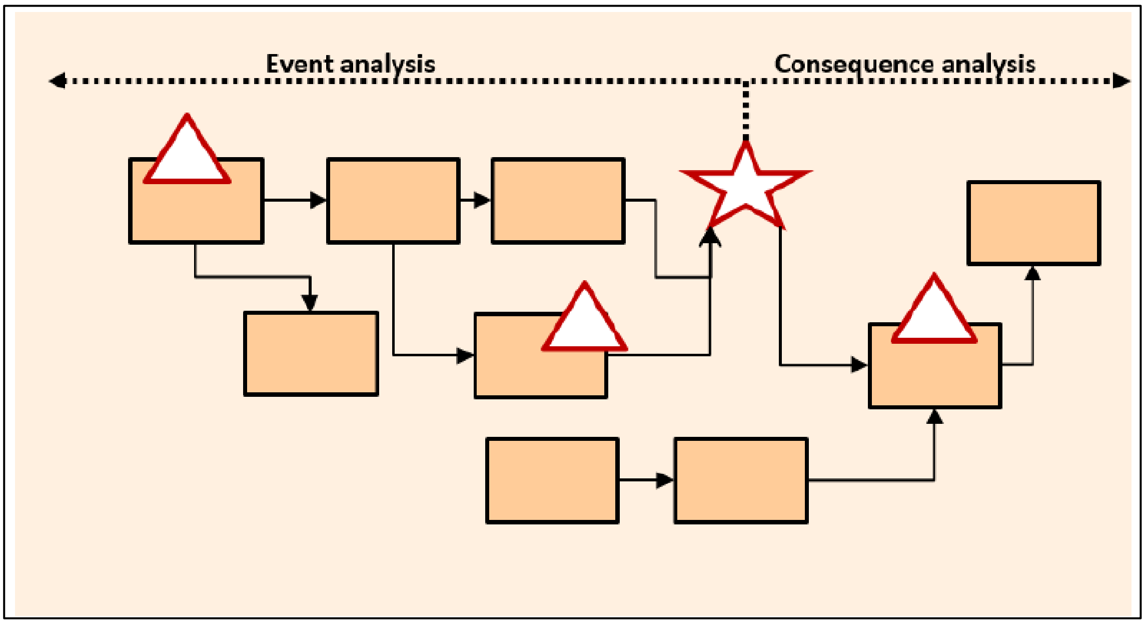


Figure 19: Stage 2. Identifying local safety problems. Source: AIBN-method.

The purpose of this phase is to identify what went wrong, and where in the sequence it happened. The local safety problems can be present in a condition or event, and may have been a latent safety problem for a long time. Local safety problems are marked by a red triangle in the sequence of events, see figure 19. For each safety problem it might be necessary with deeper examinations, and they should be considered as possible symptoms of underlying systemic safety problems (stage 6).

> *Stage 2. The local safety problems shall have been identified in the sequence of events, so that we have a clear idea and description of ‘what went wrong’. The identification of local safety problems shall then form the basis for a decision and delimitation of the topics to be investigated in more detail. This includes what data are to be collected, which investigation methods will be used and what resources are required in the further investigation.*
>
> *If relevant, this stage can also form the basis for preparing a preliminary report, status report on the investigation or a notification of safety-critical issue.*

Summary from the AIBN-method on stage 2. Source: AIBN-method.

4.1.3 Stage 3: Barrier analysis

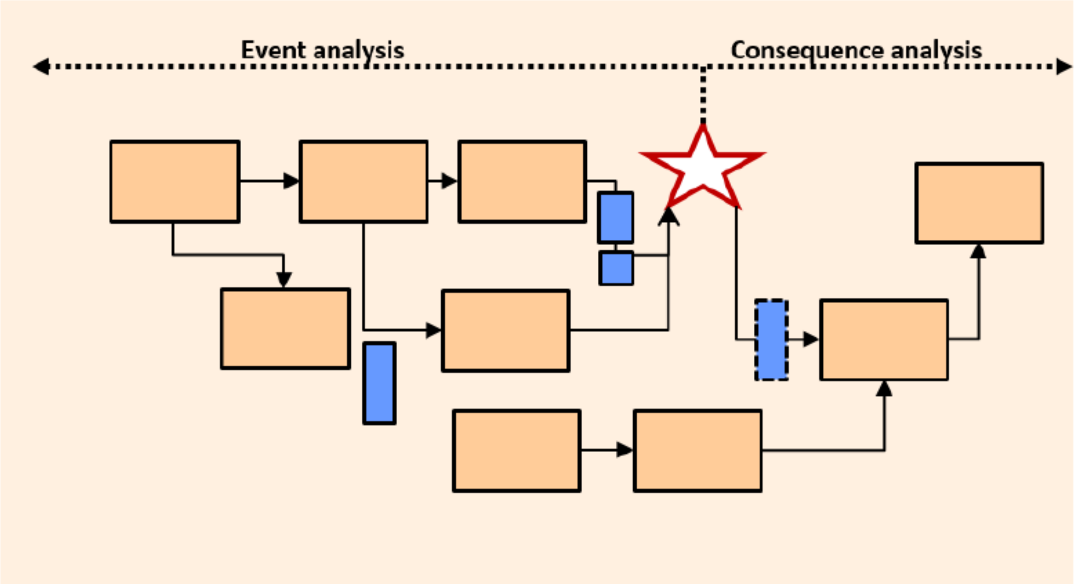


Figure 20: Stage 3. Barrier analysis. Marked by blue rectangles. Source: AIBN-Method.

If the barriers are not clearly defined during the sequence of events and safety problems, a barrier analysis can be useful. The barriers are marked by blue rectangles in the sequence of events, see figure 20. The purpose is to identify the systems protection mechanisms and barriers that were in place, or should have been in place, to prevent the accident. It is useful to distinguish between barrier that were in place, failed and or were missing.

▯ Barriers that were in place and that worked.

□ □ Weaknesses and failings in existing barriers.

⬚ Barriers that had not been established at the time of the accident (both barriers that should have been and that could have been established).

Figure 21: Illustration of barriers in the AIBN-method. Source: AIBN-method.

Stage 3. The barrier analysis shall ensure that the investigated systems' established defences are identified, and that the barriers that potentially could have been in place to prevent or limit the damages in the sequence of events in question have been identified. The barrier analysis can also form the basis for considering and prioritizing areas for improvement at Stage 6.

Summary from the AIBN-method on stage 3. Source: AIBN-method.

4.1.4 Stage 4: Identifying risk factors

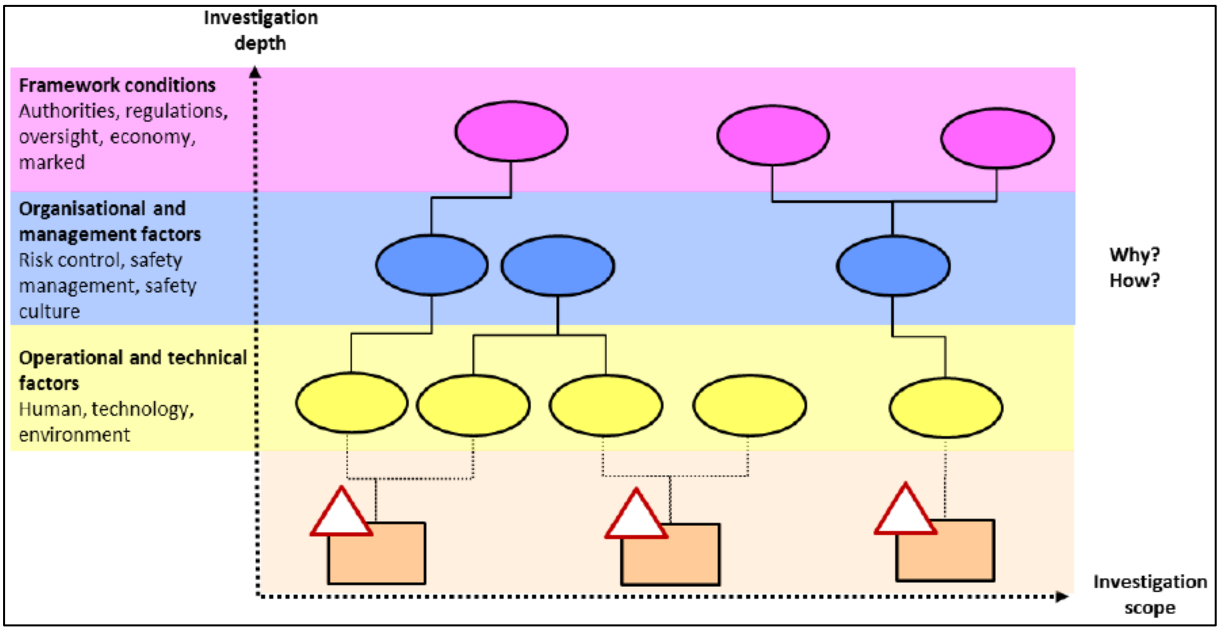

Investigation depth
Framework conditions
Authorities, regulations, oversight, economy, marked
Organisational and management factors
Risk control, safety management, safety culture
Operational and technical factors
Human, technology, environment
Why?
How?
Investigation scope

Figure 22: Stage 4. Identifying risk factors. Source: AIBN-method.

Stage 4 is a challenging step in the investigation process, and seeks to explain why and how safety problems occurred and why and how the barriers did not prevent the accident. Stage 4 and 5 are linked, and for each risk factor there must be an evaluation of the causality and importance. The intention is to establish a link between the sequence of events and the socio-technical system, see figure 22. This can be difficult as some of the factors may not have clear cause and effect relationships, but are identified as factors that increase the risk of an accident. Examples such as fatigue, work pressure, unclear procedures, lack of training, economy etc. are factors to be considered. Further analysis should identify why the organisation or authorities had not identified, or accepted the risk factors that contributed to the accident. Deep investigation into risk factors might increase the complexity of the investigation and require more information and resources, and it is important to evaluate the expected benefit of expanding the investigation (see stage 5). The investigation of risk factors has many dimensions such as:

- human factors
- technical factors
- factors in the surroundings/local conditions
- damage/injury and survival aspects
- organisational and management factors

- safety-related framework conditions
- systemic approach

The AIBN-method gives a more comprehensive description of this stage, and is recommended as further reading to learn more about the dimension of risk factors [27].

> *Stage 4. Risk factors have been identified, so that we have gained knowledge about and insight into how factors at different levels may have contributed to and affected the sequence of events and local safety problems. The width and depth of the investigation are evaluated against learning effect, safety value and resource/time spent. All sub-investigations are concluded and connected so that we have a sufficient basis for establishing an overall picture of the accident and preparing an eventual influence diagram or causal map.*

Summary from the AIBN-method on stage 4. Source: AIBN-method.

4.1.5 Stage 5: Assessing causality and importance

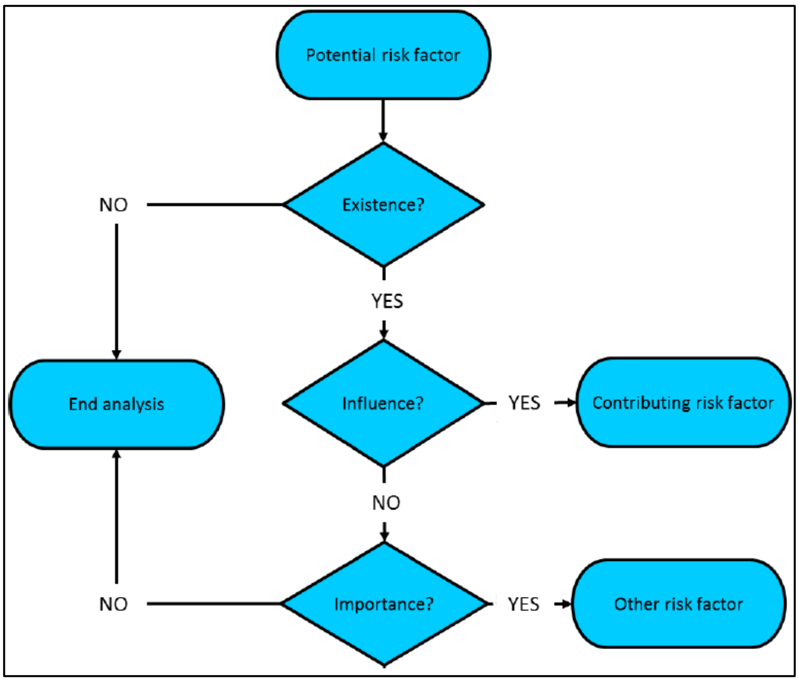


Figure 23: Stage 5: Testing potential risk factors with regard to importance. Source: ATSB, 2015.

For each risk factor identified in stage 4 the importance is evaluated in this stage. The purpose is to explain and understand the affect the risk factor had on the accident. In order to illustrate the process of testing the importance of risk factors the ATSB's (2015) description in figure 23 is useful. Some risk factors might not have contributed to the accident, but can be an important finding. It must be clearly stated in the report that the factor did not influence the accident.

> *Stage 5. Assessing causality and importance is intended to ensure transparency in how the investigation and identified risk factors, are rooted in the specific sequence of events, and contribute to make the investigation verifiable. All risk factors shall be assessed in such detail that we demonstrate that we have understood and explained the extent to which and in what way the identified factor has existed and affected the sequence of events. Factors that proves not to have contributed to the accident are examined in terms of importance with regards to safety.*

Summary from the AIBN-method on stage 5. Source: AIBN-method.

4.1.6 Stage 6: Considering systemic safety problems

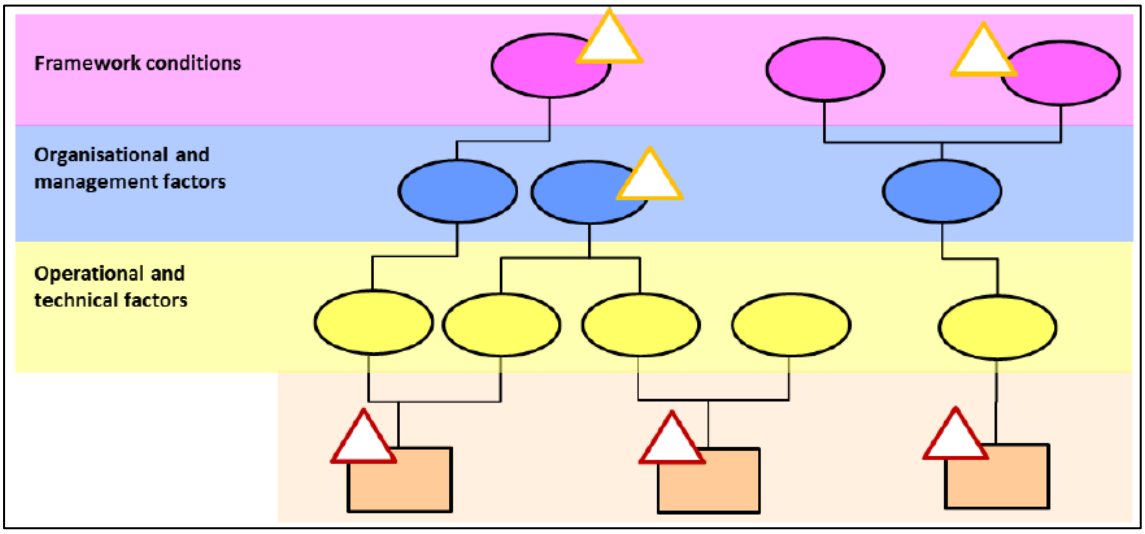

Framework conditions
Organisational and management factors
Operational and technical factors

Figure 24: Stage 6. Systemic safety problems and areas for improving safety. Source: AIBN-method.

Identification of systemic safety problems might be the most effective way to prevent future accidents. These problems can be the result of deficiencies in the authority or organisational risk control or the design of the system. Systemic safety problems and areas for improving safety are marked with yellow triangles in figure 24.

Stage 6. Assessment of how safety can be improved by considering systemic safety problems. A systemic safety problem can be described as the investigation's most significant findings for safety. It is a risk factor (independent of whether it contributed to the specific accident) which an organisation or authority has some level of control and responsibility, and which can increase the risk of future accidents.

Summary from the AIBN-method on stage 6. Source: AIBN-method.

4.1.7 Stage 7: Assessing the need for safety recommendations

The last stage of the AIBN-method is to evaluate the need to issue safety recommendations. The method list four aspects to consider when evaluating safety recommendations:

a) Importance and impact of the problem
b) Actions already taken
c) Is it possible and will to implement the recommendations
d) The expected effect on safety

The AIBN-method recommend a strategy to create safety recommendations aiming at the higher level that is expected to have to most impact on preventing accidents. Issuing recommendations aiming at the lower level such as the error or triggering mechanism has a limited impact on preventing new accidents. The method also refers to Haddon’s 10 strategies to systematise and prioritise accident prevention.

The process of creating safety recommendations is given high priority in the AIBNs railway department. For each investigation report with safety recommendations an internal group is evaluating and discussing each recommendation, before it is sent to external review to the involved actors in the investigation.

Stage 7. A reasoned decision has been made about the areas in which it is necessary to make safety recommendations. Assessing the need for safety recommendations is based on the seriousness of the identified systemic safety problems, safety action already taken, improvement effect and practicality. New accidents are best prevented through safety recommendations which are rooted in underlying/systemic factors.

Summary from the AIBN-method on stage 7. Source: AIBN-method.

4.2 CAST – Causal Analysis based on STAMP

Nancy G. Leveson is the author behind the Systems-Theoretic Accident Model and Processes (STAMP) theory, and states that this new model better can help investigations to understand the complex socio-technology systems than many old models [33]. STAMP is the basis theory for the Systems-Theoretic Process Analysis (STPA) and the Causal Analysis based on Systems Theory (CAST). STPA is a proactive hazard analysis technique, and CAST is a retroactive analysis model for accidents. Both STPA and CAST focus on safety control structure, and the first steps in both models are the same. STAMP interpret control broadly and includes all known elements from safety engineering such as design, interlocks, development processes, government regulations, culture etc. This applies in general to component failures, unsafe interactions, system operating processes, software flaw, social control and human behaviour.

The STAMP theory aims to create a better understanding of accidents and states the following:

- *"Accidents in modern transport are often so complex that it is hard for one person to understand every aspect of the process. High reliability and complicated verification process for component or parts of a system do not necessary evaluate the risk of interactions.*
- *It is important to analyse interactions among system components, and shift focus away from individual component failure or human failure.*
- *Accident are caused by inadequate control of safety in management of system interactions, rather than one failure that triggers a chain of events.*
- *Finding inadequate safety control is more important than finding the root cause in an accident. If proper safety control is missing, then new accidents from other root causes will continue to happen.*
- *Context is important to understand actions or events. Why did it make sense to take that decision, why did the "thing" not work or why did the part break down."*

4.2.1 CAST process

CAST regards accidents as involving complex processes and not just individual events. By using CAST the goal is to demonstrate the sociotechnical control structure and the violated safety constraints. This may result in multiple views of the accident, depending on the perspective and level in focus. Why the safety constraints failed and how to prevent future events are the desired results of the CAST analysis. The process of CAST must not necessarily be followed step by step, but is described in terms or parts. Leveson describes the process in nine steps, and the first three steps are the same as in the STPA-based techniques [7].

4.2.2 Stage 1: Identifying system hazards

Leveson defines system and hazard:

"A system is a set of components that act together as a whole to achieve some common goal, objective, or end. A system may contain subsystems and may also be part of a larger system.

A hazard is a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss."

In order to eliminate confusion about multiple terms such as accident, mishap or adverse event, the STPA handbook [48] introduced the term "losses". The STPA definition of loss is something of value to the stakeholder, and may include loss of human life, assets, reputation, reputation or damage to environment. After the losses are identified, than the hazards that can lead to a loss is identified. Hazards are defined as a system state or set of conditions that in worst–case will lead to a loss.

Leveson recommends that the number of system-level hazards are kept to about seven to ten, in order to make the list manageable and not too detailed. In the beginning the list of system-level hazards should be more abstract and manageable, and then refined into sub-hazards later if needed.

4.2.3 Stage 2: Identify System safety constraints and requirements

Leveson defines System safety constraints and requirements:
"*A system-level constraint specifies system conditions or behaviours that need to be satisfied to prevent hazards (and ultimately prevent losses)"*

The words constraints and requirements have the same meaning. The system safety constraints and requirements are linked to the hazard and must be controlled. In order to affect the safety the organisation need to have some form of influence in order to control the safety.

4.2.4 Stage 3: Document Safety control structure

The main focus at this stage is to identify control commands, feedback, responsibility and process models of each controller. It makes no sense that someone has the responsibility for something they cannot control, therefore a clear relationship between the control action and feedback loops for the controlled process must be established. The aim is to find the hierarchy of control and authority within the system. Each element in the safety control structure has authority and control over the entities below, and should also get feedback from those entities. By drawing a hierarchical safety control structure it should be easier to recognise the control relationship and feedback loops for the system. The safety control structure starts at an abstract level, before it is refined to a more detailed level of the operation or system in question. If STAMP has been used during the engineering process or previous accident investigations there might be a model already made to reuse.

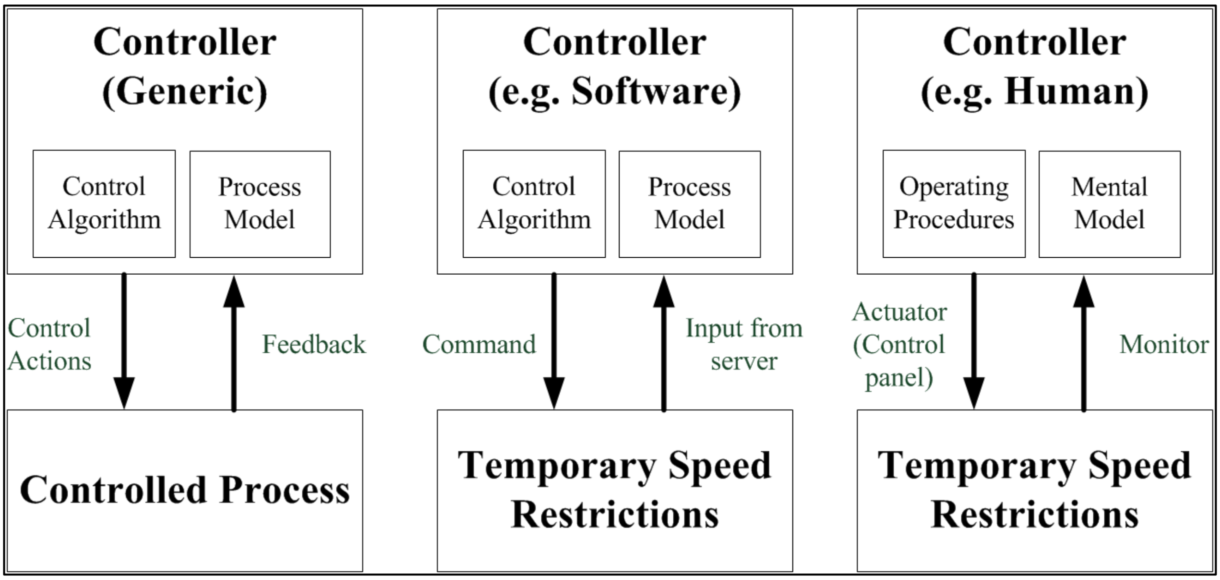


Figure 25: Generic control loop and two examples, software and human. Source: Leveson.

The generic control loop in figure 25 can be used to explain the interactions between elements in the safety control structure. Two examples that are relevant for the thesis is also shown in the figure, in order to visualise the possible use. The controller may provide a control action to influence the behaviour of the controlled process. The control algorithm or operating procedures represent the controllers' decision making process and which control action to provide. The process model or mental model represent the controller's internal beliefs about the control process or other relevant aspects to make a decision. The process model or metal model may be updated by a feedback used to observe the controlled process. For software this feedback may be in the form of a sensor, and for a human this may be a video monitor or a direct view of the controlled process. At this stage the responsibility and context of each controller must also be established. Determining the responsibility, or what it should have been, may start from the system safety requirements. In order to find the context it must be established why it made sense at the time to do the actions that was performed. The context may help explain why a "strange" action was performed, and may be repeated by a different person in the same context. Interaction between multiple control loops can be modelled in a hierarchical control structure, as shown in figure 26. The control structure may also be completed in parallel with the later steps.

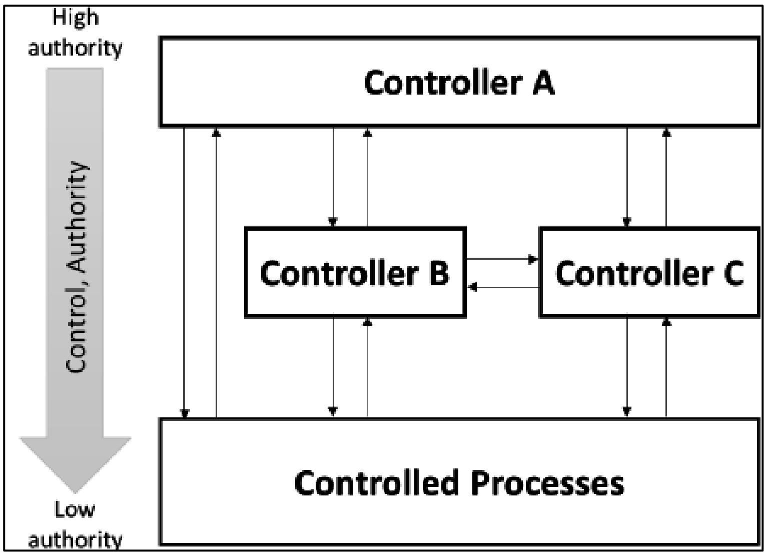


Figure 26: Generic hierarchical control structure. Source: Leveson.

4.2.5 Stage 4: Determine proximate events

In order to understand the physical process of the accident it is necessary to identify and describe the basic events related to the loss. This can be a list of the direct events that lead to the accident, or an event chain if that is more suitable to describe what happened. The goal of an STAMP-based analysis is to find out why the event occurred and not to find out whose fault it was.

4.2.6 Stage 5: Analyse loss, identify contributions and ineffective controls

The purpose is to go deeper into stage 4 and analyse why the physical control in place did not prevent the accident for each of the relevant events. This includes analysis of the physical process including the physical and operational controls, potential failures, dysfunctional interactions etc. Which controls did not work and why, are questions the analysis seeks to answer. Leveson exemplifies this stage with a table displaying the requirements and controls and the inadequate controls and failures. In addition the physical contextual factors contributing to the event are included.

4.2.7 Stage 6: How and why the inadequate control contributed

Finding and understanding the physical control inadequacy are often found short time after the investigation is started. However it is harder to analyse why the higher level of the safety control structure allowed or contributed to the loss. Leveson claims that most accident reports include some of the higher level-factors, but the factors are often described incompletely and inconsistently. Stopping after finding the lower level flaws in the safety control structure of the loss is common in accident investigation. Leveson exemplifies this stage by four headlines to analyse and describe each actor in the control structure:

- Safety-related responsibilities: what is the relevant safety tasks the actor has?
- Context: why did not or could not the person act differently?
- Unsafe descriptions and control actions: dysfunctional interactions, failures, flawed decisions etc.
- Process model flaw, flaws in feedback, algorithm, reference channel and inadequate communication or interface models.

4.2.8 Stage 7: Examine coordination and communication

Analysing and understanding how coordination and communication between technical or human controllers may be a source of unsafe behaviour. A controlled process that has several controllers may lead to confusion about who is responsible, and the coordination must be clear and unambiguous. Examples can be several actors testing the same sample, technical and human controls on the same component or break down in the coordination and communication over time.

4.2.9 Stage 8: Changes to the safety control structure over time

CAST recognises that many major accidents are a result from mitigation of the system toward reduced safety margins over time. Often there are precursors like minor incidents and accidents that can be interpreted as a warning signs about the increased risk associated with the changes. CAST exemplifies the dynamics in the safety control structure by the influence recent accidents or incidents have on behaviours. If the safety efforts are successful and a feeling grows that accidents cannot occur, this may lead to a reduction in the safety efforts and the system drifts back to an unsafe state and complacency increases.

This stage is analysing whether there has been a drift towards a reduced safety margin over time. Is the financial and competition situation healthy, or is it necessary to take risks to survive? Is it possible to keep safe operations and fulfil requirements from management? Is the safety record good, and has the guard been lowered slightly over time?

4.2.10 Stage 9: Generate recommendations

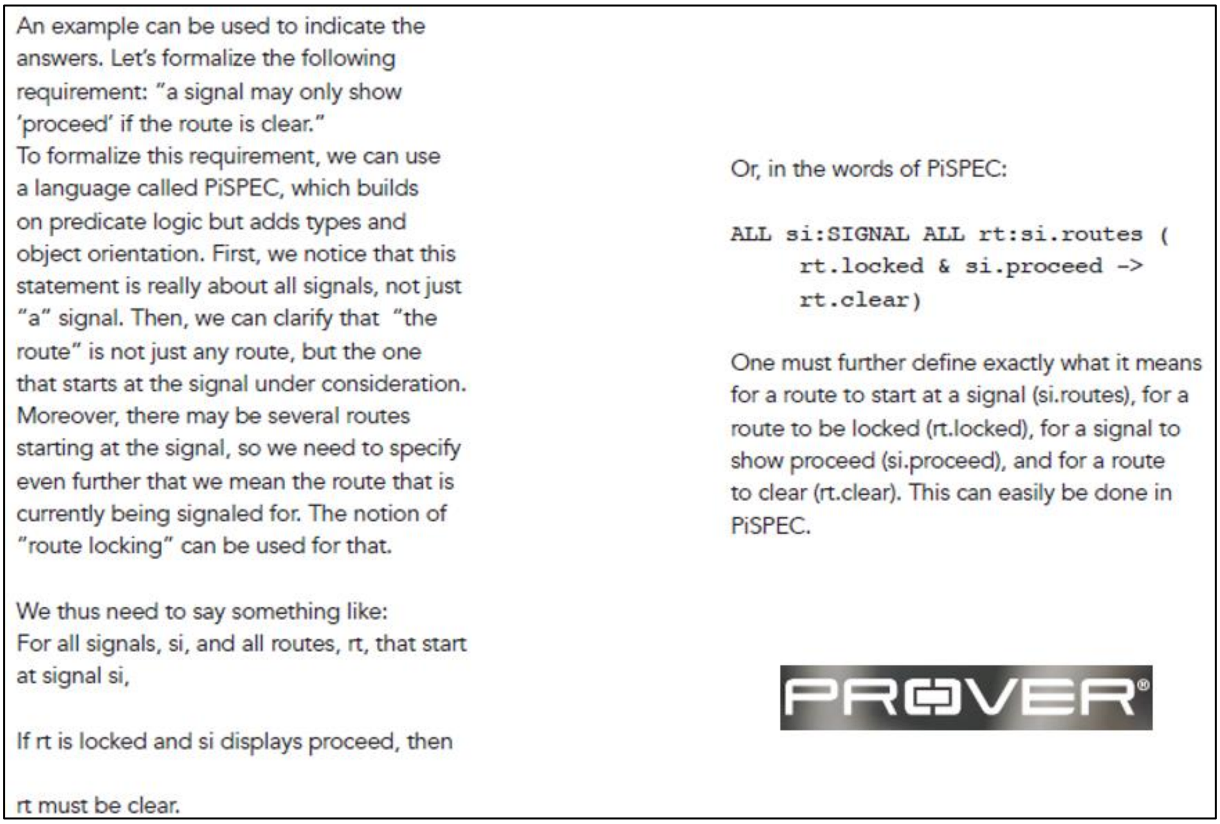
CAST clearly recommends to not assign blame or determine who is responsible for the accident. Blame can ruin a good reporting culture, and might be addressed to those with the least politically powerful positions in the control structure. The goal of an accident investigation should be maximum learning to prevent future losses. This might include change or reengineering the entire safety-control structure. If there are many recommendations there should be a determination of the most important actions that may have the greatest impact on future accidents.

4.3 Formal methods

Formal methods is relevant when software is at question in an investigation, because the methods have previously been successfully used during software development. The criticism against using formal methods are that they can be ambiguous and hard to analyse. The report discussed earlier by Qureshi [34] has a chapter where formal methods and accident investigation is reviewed, and presents a detailed description that has been a great source of information for this thesis.

Formal methods uses a specific language to provide a rigorous and systematic framework for the specification, design and verification of computer systems. The formal verification is made possible by establishing formal mathematical models of safety requirements, functional specification and program code, and using a suitable analysis tool (e.g. automated theorem prover) to verify relationships between them. In order to improve the precision and reasoning about certain aspect of accidents (e.g. software), formal accident model may be used.

Formal methods are mathematically-based techniques to prove the correctness of computer systems. The methods use a specific language (e.g. Boolean equations) and rules to precisely define notations for consistency and correctness for the specification and implementation of hardware and software system, see example in figure 27. The methods can be used to model the behaviour of a system and verify that the specification is implemented correct, in addition to identify specification and design errors. The most common area for using formal methods has been within the early stage of the system development [34].



An example can be used to indicate the answers. Let's formalize the following requirement: "a signal may only show 'proceed' if the route is clear."
To formalize this requirement, we can use a language called PiSPEC, which builds on predicate logic but adds types and object orientation. First, we notice that this statement is really about all signals, not just "a" signal. Then, we can clarify that "the route" is not just any route, but the one that starts at the signal under consideration. Moreover, there may be several routes starting at the signal, so we need to specify even further that we mean the route that is currently being signaled for. The notion of "route locking" can be used for that.

We thus need to say something like:
For all signals, si, and all routes, rt, that start at signal si,

If rt is locked and si displays proceed, then

rt must be clear.

Or, in the words of PiSPEC:

```
ALL si:SIGNAL ALL rt:si.routes (
     rt.locked & si.proceed ->
     rt.clear)
```

One must further define exactly what it means for a route to start at a signal (si.routes), for a route to be locked (rt.locked), for a signal to show proceed (si.proceed), and for a route to clear (rt.clear). This can easily be done in PiSPEC.

Figure 27: Example from Prover on the formalisation of requirements. Source: Prover.com.

The Why-Because Analysis is an example on a formal accident model, and the method has demonstrated benefits in a number of case studies in aviation and train accidents [34]. In 1994 Thomas used a first order logic to formalise software code, and used it to identify the underlying cause of unexpected behaviour in the Therac-25 radiation machine. An automated theorem prover called Larch Prover was used to reason about the behaviour of the code. In 2003 Vernez et al. demonstrated that Petri nets are able to model complex events by identifying the cause to consequence relationship.

In Qureshi’s review he concludes that formal methods have limitations in scalability to model complex sociotechnical systems, they need specialists in mathematics and it is difficult to formalise every aspect of an accident.

The Joint Software Systems Safety Handbook (JSSSH) from 2010 [49] is somewhat critical to the use of formal methods and states that “*Formal proofs of correctness are appropriate only for small but critical software or when mandated by Government regulations or standards*”. The handbook report issues such as formal methods are not able to identify missing requirements or changes to design that are new or network-based. It states that assuring that the object code generated by the compiler and implemented on the processor is correct or not also requires another formal method. In addition the report states that the complexity of systems, modern processors and features such as interrupts and exception handling makes formal assessment difficult.

4.3.1 ERTMS and formal methods tools

In January 2015 [50] a grant agreement between the Innovation and Networks Executive Agency and the ERTMS Users Group was initiated. The aim is to help the railway companies with technical and operational matters and guidance on commercial implications and impact.

ERTMS Solutions has developed the tool ERTMSFormalSpecs (EFS), to formally model ERTMS requirements for train borne and trackside systems. The tool aims to model test scenarios, change requests, management, analysis of requirements, traceability etc.

Another initiative that has developed a tool for the implementation of ETCS is the openETCS project [51]. The project is a European consortium funded by the ITEA2 program, and consists of 30 contributing companies. The main goal of the project was to develop a framework that provides a formal method tool for the development of ETCS software. Deutche Bahn is expecting to reduce the cost of procurement and installation per onboard-unit from 350.000 to 100.000 Euros per unit, in addition to reducing the annual software maintenance costs. More information on the benefits from this project can be found on the ITEA webpage [52].

4.3.2 Norwegian experience with formal methods

Bane NOR is a state-owned infrastructure manager for the Norwegian railway infrastructure. Terje Sivertsen, chief engineer at Bane NOR, has provided a detailed description of the experience they have on the use of formal methods during the development of the proprietary signalling system called NSB-94 (Annex A). The system is based on older relay-based signalling systems (NSI-63), but the interlocking logic is implemented in PLC software instead of relays.

For the NSB-94 signalling system the infrastructure manager formulated all safety-related functional requirements in one document. The infrastructure manager used the Swedish company Prover to perform the formal verification analysis, based on a patented method. This was done by establishing formal mathematical models of safety requirements, functional specification and program code.

The Boolean equations in the functional and design specification gives a correlation between the equations and program code. This makes it possible to verify that the program code is a correct implementation of the function specifications.

4.3.3 Formal methods in accident investigation of signalling systems

The “ordinary” investigation team should be able to analyse if the signalling system contributed to the accident or not. It might be a difficult task to “prove” that the signalling system works correctly or not, as the system might be complex to understand. When investigating a signalling system the methods used when procuring or developing the signalling system will be relevant. If the development process has followed the CENELEC standards, then looking back at the functional steps in figure 9 might be a good place to start. An evaluation of these steps should be evaluated to decide if they also can be used for the investigation.

Two important questions must be addressed when investigation a software system.

- Are the right requirements specified for the system?
- Does the system fulfill the requirements?

By focusing on these two questions Terje Sivertsen has proposed a combination of questions before a formal method is applied to the analysis, see figure 28 (larger version in Annex E). If a deficiency is found during the analysis it might be sufficient to stop further analysis of the software system.

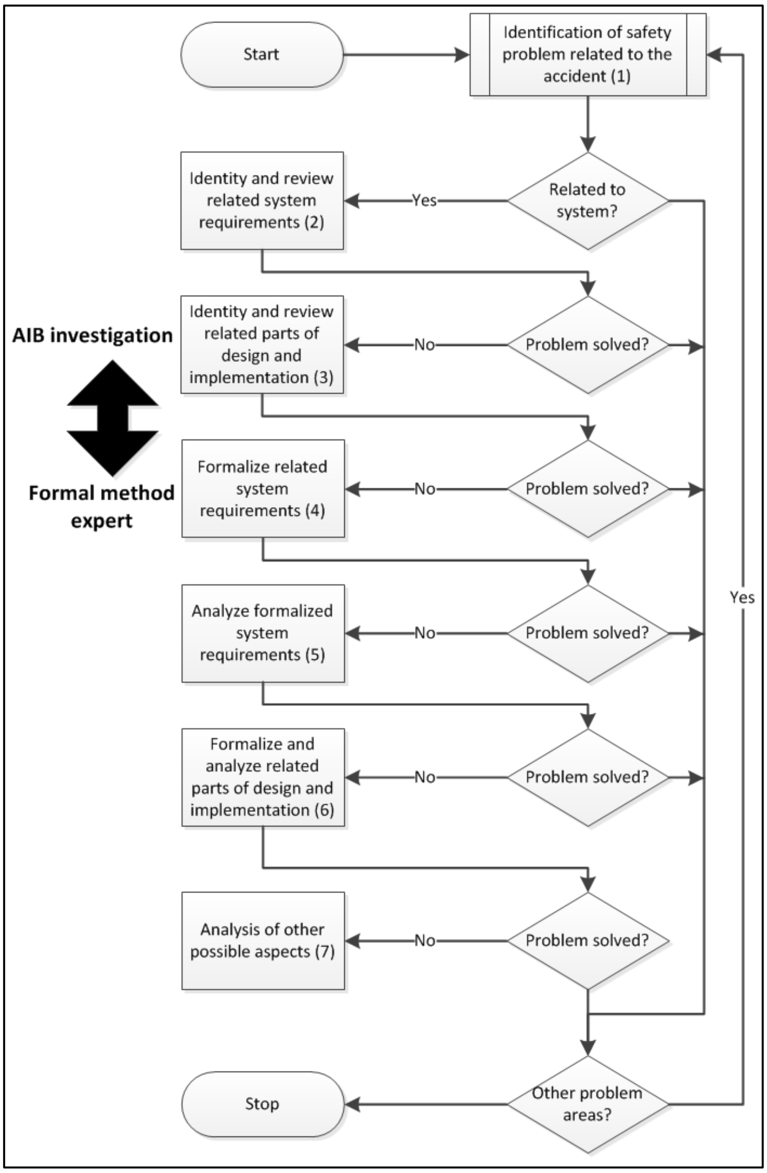

Start
Identification of safety problem related to the accident (1)
Related to system?
Yes
Identity and review related system requirements (2)
Problem solved?
No
Identity and review related parts of design and implementation (3)
AIB investigation
Formal method expert
Formalize related system requirements (4)
Analyze formalized system requirements (5)
Formalize and analyze related parts of design and implementation (6)
Analysis of other possible aspects (7)
Other problem areas?
Stop
Yes

Figure 28: Flowchart of the investigation process of software. Source: Terje Sivertsen.

1. The initial investigations should identify safety problems (e.g. AIBN-method stage 2).
2. Identification of the system requirements for the safety problems. The investigation team will narrow down the scope of the system requirements that are scrutinised. The team will most likely be able to form an opinion on the requirements for the safety problem. If the requirements are not specified correctly the analysis can stop.
3. Identification of the specifications of the design and implementation for the safety problem. If the system requirements are correct, the next step is to see how they are specified in the design and implementation documents. The investigation team will normally be able to narrow down the scope of the design and implementation requirements that are scrutinised. The team will most likely be able to form an opinion

on the requirements for the safety problem. If the requirements are not specified correctly the analysis can stop.

4. If it is complex or unclear at this stage, a formal method may be used to formalise the current system requirements. Expert help will most likely be required for the formalisation of requirements. This will lead the investigation from a qualitative point of view to a mathematical setup of absolutes. The formalisation of the system requirements may be sufficient to reveal any shortcomings in the foundation of requirements.
5. The next level could be to analyse the formalised requirements with regard to whether they meet expected invariant properties.
6. If the analysis of the formalised specification does not reveal any deficiency, a formalisation of the design and implementation will be the next step. This will be used to verify the specifications of the design and implementation against the formalised specification of requirements. This is a labor intensive process and it is important that the scope of the analysis is pinpointed at the requirements and design around the safety problem. This may also be analysed by the supplier, who should have a great interest in finding the cause and correct it. In order to perform this analysis the supplier's documentation of design and implementation of program code is needed. A cooperation should be established and the role of the investigation team is to make sure the surveys are objective and systematic to provide credibility.
7. If the analysis has not revealed any shortcomings at this point, it will be appropriate to identify alternative safety problems to analyse.

In many cases it is expected to find shortcomings in the first steps regarding system requirements or the fulfilment of the requirements [53]. If this is the case it will be an important safety lesson that can be highlighted and explained in the investigation report in order to propose safety recommendations.

The U.S. Department of defence, Joint Software Systems Safety Engineering Handbook (JSSSH - 2010), is a guideline in management and engineering of software safety. The handbook is describing the desired minimum qualification for personnel assigned to perform the software safety portion of the system safety:

> *“Undergraduate degree in engineering or technically-related subject (e.g., chemistry, physics, mathematics, engineering technology, industrial technology, or computer science)*
> *System safety management course*
> *System safety analysis course*
> *Software safety engineering course*
> *Software acquisition and development course*
> *Systems engineering course*
> *Two to five years’ experience in system safety engineering or management.”*

This JSSSH minimum qualification can be a guide when considering the competence needed for personnel performing a software investigation.

5 Application of the methods

In this chapter a case example is applied to the AIBN-method and CAST-method in order to demonstrate how the methods are used to analyse the case example. The case example is not used for the formal method demonstration, instead a flowchart and a series of questions is proposed to guide the investigation to systematically start a process towards the possible use of formal methods.

Disclaimer: The application of the following methods should be regarded as an attempt to demonstrate the steps in the two methods, and not as a representative investigation result. The official investigation result will be published by the RAIB.

5.1 The case example

From the RAIB interim report [41]:
“*On 20 October 2017, during a conversation with the controlling signaller, a train driver advised that the maximum permitted speed shown on his in-cab display was not taking account of temporary speed restrictions. This occurred on the Cambrian lines in Wales where permitted speeds are transmitted to trains by a signalling system installed as a trial for the future deployment of in-cab signalling on other parts of Network Rail infrastructure. Subsequent*

investigation found that temporary speed restriction information had not been provided to trains in the area since the previous evening."

5.2 Applying the AIBN-method

This section aims demonstrate the use of the 7 stages in the AIBN-method for the accident analysis process. The theoretical background for method is explained in chapter 4.1.

Usually an AIB investigation will be managed by an accident inspector with access to required expertise, and the time to perform more in-depth analysis than in this case example. The AIBN-method is an iterative process and the stages have been reconsidered and changed several times before it ended up as it is shown in this thesis.

The case example presented in this thesis is based on a real occurrence on the Cambrian lines in Wales on 20 October 2017 and the interim report by the RAIB [41]. The information used to demonstrate the AIBN-method is mainly from the interim report and a meeting with the RAIB in January 2019.

5.2.1 Stage 1: Clarifying the sequence of events and circumstances

To understand and describe what happened in the accident the AIBN-method recommends to use a simple time line with the most important events and actions in chronological order. The description starts at a point when the transport was functioning normally, and stops when the accidental event is under control. In figure 29 the actors are listed on the right side, and the events and actions are described by the square boxes. The red star is defined as the accident, and represents the undesired event. Table 1 is listing the sequence of events.

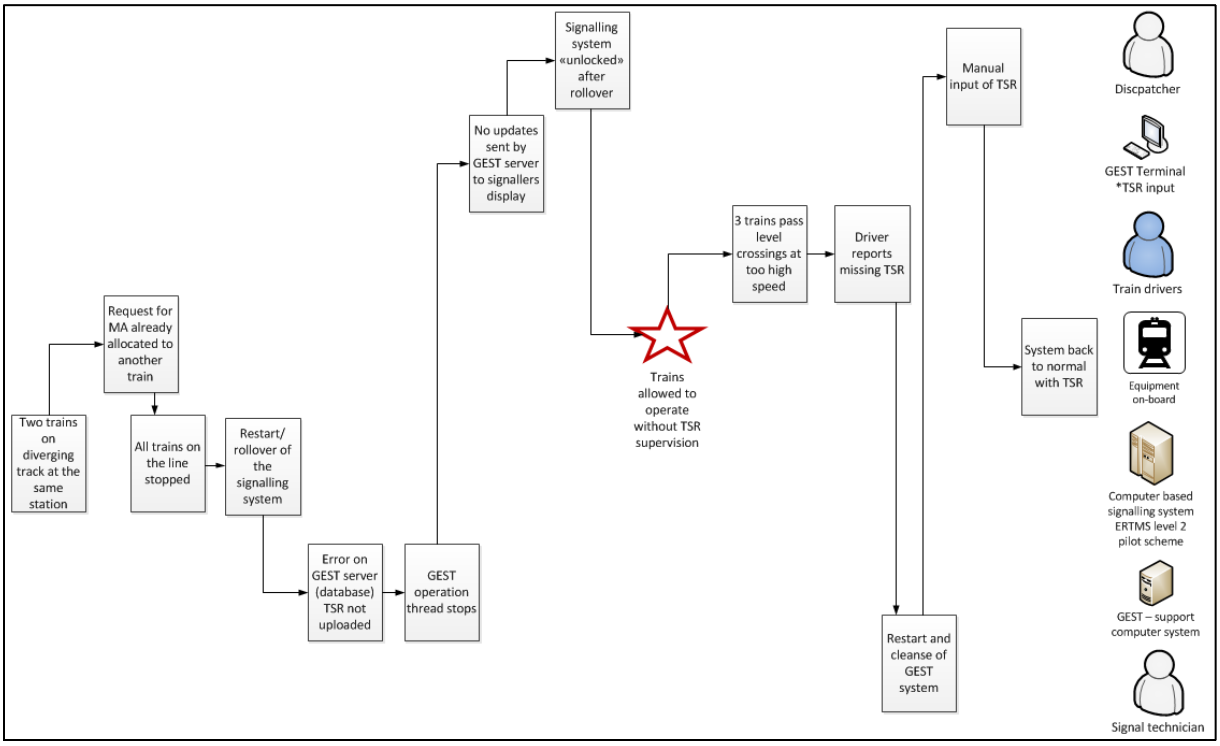

Two trains on diverging track at the same station
Request for MA already allocated to another train
All trains on the line stopped
Restart/ rollover of the signalling system
Error on GEST server (database) TSR not uploaded
GEST operation thread stops
No updates sent by GEST server to signallers display
Signalling system «unlocked» after rollover
Trains allowed to operate without TSR supervision
3 trains pass level crossings at too high speed
Driver reports missing TSR
Restart and cleanse of GEST system
Manual input of TSR
System back to normal with TSR
Discpatcher
GEST Terminal *TSR input
Train drivers
Equipment on-board
Computer based signalling system ERTMS level 2 pilot scheme
GEST – support computer system
Signal technician

Figure 29: Stage 1. Clarifying the sequence of events and circumstances.

Table 1: Sequence of events.

Actor	**Event or action**
Signalling system	Two trains at diverging track at the same station. This is starting point where the transport process was functioning normally.
On-board equipment	The train on-board computer requested a movement authority already allocated to another train.
Signalling system	Stopped movement authorities being given to trains and restarted the system as a defensive response.
Signalling system	The request triggers an automatic software reset (rollover), due to a logic mishap in the signalling system handling MA on diverting tracks. Rollovers occur 10-12 times a year.
GEST	During the rollover an error on the GEST server was "activated" and stopped the transmission of Temporary speed Restrictions (TSR).
GEST	The missing transmission of TSR was not detected and the system status indicating that everything was ok. However the status is wrong because there is a mismatch between the TSR in the database and the status sent to the GEST screen.

GEST terminal	No updates sent by GEST server to signallers display. GEST terminal display green flags, indicating all is ok with TSR upload.
Dispatcher	Unlocks the signalling system on the GEST terminal after checking that flags are green.
On-board ☆	Temporary speed Restrictions (TSR) are not transmitted to the trains
Train driver	Drivers do not notice missing speed restrictions. 3 trains pass level crossings at too high speed.
Train driver	Driver of train 2J03 noticed the missing TSR and reported a fault with the speed restriction.
Signalling staff	After several unsuccessful attempts to reload the database, the fault was reported to Ansaldo STS. Ansaldo STS advised the signalling technician to cleanse data from the signalling system. During this cleanse the GEST server logs were deleted and information important to understanding the incident was lost.
GEST	All temporary speed restriction information was manually re-entered into the support computer terminal.
On-board Train driver	Correct indication of the temporary speed restrictions on the in-cab displays. This was verified by a test train driver.

5.2.2 Stage 2: Identifying local safety problems

The local safety problems are visualised with numbered red triangles and placed on the event or action in the sequence of events, see figure 30. The identified problems will be investigated deeper at later stages in the analysis.

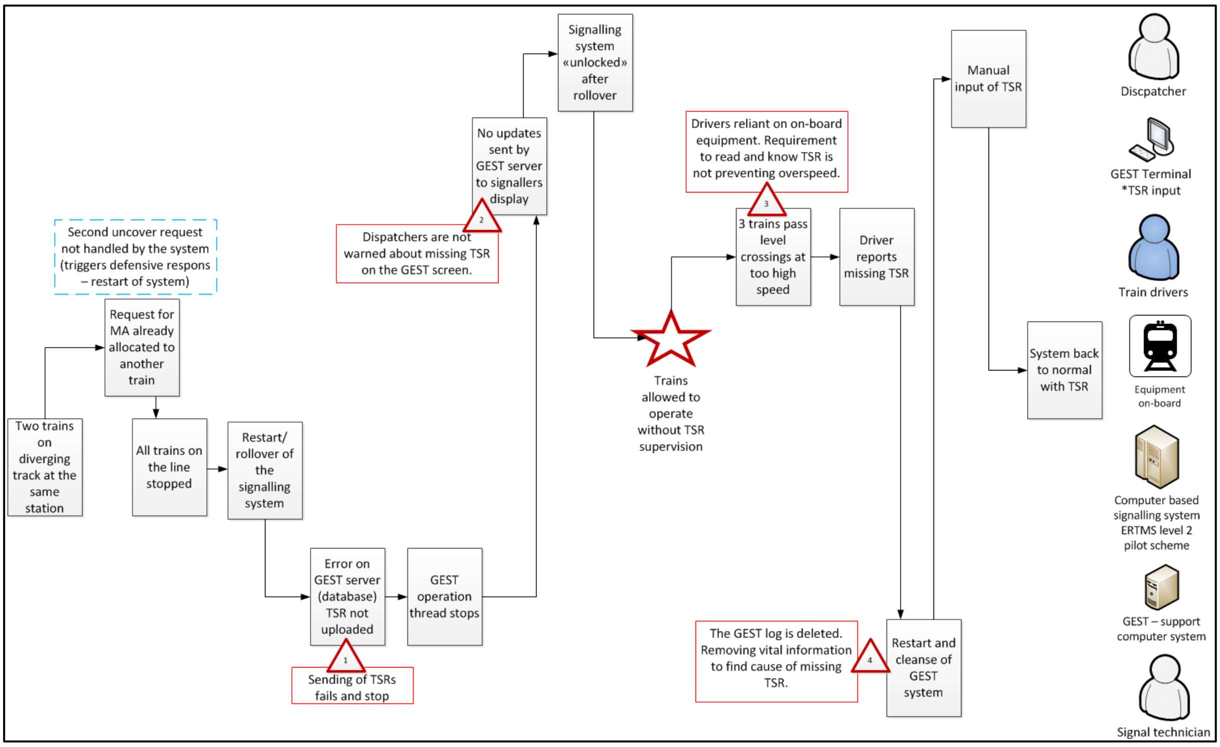

Signalling system «unlocked» after rollover
No updates sent by GEST server to signallers display
2
Dispatchers are not warned about missing TSR on the GEST screen.
Second uncover request not handled by the system (triggers defensive respons – restart of system)
Request for MA already allocated to another train
Two trains on diverging track at the same station
All trains on the line stopped
Restart/ rollover of the signalling system
Error on GEST server (database) TSR not uploaded
1
Sending of TSRs fails and stop
GEST operation thread stops
Drivers reliant on on-board equipment. Requirement to read and know TSR is not preventing overspeed.
3
3 trains pass level crossings at too high speed
Driver reports missing TSR
Trains allowed to operate without TSR supervision
Manual input of TSR
System back to normal with TSR
The GEST log is deleted. Removing vital information to find cause of missing TSR.
4
Restart and cleanse of GEST system
Discpatcher
GEST Terminal *TSR input
Train drivers
Equipment on-board
Computer based signalling system ERTMS level 2 pilot scheme
GEST – support computer system
Signal technician

Figure 30: Stage 2. Identifying local safety problems marked with red triangles in the figure.

The safety problems are numbered and described in the table 2 below. The description of the event that triggered the restart is also included. The triggering event is a defensive response, and did not cause the error on the GEST server. It is therefore not listed as a safety problem that will be handled in the analysis. However the restart “activated” the error on the GEST server that stopped the transmission of TSR.

Table 2: Local safety problems.

No.	Local Safety problems
-	Second uncover request not handled by the system (triggers defensive response – restart of system). This conflict had been detected earlier and the software modification was awaiting validation.
1	An error on the GEST server stops the TSR function and the transmission of the speed restrictions.
2	Dispatchers are not warned about missing TSR on the GEST screen.
3	Drivers reliant on on-board equipment. Requirement to read and know TSR is not preventing over speed.
4	The GEST log was deleted and removed vital information that could have assisted in finding the cause of missing TSR faster and easier. One of the

	reasons the RAIB was involved was because Ansaldo could not explain why the TSR was missing. After the RAIB was involved a replica system was established, and the condition that caused the error was possible to recreate. Without the log or replica system explaining what went wrong, and showing the lack of monitoring on the GEST communication thread, this error might have occurred again.

5.2.3 Stage 3: Barrier analysis

The barrier analysis is visualised with blue rectangles marked with letters and placed between the event or action in the sequence of events in figure 31. The description of the barrier and the flaw in the barrier is listed in table 3

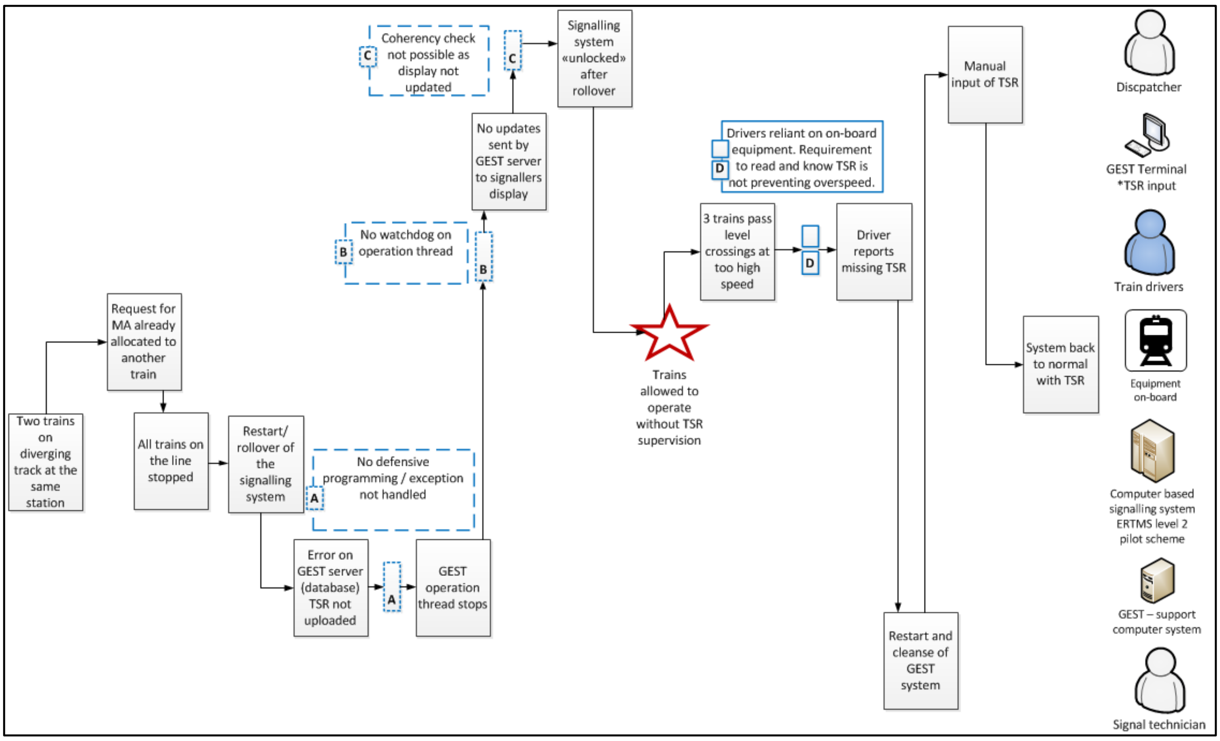

Coherency check not possible as display not updated
C
C
Signalling system «unlocked» after rollover
No updates sent by GEST server to signallers display
No watchdog on operation thread
B
B
Request for MA already allocated to another train
Two trains on diverging track at the same station
All trains on the line stopped
Restart/ rollover of the signalling system
No defensive programming / exception not handled
A
Error on GEST server (database) TSR not uploaded
A
GEST operation thread stops
Drivers reliant on on-board equipment. Requirement to read and know TSR is not preventing overspeed.
D
3 trains pass level crossings at too high speed
D
Driver reports missing TSR
Trains allowed to operate without TSR supervision
Manual input of TSR
System back to normal with TSR
Restart and cleanse of GEST system
Discpatcher
GEST Terminal *TSR input
Train drivers
Equipment on-board
Computer based signalling system ERTMS level 2 pilot scheme
GEST – support computer system
Signal technician

Figure 31: Stage 3. Barrier analysis. Marked by blue rectangles.

The following definition of barrier is used in the AIBN-method:

"*Technical, operational or organisational measures that separately or together could have prevented or stopped the sequence of events in question, or limited the consequences of the accident.*"

Table 3: Barrier and flaws.

Item	Barrier	Flaw
A ⬚	Detection and handling of errors on the GEST server database.	No defensive programming / exception not handled
B ⬚	Monitoring of the operations thread on the GEST server.	No watchdog on operation thread.
C ⬚	Check that the GEST screen display correct information.	Coherency check not possible as display not updated.
D ⊟	Drivers detect missing information on the train monitor.	Drivers are too reliant on on-board equipment (complacency)? Requirement to read and know TSR did not prevent over speed.

▯ Barriers that were in place and worked.

⊟ Weaknesses and failings in existing barriers.

⬚ Barriers that had not been established at the time of the accident (both barriers that should have been and that could have been established).

5.2.4 Stage 4: Identifying risk factors

Stage 4 and 5 are the causal analysis of the investigation, and should identify connections between the sequence of events and the risk factors. This stage should study the risk factors and be able to explain and understand how and why the safety problems were present. The analysis should also explain how and why safety systems or barriers were lacking or not working as intended.

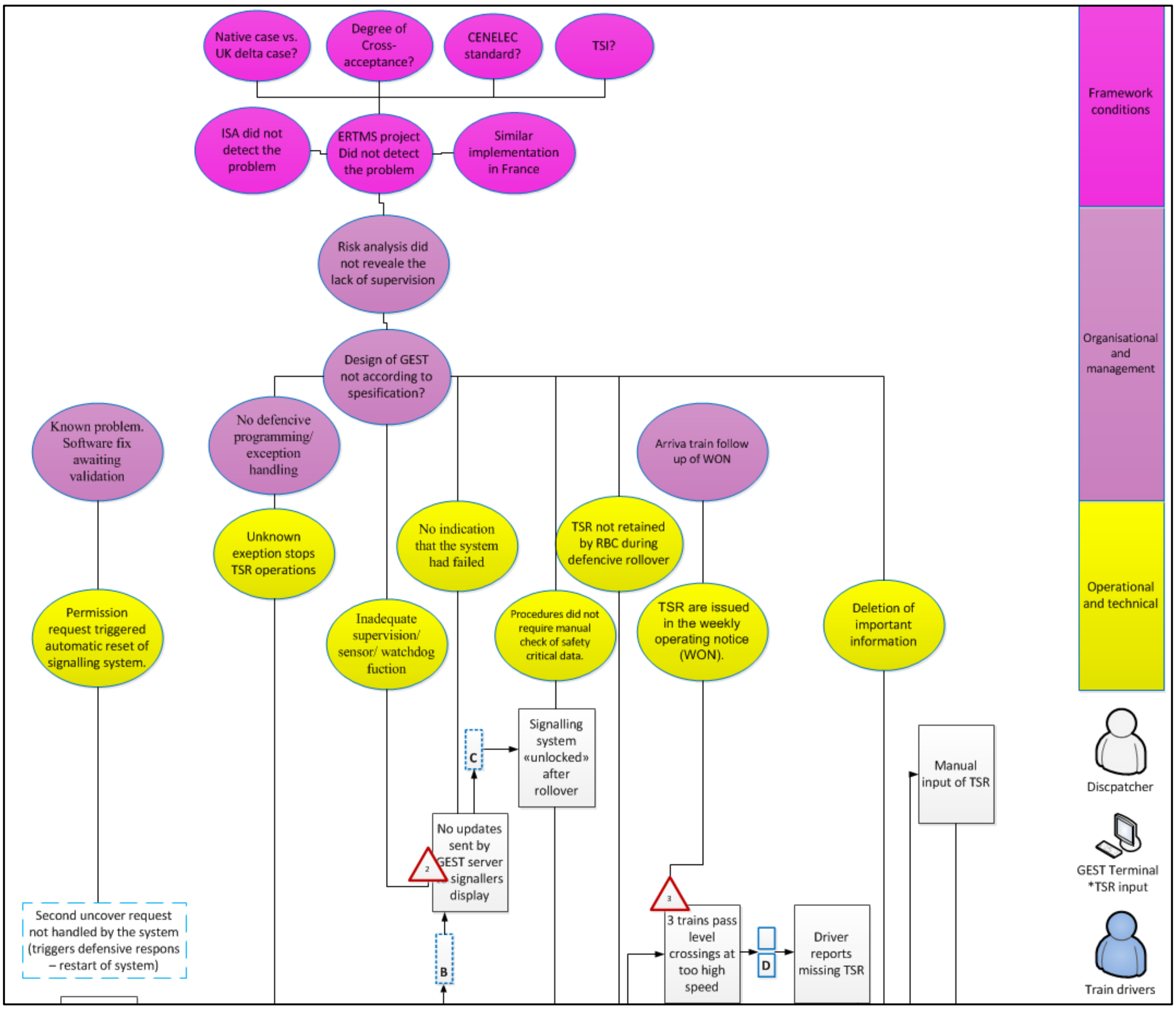

Native case vs. UK delta case?
Degree of Cross-acceptance?
CENELEC standard?
TSI?
ISA did not detect the problem
ERTMS project Did not detect the problem
Similar implementation in France
Risk analysis did not reveale the lack of supervision
Design of GEST not according to spesification?
Known problem. Software fix awaiting validation
No defencive programming/ exception handling
Arriva train follow up of WON
Unknown exeption stops TSR operations
No indication that the system had failed
TSR not retained by RBC during defencive rollover
Permission request triggered automatic reset of signalling system.
Inadequate supervision/ sensor/ watchdog fuction
Procedures did not require manual check of safety critical data.
TSR are issued in the weekly operating notice (WON).
Deletion of important information
Signalling system «unlocked» after rollover
C
Manual input of TSR
No updates sent by GEST server signallers display
2
3
3 trains pass level crossings at too high speed
D
Driver reports missing TSR
B
Second uncover request not handled by the system (triggers defensive respons – restart of system)
Framework conditions
Organisational and management
Operational and technical
Discpatcher
GEST Terminal *TSR input
Train drivers

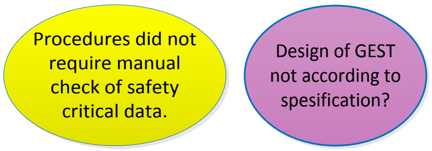
Figure 32: Stage 4. Moving up in the analysis and identifying risk factors.

Stage 4 identifies the risk factors and stage 5 evaluates the existence, influence and importance of each risk factors. The risk factors in figure 32 are identified from the sequence of events and risk factors displayed in the previous figures, and explained in more detail in the next chapters. They are found by asking how the system could accept, or had not identified, the accident risk. Some factors do not necessarily have a clear cause-and –effect relationship, but are considered to increase the risk of an accident. The result of the information in figure 32 is based on the

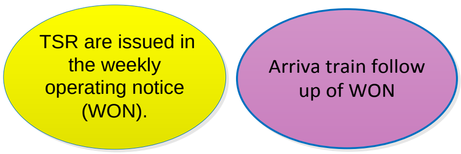
RAIB interim report [41], meeting with the RAIB and some assumptions. The connection between stage 4 and 5 is important with regard to how much effort is put into the investigation of the risk factor. If it turns out that a described risk factor actually did not contribute to the accident, it must be clearly stated in the report. The analysis at this stage may require more resources and also a need to hire expert help to perform a "sub-investigation". Examples could be use of psychologist for human factors or testing, simulating, reconstructing or examining equipment. The result from testing the replica system in the lab is used in this stage. As an alternative to the replica system formal methods could have been used as a technique, but it was not possible to get access to the required information to perform a formal method for the GEST system. The use of formal methods which is described earlier in chapter 4.3 fits into the AIBN-method at this stage. The expected learning effect from describing the details of the risk factor must be evaluated against the resource and time required.

The identified risk factors are categorised by three different colours according to the various levels in the sosio-technical system based on the work of Rasmussen [31]. The AIBN-method [27] offers a guidance in analysing the dimension of risk factors in the structure as described in the headlines below (chapter 4.1.4):

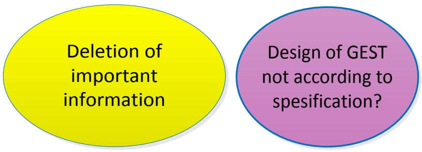
5.2.4.1 Human factors


Procedures did not require manual check of safety critical data.
Design of GEST not according to spesification?

Software rollovers occur 10-12 times a year at the Cambrian line and the signalling staff followed their established procedures for returning to normal services. The procedure at the time did not specify any extra control or check of the TSR data. When the procedure was written there was an assumption that the status on the GEST screen always was accurate and correct. After the TSR was discovered to be missing, the signalling staff controlled and confirmed to Ansaldo that the restriction flag at the GEST terminal was green. *The signalling staff acted as expected and in accordance with the established procedure.*


TSR are issued in the weekly operating notice (WON).
Arriva train follow up of WON

The drivers should be aware of the TSR which are issued in the weekly operating notice (WON). On traditional lines the TSR is also marked by trackside signs, but on the Cambrian ERTMS line the TSR is displayed on-board the train. Three trains passed level crossings without reporting the missing TSR. It was the driver of the fourth train that first reported a fault with the TSR provided to him in the in-cab display. However this barrier is considered as weak, because this case shows the first drivers did not detect the missing TSR. This must be expected for manual procedures, and if the risk for accidents is high there should be other means than manual procedures to prevent an accident. One could argue that the barrier worked because the fourth driver was the one discovering the missing TSR, but there could also have been a level crossing accident with one of the over speeding train. Even though it is considered a weak barrier, it is not considered as useless and should be used with caution. *Three drivers did not act as expected according to the WON, the fourth driver discovered the missing TSR.*


Deletion of important information
Design of GEST not according to spesification?

In an attempt to resolve the missing TSRs, data was cleansed from the system, and information stored in the system memory and associated databases were deleted. The logs were not saved, and it was indicated that the signalling staff believed they did not contain any important information. The thesis has not had access to information regarding this issue, and some unanswered questions remain.

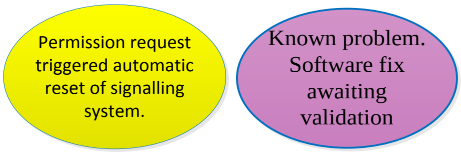
- How was the staff trained or informed about the information in the logs?
- Why was there no automatic copy and storage of the logs?

During the initial internal investigation Ansaldo STS were hampered by having only limited data from the time shortly before and following the rollover. This could be a safety problem if the cause of the problem is not found due to missing information. If the error is not found and corrected, the problem might keep occurring until it causes a major accident or loss, and the public demand to find the cause is a pressing issue.

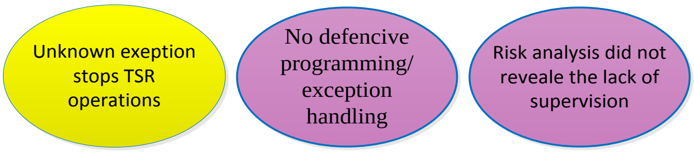
5.2.4.2 Technical factors

In this investigation the technical factors concerning the GEST system have been given comprehensive attention, as it was quickly established as a vital system in the incident. In the beginning of the investigation there were no explanation on how the missing TSR had occurred. When the RAIB entered the investigation Ansaldo set up a replica GEST system in a lab to test different conditions. The main goal was to test if it was possible to recreate the missing TSR and produce green flags on the GEST terminal. The replica system was able to recreate the missing TSR and green flags, and a weakness in the communication thread on the GEST server was found.

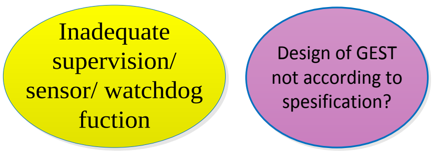
Setting up a replica system for testing has proven to be one possible way of finding the weakness in this investigation. Another possible way of investigating the weakness in a software system is to use formal methods. The use of formal methods is explained in chapter 4.3 and 4.3.3.


Permission request triggered automatic reset of signalling system.
Known problem. Software fix awaiting validation

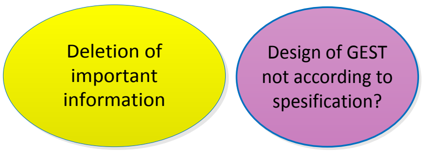
The first events that started the chain of events was an automatic requested for an updated movement authority (MA) by a train at the Cambrian line. The requested MA was already allocated to another train, and not released as it should have been at the diverging junction. This triggered an automatic reset, known as a rollover, in the computer based signalling system controlling the Cambrian lines. The rollover is a defensive mechanism in the signalling system when something unexpected or unforeseen occurs. *The signalling system acted as expected by triggering a rollover/ reset as a defensive mechanism.*


Unknown exeption stops TSR operations
No defencive programming/ exception handling
Risk analysis did not reveale the lack of supervision

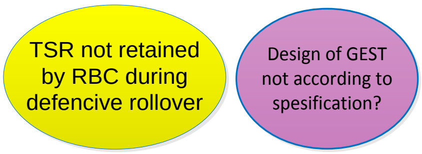
In this specific reset safety critical data, i.e. the temporary speed restrictions (TSR), were not correct reloaded into the signalling system. The communication thread on the GEST server failed due to an unexpected exception on the server. The error stopped the transmission of TSR, and the automatic logic to restore TSRs actually removed the TSRs from the RBC that is sending the information to the trains. The unexpected exception was not foreseen and therefore not handled by defensive programming or exception handling operations. RAIB states that during the investigation of the SRS it was evident that this situation was not foreseen as there were no requirement for dealing with this situation, because the mitigation relied on the GEST system operating correctly. *The GEST server did not operate as expected, because it stopped working without a proper system to notify about errors.*


Inadequate supervision/ sensor/ watchdog fuction
Design of GEST not according to spesification?

The TSR was stored in the GEST server, and the signalling staff used a GEST computer terminal to apply the TSR on the Cambrian line. The GEST system had a status indicator using coloured flags to confirm the status of the TSR. If a TSR was uploaded from GEST to the signalling control system a green flag should be displayed on the GEST terminal. If the TSR was not available to the signalling control system due to an error, the flag should be red and all trains stopped from operating. However there were no watchdog function that supervised this operation, hence the red flag function was inadequate. The error stopped the update of information from the GEST server to the GEST terminal screen. This also stopped the communication between the RBC and the GEST server. The GEST terminal however displayed green flags, and allowing the signallers to "unlock" the signalling system. The problem was that the "old" status was not updated because of the unknown exception, and therefore the terminal displayed the green flags based on wrong information. *The watchdog functions did not operate as expected as green flags were displayed to the staff on the terminal when the system was in an error state.*


Deletion of important information
Design of GEST not according to spesification?

After several attempts to resolve the problem with missing TSRs, data were cleansed and deleted from the GEST system. Following the cleanse TSR data was manually input into the GEST system again. During the investigation performed by the supplier Ansaldo they found very limited data from the time before and following the initial rollover. This was a result from data being deleted from the system memory and associated databases. The deleted data could have assisted in finding the cause of the incident, and Ansaldo might not have needed to create a replica system to test in a lab. The GEST log was required during development of the Cambrian ERTMS, and no longer a required functionality in operations. The log function had not been removed and it was fortunate, but not planned, that the log was available to assist the RAIB investigation. *The storage of log data was not expected to be provided.* The relevant event logs and databases should be stored or copied automatically to a safe location to prevent loss of important data.


TSR not retained by RBC during defencive rollover
Design of GEST not according to spesification?

During a restart the TSR memory in the RBC server will be lost. The validation of the GEST system was based on a similar system in Europe, but this system was not put in service at the time the Cambrian line was approved. Later the European system was changed from volatile memory to non-volatile memory. This change was not considered necessary on the Cambrian line because the signallers are required to check the GEST server for green flags and "unlock" the RBC after a restart. This decision indicates a lack of understanding of the systems function and latent single point of failure. *The RBC did not behave as expected because safety critical information was lost during a restart.*

5.2.4.3 Damage/injury and survival aspects

During the time the TSR was missing, the risk of a level crossing accident was increased. The highest speed violation was a level crossing with a speed limit on 30 km/h that was passed at 90 km/h. This significantly reduces the chances to detect the train at the level crossing, and also dramatically increases the brake distance for the train.

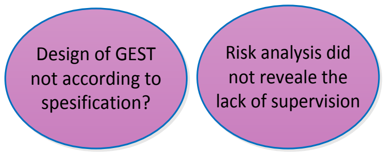
This incident did not have any physical damages, but due to the fact that it was not obvious what had happened there was a need to use considerable efforts investigating the case. The effort and resource use might have been reduced if the GEST server logs had not been deleted. A replica system of the Machmynllet control centre was set up and tested for different scenarios at a lab in France.

5.2.4.4 Organisational and management factors

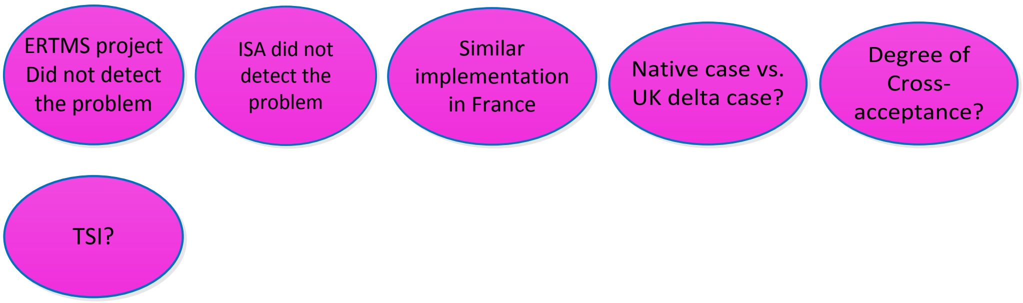
Most of the organisational and management factors are already mentioned in the human and technical factors. Some questions remain unanswered due to missing information:

- How did Arriva trains follow up that the information in WON was known to the drivers?
- How was the signalling staff trained and informed about the GEST system and logs?

5.2.4.5 Safety-related framework conditions


Design of GEST not according to spesification?
Risk analysis did not reveale the lack of supervision

The investigation has shown that the design of the system was a major problem in the incident. The next step is to find out why the flaw in the design was not discovered during the system development. The requirements and standards applicable for ERTMS systems are comprehensive and should prevent this type of flaw.


ERTMS project Did not detect the problem
ISA did not detect the problem
Similar implementation in France
Native case vs. UK delta case?
Degree of Cross-acceptance?
TSI?

The fact that the implementation on the Cambrian lines was being guided by on-going design for the French system might also have given the impression that the system was already comprehensively examined and safe to use. The GEST system was approved by the French state railways (SNCF) after approval for use on the Cambrian lines. In addition the European system was changed before it was put into service. Computer memory was not changed on the Cambrian line when this change was made to the French system. This change was not regarded as necessary for the Cambrian line. This information was not provided to the UK independent Safety Assessor, and they were not aware of this difference in the application.

The information provided by the Cambrian interim report has not provided enough information to go deeper into the framework conditions. Some questions remain unanswered, such as:

- The degree of cross acceptance, how much was regarded as specific for the Cambrian line?
- What parts of the CENELEC standards should have prevented this flaw?
- Should the TSI requirements have prevented this?
- Was there any problems in the ERTMS project?
- How was the risk analysis process managed in the ERTMS development project?
    - Did they follow the CENELEC standards?
    - What methods did they use?
    - What competence did the staff performing the risk analysis have?
    - Was any risk analysis skipped due to a mistaken belief that there was the European approval?

5.2.4.6 Systemic approach

The circle in figure 17 represents the systemic approach, and the AIBN-method do not give a comprehensive description of systemic methods, other than referring to other sources. The AIBN-method states that accidents in complex systems can be difficult to describe. If it is difficult to clarify the first stages in the AIBN-method, this might be an indication on a complex system. The systemic approach is however a complement to the AIBN-method, and not a replacement of the stages in the analytical process.

The study of systematic approaches to support the AIBN-method is one of the main reasons the topic of this thesis was selected. There are several systematic approaches available, such as FRAM, HFACS, STAMP and Accimap. In this thesis the systematic approach CAST which is based on STAMP was selected. See chapter 5.3 for description of how the case has been analysed by using CAST.

5.2.5 Stage 5: Assessing causality and importance

Step 5 is the documentation of the evaluation of which risk factors contributed to the accident, and are analysed in stage 4. In order to evaluate how much resources that should be used to investigate the risk factor, the causality and importance must be addressed. One way of systematically doing this is described in figure 33.

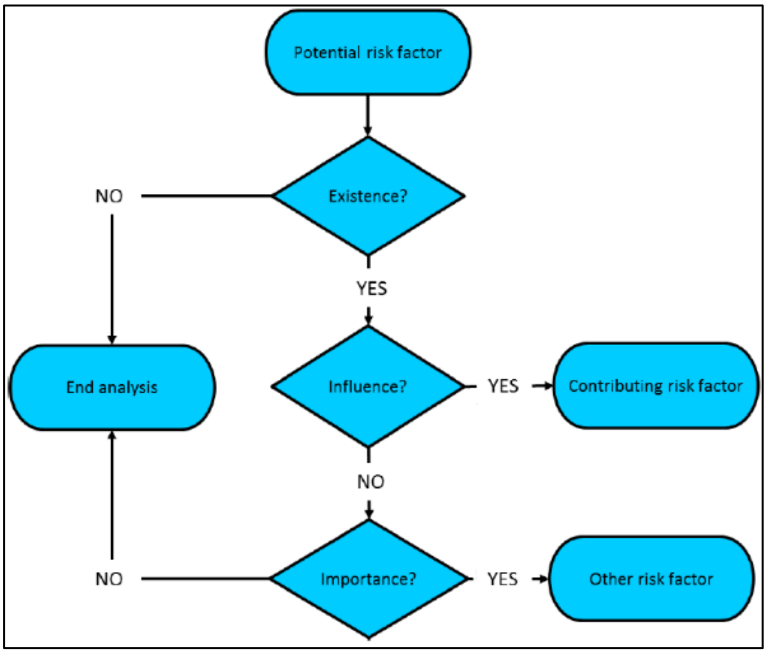


Figure 33: Stage 5: Testing potential risk factors. Source: ATSB, 2015.

Table 4 display the evaluation of some selected risk factors identified in the Cambrian line analysis in order to demonstrate the testing process, and do not include all risk factors identified.

Table 4: Evaluation of risk factors.

Potential risk factor	**Existence**	**Influence**	**Importance**	**Comment**
Automatic rollover/ reset of the ERTMS system	Yes	Yes	No	This is a defensive response that is expected to be a part of the system, and did not cause the error on the GEST server. It is therefore not considered as an important factor to investigate further.
Sending of TSRs fails and stop	Yes	Yes	Yes	This is an error that should have been detected and stopped the MA to trains until the operation was back and ok.
Dispatchers are not warned about missing TSR on the GEST screen.	Yes	Yes	Yes	This indicates that there is a logic error in the design of the system. Loss of speed restrictions is serious.
Drivers reliant on on-board equipment. Requirement to read and know TSR is not preventing over speed.	Yes	Yes	Yes	Screens with information that rarely fails is hard to detect for humans, and error detection should rely on technical means. However this is still a barrier, and the process to make sure drivers know the WON should be analysed.
The GEST log is deleted. Removing vital information to confirming the cause of missing TSR.	Yes	Yes	Yes	During the attempts to restore TSR, the GEST event log was deleted. The log contained information that could have helped finding the cause of the missing TSR. Event logs for safety critical systems should not be deleted after incidents, and why this happened should be analysed.

5.2.6 Stage 6: Considering systemic safety problems

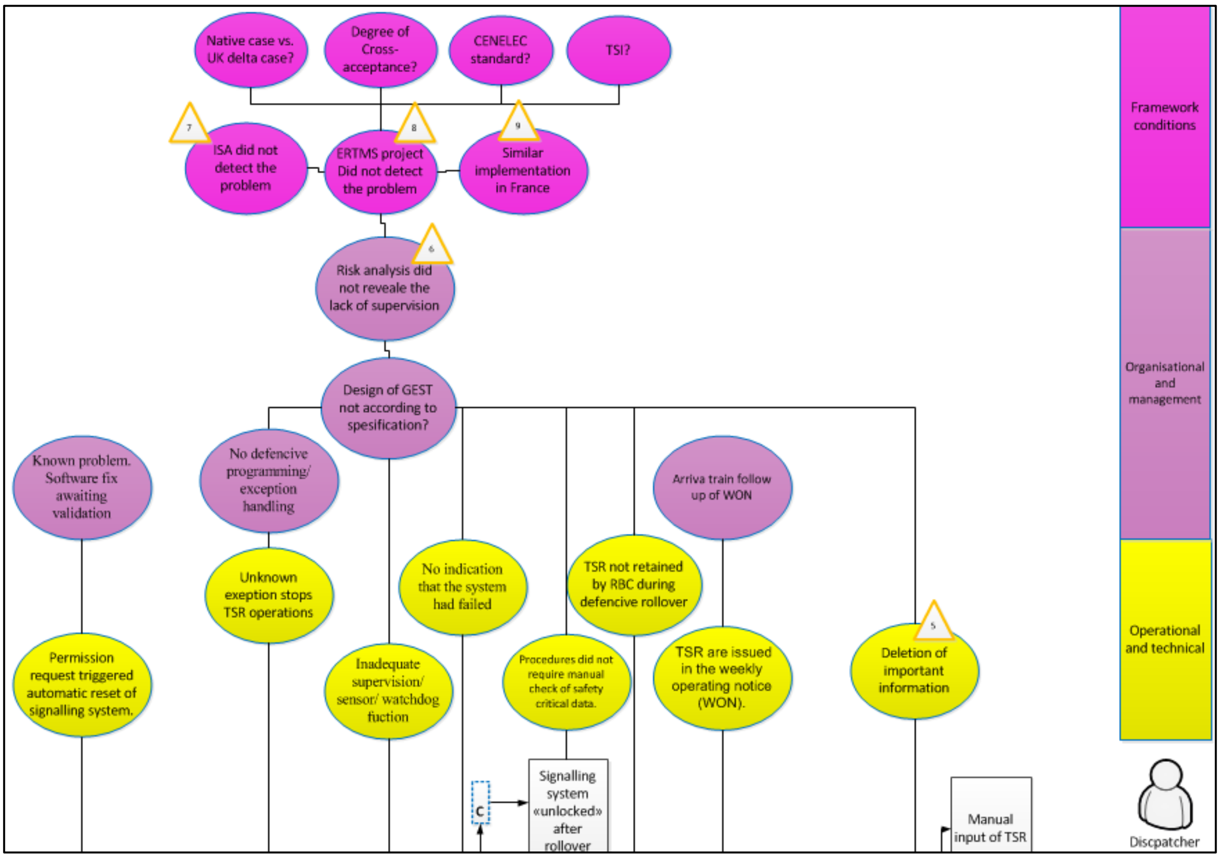

Native case vs. UK delta case?
Degree of Cross-acceptance?
CENELEC standard?
TSI?
Framework conditions
7
ISA did not detect the problem
8
ERTMS project Did not detect the problem
9
Similar implementation in France
6
Risk analysis did not reveale the lack of supervision
Organisational and management
Design of GEST not according to spesification?
Known problem. Software fix awaiting validation
No defencive programming/ exception handling
Arriva train follow up of WON
Unknown exeption stops TSR operations
No indication that the system had failed
TSR not retained by RBC during defencive rollover
Permission request triggered automatic reset of signalling system.
Inadequate supervision/ sensor/ watchdog fuction
Procedures did not require manual check of safety critical data.
TSR are issued in the weekly operating notice (WON).
5
Deletion of important information
Operational and technical
C
Signalling system «unlocked» after rollover
Manual input of TSR
Discpatcher

Figure 34: Stage 6. Considering systemic safety problems and areas for improving safety.

Systemic safety problems can be faults or weaknesses in technical design or problems with organisational risk controls, barriers or framework conditions. The systemic safety problems are marked with yellow triangles in figure 34 (larger version in Annex C). The AIBN-method describes the systemic safety problem as the investigations' most important findings for safety, and if improved might have the greatest impact on improving safety. In the Cambrian investigation the fact that a single point of failure, related to the communication thread on the GEST server, managed to slip through the comprehensive development and approval process is considered a systemic safety problem. This is an area were more investigation should be done, but this thesis has had a limited access to information and has not had the possibility to go deep into this area. The potential systemic safety problems are listed in the same way as local safety problems, but due to lack of information in the interim report [41] questions rather than answers are listed in table 5.

Table 5: Systemic safety problems.

No.	Systemic Safety problems
5	The logs were manually deleted following the rollover. • What was the purpose with the GEST log? • Why were the logs not saved? • How was the technicians trained and informed about the GEST logs?
6	No risk analysis showed the potential risk of failure on the GEST operating system. • What type of risk analysis was performed by the GEST project? • Have all the required analysis been performed? • Have the analysis been performed correct?
7	The independent safety assessor did not detect any flaws in the design process. • What information did the ISA receive and review? • How do the ISA check that statements are correct? • What process did the ISA follow to "check" the projects work?
8	The ERTMS project did not detect the problem. • How did the project manage risk analysis? • Is the TSR risk analysed?
9	Implementation on the Cambrian lines was being guided by on-going design for the French system might also have given the impression that the system was already comprehensively examined and safe to use: • Was there any translation problems? • How was this statement proved and documented? • Was the ERTMS project informed that the GEST server at that point was not in service?

5.2.7 Stage 7: Assessing the need for safety recommendations

It is important to stress that this thesis is based on an interim report, and therefore the information about the investigation has been limited. It is expected that the final RAIB report will give a more comprehensive analysis and list of recommendations. Based on the information available in the case study there are some areas that stands out as possible to improve:

- Improve the independent safety assessment of safety requirements and design.
- Make sure the comparative information, such as the statement about European approval, is legitimate and identical.
- Improve the hazard analyses process.
  - Are suitable analyses methods used (CENELEC)?
  - Can they detect single point of failure?
  - Are the methods used correct?
- Handling of all unexpected exceptions/ erroneous data so that it does not lead to a failure.

5.3 Applying the CAST-method

This section will demonstrate the use of the CAST-method, which is a part of the STAMP theory introduced by Nancy Leveson. The theoretical background for method is explained in chapter 4.2.

The CAST-method was selected in order to evaluate a more systemic oriented method and compare it to the AIBN-method. The selection of the CAST-method was based on recommendations from Professor Lundteigen and Postdoc Kim at the NTNU, and literature review on systemic methods for accident analysis.

5.3.1 Stage 1: Identifying system hazards

In order to identify hazards the processes that are being controlled must be described. For the railway there are many independent systems that are interacting in order to make the trains move. In general simplified terms an infrastructure manager is responsible for the track and traffic control, and the operator for driving the train safely. Accidents may be defined as derailments, collision, fire etc. that results in death or injury. The hazards being controlled by the infrastructure manager and the operator are related, but can occur at different places.

In this thesis the word for loss is accident because this is the term used in the RSD [6]. The case example involves several trains that where driving too fast when they were passing unprotected level crossings. The speed limit is provided to the train's monitor, and it was not displaying the correct speed restriction. The speed limit at the level crossings had a long standing temporary speed restriction (TSR), to provide sufficient warning of approaching trains so the users could cross safely. After a system reboot the TSR was not transmitted to the trains as it should, and three trains passed level crossings at too high speed before anyone noticed the fault. The risk of a level crossing accident was increasing when the trains where driving too fast, and severely reduced the time a level crossing user had to detect the passing trains. The high-level potential accidents (loss) for train operations are listed in table 6.

Table 6: Potential accidents.

Potential accident
Loss of life or serious injury to train passengers or people in the area of the train
Unacceptable damage to the train or objects outside the train

In this CAST analysis the focus is on the missing TSR. The case did not lead to a loss or accident, but the missing TSR led to a wrongly indicated too high speed for trains at the level crossings.

<u>**Hazard:**</u> **Trains exceeded maximum allowed temporary speed restriction at level-crossing.**

There is also a danger of derailment if the TSR is put in place due to construction work, or track errors where the speed temporarily must be reduced in order to pass safely.

Train accidents are defined in the Railways Safety Directive (RSD) 2004/49 article 3 k, and shown in table 7. This can be used as a basis for establishing high-level hazards on the European rail network.

"Accident means an unwanted or unintended sudden event or a specific chain of such events which have harmful consequences."

Table 7: Accident categories.

Accident categories according to RSD 2004/49
Derailment
Collision with object
Level-crossing accident
Accidents to persons caused by rolling stock in motion
Fires and others

The category "Other" is a collection for all the other accidents that may occur. Examples on other accident may be injury to passengers on platforms, during boarding and disembarking the train and accidents related to the infrastructure such as electrical current, accidents during maintenance work, trespassing etc.

5.3.2 Stage 2: Safety constraints and requirements

At a level crossing vehicles and pedestrians can cross the train line. Historically there have been a lot of serious accidents at level crossings and they are still a major contributor to train accidents. The speed restriction at level crossings on the Cambrian line was set to provide level crossing users with sufficient warning about approaching trains, so they could cross safely. Level crossings have different grade of protection, and may be protected with barriers, blinking light and alarm sound, or not any protection at all. At the level crossings in the case example there were gates and signs to stop and warn the users about the level crossing. The level of protection often depend on the amount of traffic on both the road and rail, the train speed and sometimes also economy.

The safety constraints in place to control the risk of level crossing accidents was violated:
<u>Safety constraint:</u> Trains must not exceed maximum allowed temporary speed restriction at level crossings.

5.3.3 Stage 3: Identifying control structure

The safety control structure is based on Leveson example on common regulated safety-critical industry in the United States. The structure has two basic control phases, one for developing the system and one for the operation of the system. The safety of the operations are dependent on the original design and the prescribed operating instructions. The operational environment will in turn provide feedback to the manufacturer and help tune and improve the system.

Compared to how Leveson has exemplified control structure in figure 14, this thesis has added a few items to the graphical presentation of the structure in figure 35 (larger version in annex D). The control structure is based on the general British safety control-structure for railways, and the descriptions in the RAIB interim report [41]. For the development and operations of the system most actors are the same. The top level organisations in the control structure is the European parliament that generate directives, which is implemented in the UK legislation by the Parliament. Office of Road and Rail is the economic and safety regulator, and the Department for Transport is setting the strategic direction, funding investments, managing rail franchises and regulation fares. Arriva trains employs the train drivers on the Cambrian line, and Network rail is the infrastructure manager. Ansaldo STS was awarded the contract to deliver the ERTMS system for the Cambrian pilot line in 2006, and together with Arriva trains and Network rail they form the ERTMS project. The independent safety assessor for the ERTMS project was Lloyd’s register. Further down in the control hierarchy the operating process of sending temporary speed restrictions to the trains are shown in the blue box at the down right corner. Some elements such as the interlocking (see figure 3) has been left out of the operating process to simplify the structure. The operating process can easily be changed to another operating process for a later investigation or risk analysis. All of the actors and elements on the control structure is analysed in the later stages of the CAST method.

The description of the organisations are visualised with logos or other objects to make them easier to recognise. The control actions are visualised by blue arrows, and the feedback is shown by black arrows. Missing control actions or feedback is shown by red arrows with red text. Inspiration from the AIBN-method has been applied to the control structure, and the safety problems are visualised as hazards in the control structure with red numbered triangles and explained in short in the figure.

The control structure was developed and completed in parallel with the later steps, and may be perceived as quite complex. However during the work with the analysis the control structure and was a great way of showing where the problems are, and summarising the whole investigation. This can be a nice tool and overview for the investigator when the investigation report shall be written, and similar to the final visualisation of the AIBN-method.

Compared to the AIBN-method CAST found 9 safety problems during this analysis, while the AIBN-method found 4 local safety problems. The main reason is that the AIBN-method is not looking at the development phase during the initial investigation, and is doing this later in the analysis at stage 6 when systemic safety problems are analysed.

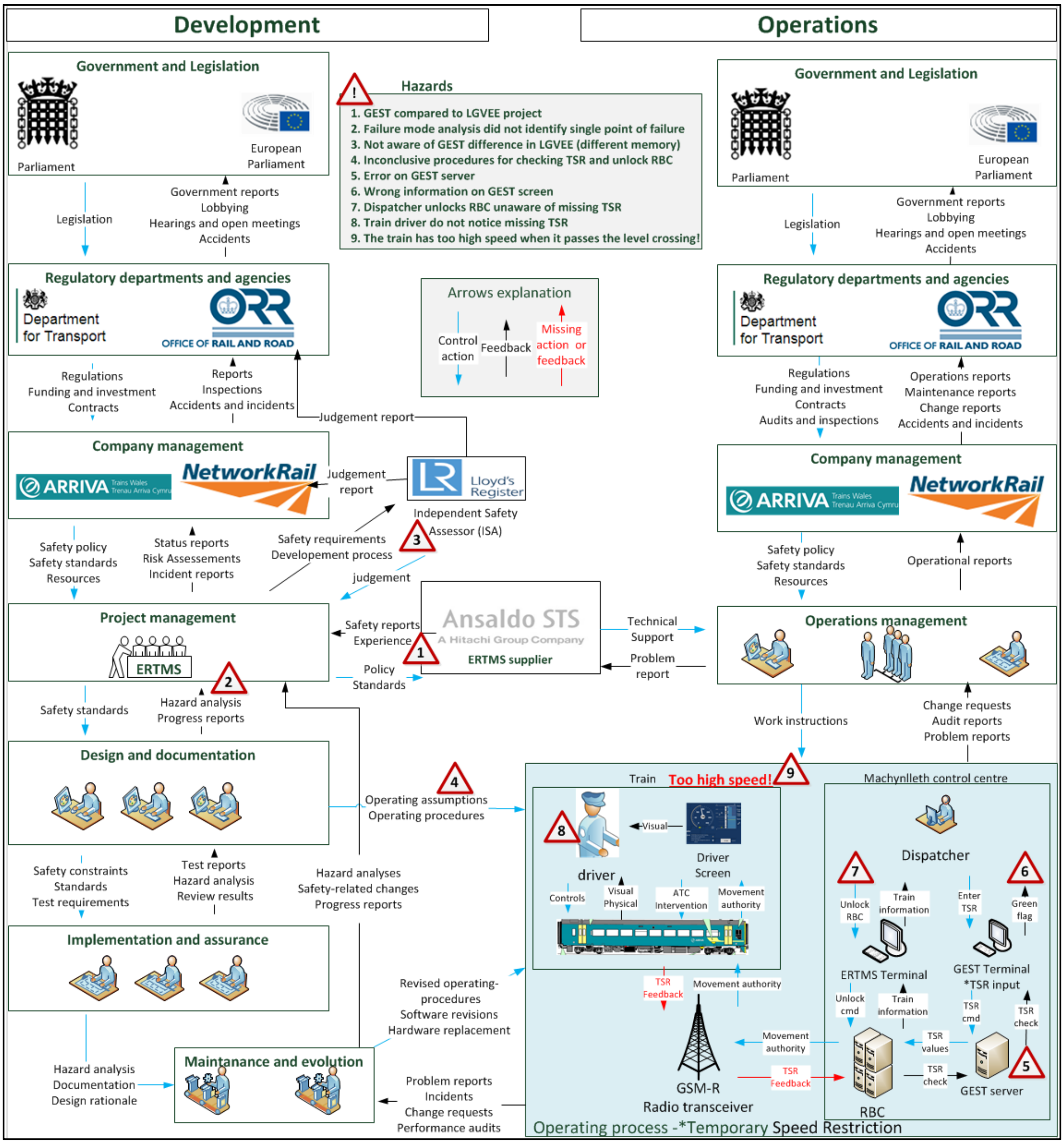


Figure 35: Cambrian line ERTMS level 2 – model of sociotechnical control structure.

5.3.4 Stage 4: Proximate events

In order to understand the physical process of setting speed restrictions for trains the basic events that lead to the trains driving too fast must be identified. The events are extracted from the RAIB-interim report [41], but the AIBN-method stage 1 has also had an influence on how the events are presented.

- A train on diverging track requested a movement authority already allocated to another train.

- The request triggered an automatic software reset (rollover).
- The Signalling system stopped transmitting all movement authorities to trains.
- During the rollover the GEST server experienced an unknown exception (no. 5 figure 35).
- Temporary speed Restrictions (TSR) are not transmitted from GEST to the signalling system.
- Green flags indicates (wrongly) that TSR are applied to the system and being sent correct (no. 6 figure 35).
- The dispatcher "unlocks" the signalling system after checking that flags are green (no. 7 figure 35).
- Temporary speed restrictions failed to reload into the signalling system (RBC).
- New movement authority displayed without temporary speed restrictions.
- First drivers do not notice missing speed restrictions, and 3 trains pass level crossings at too high speed (no. 8 and 9 in figure 35).
- Driver of train 2J03 reported a fault with the speed restriction.
- Dispatcher discovered that TSR information was not being transmitted to any trains.
- The signalling technician forced a signalling system reset.
- The signalling technician reset the GEST system.
- The signalling technician forced another signalling system reset.
- After several unsuccessful attempts to reload the database, the fault was reported to Ansaldo STS.
- Ansaldo STS advised the signalling technician to cleanse data from the signalling system. This lead to a loss of important diagnostic data in the GEST systems.
- All temporary speed restriction information was manually re-entered into the GEST computer terminal.
- Correct indication of the temporary speed restrictions on the in-cab displays and verified by a test train driver.

5.3.5 Stage 5: Analyse loss, contributions and ineffective controls

Information in this section is based on the RAIB interim report [41], and a meeting with RAIB in January 2019. The first part of this analysis is a visual break down and analysis of the GEST system, and the second part is a textual description of the analysis.

The physical system GEST system is an integral part of the ERTMS signalling system, and safety related decisions are made based on the information displayed on the GEST terminal screen (figure 36). The system is used to apply Temporary Speed Restrictions (TSR) to the Cambrian line, and to return the signalling system to service after a rollover.

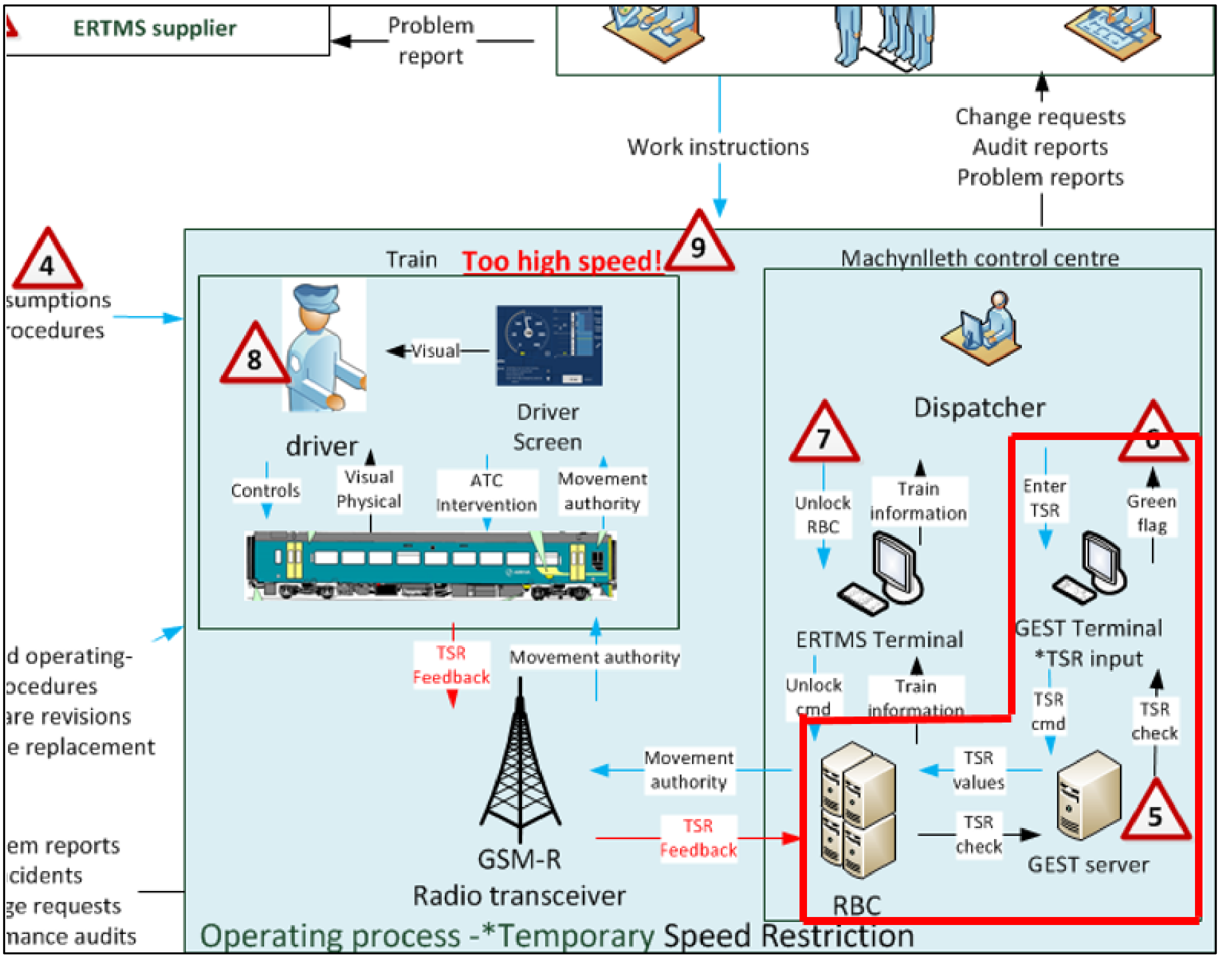


Figure 36: Analysis of the GEST system.

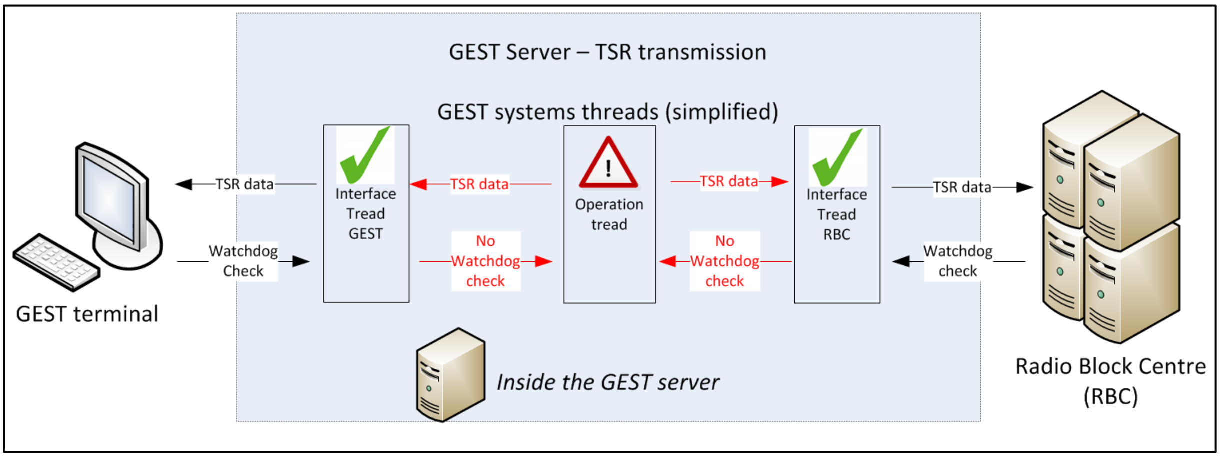


Figure 37: Refined control structure of TSR transmission inside the GEST server.

The details of the GEST-system is business secret, and only s simplified view is shown in figure 37. The flaw was found by setting up a replica system in a laboratory, performed by Ansaldo STS. Using black box and white box test methods, one communication thread was found to give a similar failure mode. This thread forms the backbone of the GEST sub-system. Figure 38 displays how the GEST control flaw fits into the STAMP classification of control flaws leading to hazards. This abstract model was provided in 2011 [53] to assist generating scenarios, however in 2018 [48] the model was replaced with a more detailed model. The main reason the old model was replaced was that it was too abstract and left out important details, and not distinguishing between the automated and human controller. The old model is used to demonstrate the flaw, because it is easier to understand. The new model is very detailed, and it is recommended to use the STPA Handbook from 2018 [48] for an explanation of the model.

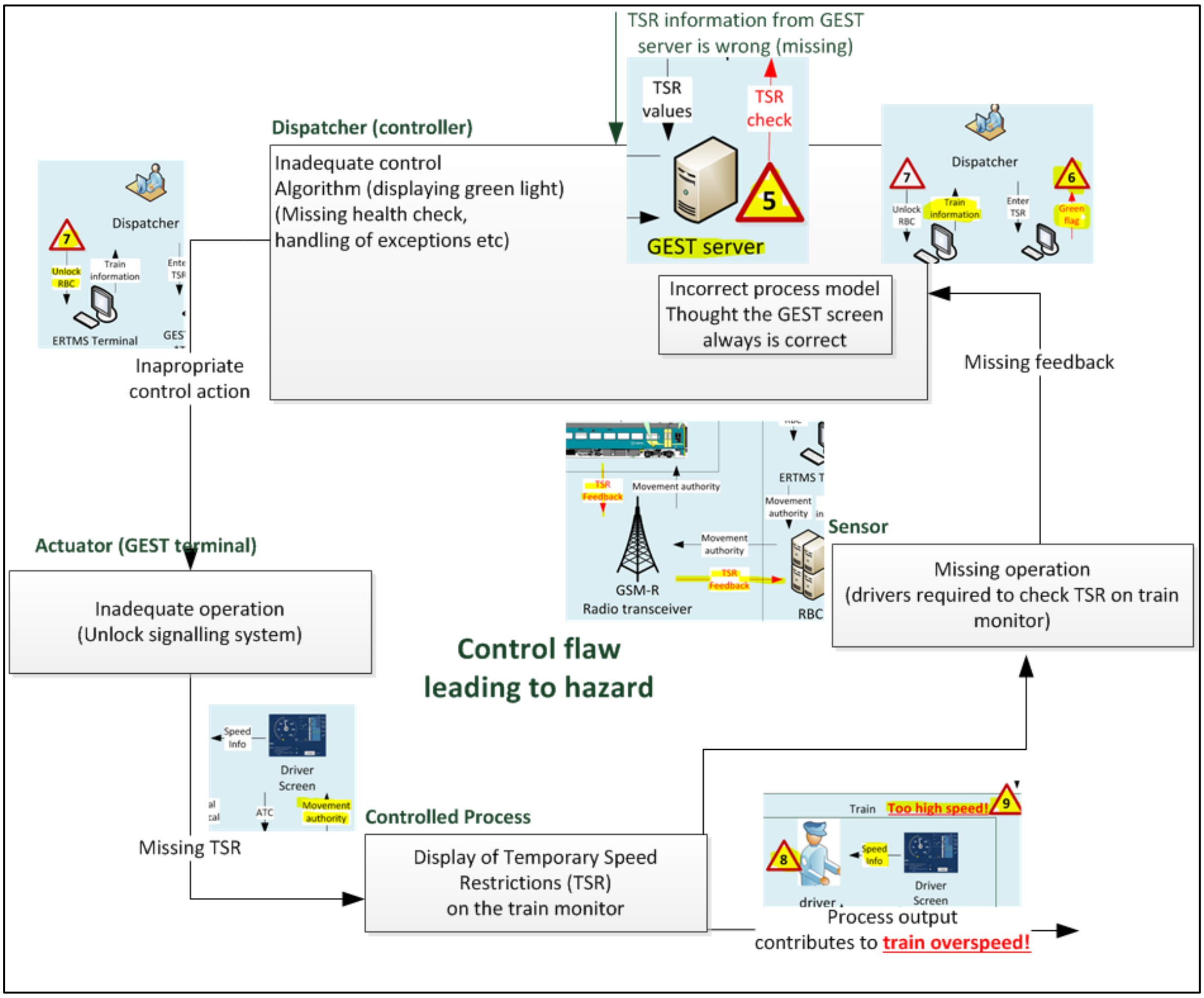

TSR information from GEST server is wrong (missing)
TSR values
TSR check
5
GEST server
Dispatcher (controller)
Inadequate control Algorithm (displaying green light) (Missing health check, handling of exceptions etc)
Incorrect process model Thought the GEST screen always is correct
Dispatcher
7
Unlock RBC
Train information
Enter TSR
6
Green flag
Missing feedback
Dispatcher
7
Unlock RBC
Train information
Ente TSR
ERTMS Terminal
GES
Inapropriate control action
TSR Feedback
Movement authority
ERTMS T
Movement authority
Movement authority
TSR Feedback
GSM-R Radio transceiver
RBC
Sensor
Missing operation (drivers required to check TSR on train monitor)
Actuator (GEST terminal)
Inadequate operation (Unlock signalling system)
Control flaw leading to hazard
Speed Info
Driver Screen
ATC
Movement authority
Missing TSR
Controlled Process
Display of Temporary Speed Restrictions (TSR) on the train monitor
Train
Too high speed!
9
8
Speed Info
Driver Screen
driver
Process output contributes to train overspeed!

Figure 38: Classification of GEST control flaw.

In figure 39 the analysis of the GEST system are listed, this include the requirements, controls, failures and inadequate control and the physical contextual factors. The headings of the analysis is based on Leveson's figure 11.2 [53].

5 **GEST SYSTEM**

Safety requirements and safety constraints violated:

- Sending enforced Temporary Speed Restrictions (TSR) to the RBC
- Displaying correct green flags, allowing signallers to open system for traffic with missing TSR's. The flag should have been red, because the conditions were not fulfilled for a green flag.

Safety Equipment (Controls):

- Gest terminal (operating room)
- 2 x GEST servers for redundancy (equipment room)
- Radio Block Center (RBC) (equipment room)
- Transceiver GSM-R (antenna outdoors)
- Train - On board Unit (OBU) – (driver display)
- Balise group to identify train location (along the track)
- Interlocking determines movement authority availability based on conflicts and route legitimacy

Failures and Inadequate control:

- GEST server failed to automatically upload TSRs following rollover of RBC
- Coherency check between RBC and GEST server failed to identify TSRs were missing from RBC
- Inadequate supervision/ watchdog function on the GEST communication thread
- TSR not retained by RBC during defensive rollover
- No indication that the system had failed was provided to the signallers
- Unknown exception message was "hidden" in GEST server data log (and deleted when restoring the system)
- GEST operation thread not provided with defensive programming

Physical Contextual Factors:

- Volatile memory

Figure 39: STAMP analysis of the GEST-system.

5.3.6 Stage 6: How and why the inadequate control contributed

Many of the elements in the control structure have not been analysed due to missing information. Some are high level organisations such as Department of Transport, Office of Road and Rail etc., and may not play a part in the incident. However the role of the independent safety assessor and the ERTMS project is very interesting for the analysis. It is expected that RAIB will give details about their role in the final investigating report.

For those elements that have been analysed in order to demonstrate the use of the method, it should be noted that some assumptions have been made in addition to the information in the interim report and the meeting with RAIB in January 2019. These assumptions may not be correct. It is therefore important to stress that the official investigation result is presented by the RAIB in their final report. For some of the unknown elements questions are listed in the analysis.

Arriva trains employs the train drivers on the Cambrian line (Figure 40). ERTMS lines have a different way of receiving information than on conventional railway lines. On ERTMS lines the driver receives all information on a screen onboard the train (figure 5), while conventional signalling systems have physical equipment placed at the track (see chapter 2.1.1.2). Three train drivers did not notice the missing TSR and had too high speed at level crossings, and the analysis of trains drivers are shown in figure 41.

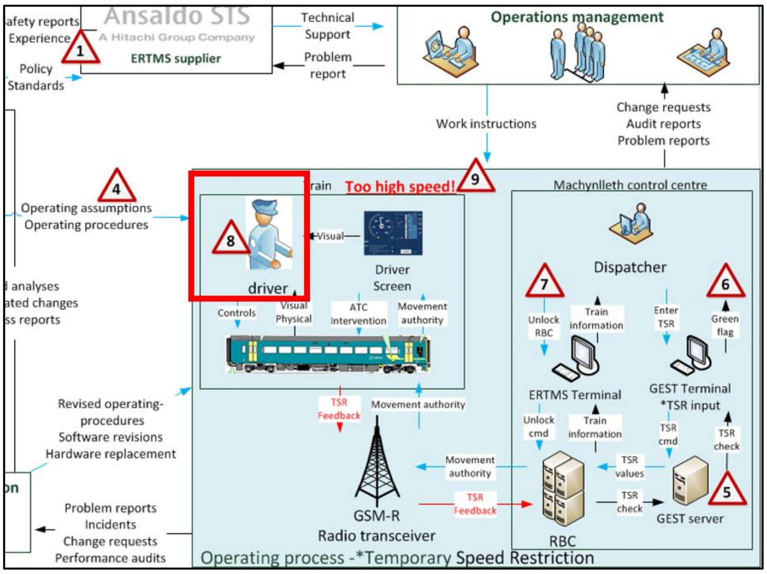


Figure 40: Train drivers are employed in Arriva trains.

⚠8 TRAIN DRIVER

Safety requirements and safety constraints violated:

- Drives with higher speed than allowed by the Temporary Speed Restriction (TSR)

Context:

- ERTMS pilot project
- TSR is not displayed in the DMI
- No physical signs at the trackside

Inadequate control action

- The driver does not notice the missing TSR
- Make sure driver has read and understood the WON

Mental model flaw

- Did not react at too high speed at level crossings
- Not aware of the reason why the TSR was informed?
- Thought the TSR was removed on purpose?
- Too high reliance on the technical system?

Figure 41: Analysis of the train driver.

The train dispatchers are employed by Network rail and located at the Machynlleth signalling control centre, and are controlling the ERTMS system via computer terminals (figure 42). The dispatchers are controlling the movements of all trains on the Cambrian line, and have a visual overview of all trains and can communicate with the train drivers. The analysis of the dispatchers are shown in figure 43.

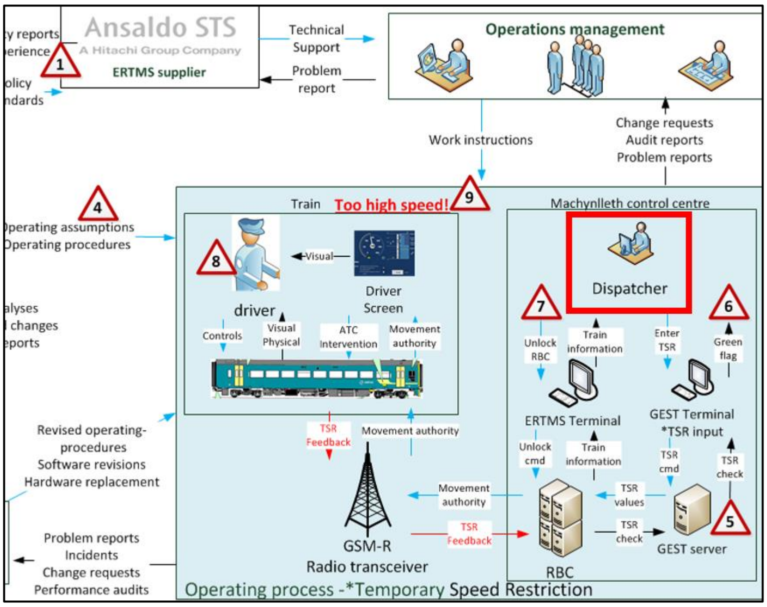


Figure 42: Dispatchers are employed by Network rail.

7 SIGNALLING STAFF (DISPATCHER)

Safety requirements and safety constraints violated:

- “Unlocked” the signalling system with missing TSR after a rollover

Context:

- No indication of error (GEST status display green flag – meaning all is OK)
- ERTMS pilot project

Inadequate control action:

- No check (manual or automatic) of TSR-data integrity (missing or corrupt) after restart

Mental model flaw:

- Did not know that the GEST status on the terminal screen could be wrong

Figure 43: Analysis of dispatchers.

The technical signalling staff is employed by Network rail and are monitoring and maintaining the hardware and infrastructure of the signalling system at Machynlleth signalling control centre (figure 44). They are the first line of technical support if there are any problems, and the analysis of the signalling technicians are shown in figure 45.

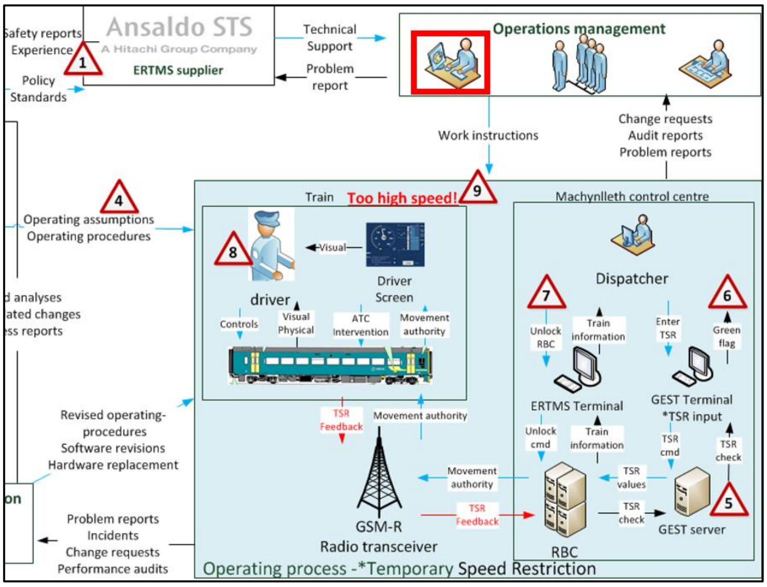


Figure 44: Signalling technician employed by Network rail.

SIGNALLING STAFF (TECHNICIAN)

Safety requirements and safety constraints violated:

- Deleted event logs in GEST system (cleanse)

Context:

- ERTMS pilot project
- Not trained for the situation?
- Had never used the log, did not see the importance?

Inadequate control action:

- Failure mode not identified before the system is operative?

Mental model flaw:

- Not aware of potential failure mode?

Figure 45: Analysis of signalling technicians.

The technical signalling staff at Ansaldo is supporting the local signalling staff at Machynlleth signalling control centre if they encounter problems they are not able to solve themselves (figure 46). The analysis of Ansaldo technical staff is shown in figure 47.

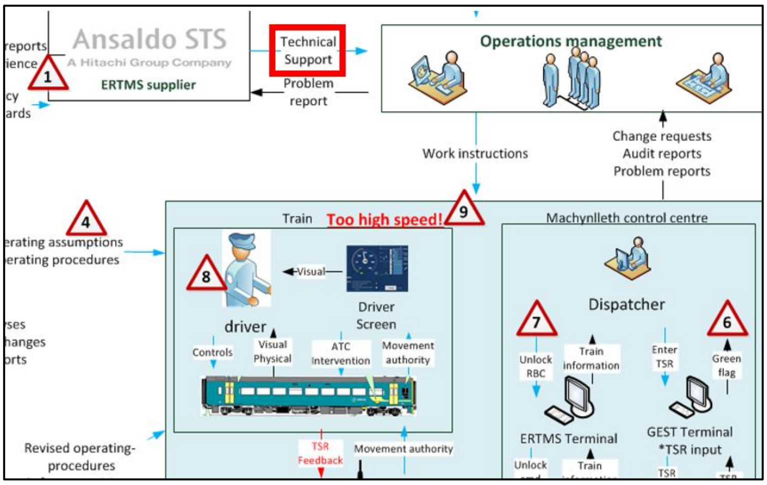


Figure 46: Ansaldo technical staff.

ANSALDO STS STAFF

Safety requirements and safety constraints violated:

- Instructed signalling staff to cleanse databases to restore TSR data, and lost important event log information

Context:

- ERTMS pilot project
- Hampered by having only very limited data from the time shortly before and following the rollover

Inadequate control action:

- Did not download copies of event log or databases before performing the cleanse that deleted the data.

Mental model flaw:

- Did not know that the cleanse would delete event logs and databases?
- Did not know that event logs and databases was important?

Figure 47: Analysis of Ansaldo technical staff.

Ansaldo STS is an international company with headquarter in Italy, that design and implement solutions for rail transport, and employs about 4.000 people around the world (figure 48). The company provides components and services, with the signalling and control system, or separately. The company was awarded the contract to deliver the ERTMS system for the Cambrian pilot line in 2006. The analysis of Ansaldo is shown in figure 49.

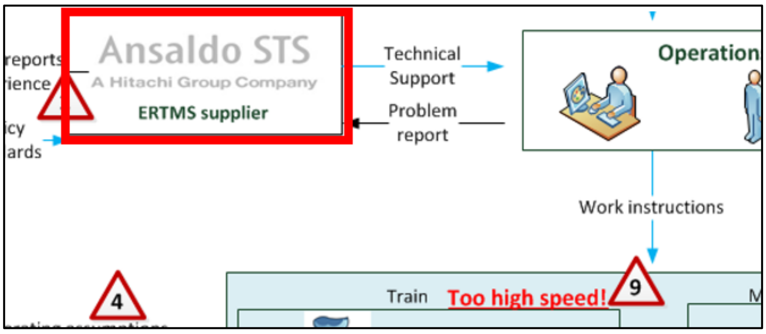


Figure 48: Ansaldo STS company.

1

ANSALDO STS COMPANY

Safety requirements and safety constraints violated:

- Supplying a safety critical system with a flaw
- TSR data unintended deleted or missing during rollover

Context:

- TSR system (GEST) developed in Spain for a high speed line several years before its use on the Cambrian lines.
- Implementation on the Cambrian lines was being guided by on-going design for the French system. Computer memory was not changed on the Cambrian when this change was made to the French system.

Inadequate control action:

- Missing health check on the GEST server, watchdog function missing.
- Risk analysis did not detect hazard of missing TSR.
- Implementation process did not detect the hazards (test, verification and validation)

Mental model flaw:

- Misconception. Reliance that the GEST screen is always accurate.

Figure 49: Analysis of Ansaldo STS company.

Network rail is the infrastructure manager of Britain's railway, which includes the Cambrian ERTMS line. Together with Arriva trains and Ansaldo they form the ERTMS project management (figure 50). The Cambrian lines were used for the UK's ERTMS pilot project. The main purpose of the project was to test and gather experience on the technology. Use of ERTMS for passenger services started in 2010. The Analysis of ERTMS Project management is shown in figure 51.

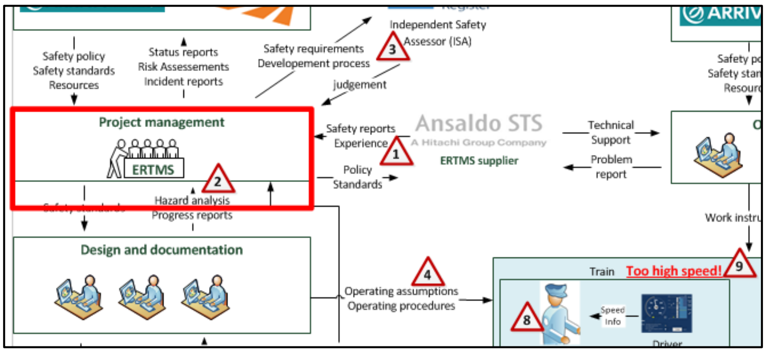


Figure 50: ERTMS Project management.

2 **ERTMS Project management**

Safety requirements and safety constraints violated:

- Implementation process did not detect the potential hazard of missing TSR

Context:

- ERTMS pilot project
- GEST product validation already achieved in Europe (but changed)
- British ISA was not made aware of the difference (the change)

Inadequate control action:

- Hazard analysis, risk analysis, ISA did not detect the flaw. Missing watchdog function.

Mental model flaw:

- Misconception of how the system works. Also the supplier and ISA had misunderstood how the system works.

Figure 51: Analysis of ERTMS Project management.

Lloyd's register was the independent safety assessor for the project (figure 52). The Analysis of Independent safety assessor is shown in figure 53.

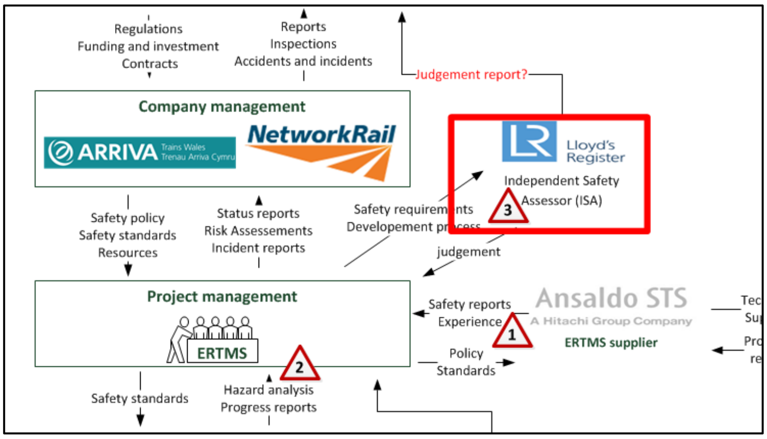


Figure 52: Independent safety assessor.

3 Independent safety assessor

Safety requirements and safety constraints violated:

- Judgement of requirements and process did not detect the hazard of missing TSR

Context:

- ERTMS pilot project
- GEST product validation already achieved in Europe (but changed)
- Not made aware of the difference in application LGVEE vs Cambrian (memory)

Inadequate control action:

- Hazard analysis, risk analysis?

Mental model flaw:

- Misconception of how the system works?

Figure 53: Analysis of Independent safety assessor.

5.3.7 Stage 7: Coordination and communication

The requirements were written in both French and English and then translated into Spanish, English and French. Due to a lack of information it has not been possible to establish if the translations subtly changed the meaning in the different languages. The GEST system does not follow what would be the expected intent of the requirements. There is a potential misunderstanding of the system function, and a latent single point of failure. A decision to not update the Cambrian RBC to also use non-volatile memory based on the GEST screen always being accurate shows lack of understanding how the system works. The Cambrian ERTMS user manual requires signallers to check the GEST screen to control that TSR are green before unlocking the RBC. The failure mode analysis refers to the signaller's check of the GEST screen as the final check that the TSR's are correctly loaded in the RBC.

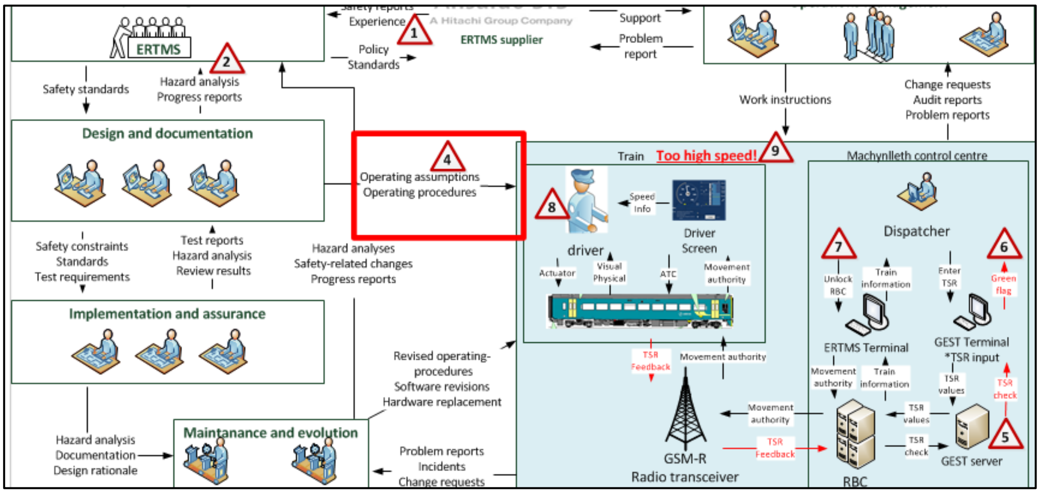


Figure 54: Misconception of how the system works.

5.3.8 Stage 8: Changes to the safety control structure over time

GEST was assessed by comparison with Ligne à Grande Vitesse Est européenne (LGVEE), even though the application was not in use at the time, and changed to non-volatile memory before it was put in service. The application of GEST was approved by Société nationale des chemins de fer français (SNCF). Lloyd's register (the British ISA) was not made aware of the difference in application (volatile memory).

The use of TSR was selected for long standing speed restrictions. Risk analysis demonstrated that TSR was safe to use, instead of using Permanent Speed Restrictions (PSR). The assumptions in the risk analysis proved to be wrong, due to the flaw in the communication thread of the GEST system.

5.3.9 Stage 9: Recommendations

It is difficult to give detailed recommendations when more details are required and the case has not been investigated completely. The areas that are listed below would normally be analysed in more detail before a recommendation is given. The suggested scope that points out as having a potential for improvements are:

- Improve the independent safety assessment of safety requirements and design.

- Make sure the comparative information, such as the statement about European approval, is legitimate and identical.
- Improve the hazard analysis process.
  - Are suitable analysis methods used (CENELEC)?
  - Can they detect single point of failure?
  - Are the methods used correct?
- Handling of all unexpected exceptions/ erroneous data so that it does not lead to a failure.

6 Results and analysis

The discussion chapter revisits the research questions and explain and interpret the results of the study. The differences in the methods demonstrated in chapter 5 are discussed and compared, and also how other studies relates to the findings in this study. Some of my personal experience is also reflected in the discussion with 18 years of work within the safety domain, and almost 10 of these years as an accident inspector.

6.1 ERTMS and accident investigation

How will the introduction of ERTMS affect the way accidents are investigated?

Many European countries have had proprietary computer based signalling systems before ERTMS was selected as the European railway signalling system. The introduction of computer based signalling systems on the railway did not change the way accidents were investigated over night, but it increased the complexity of the investigations. During the last decades, the way of investigating railway accidents in Europe has changed, but maybe not in the same paste as the development of new technology. Most European countries have established independent National Investigation Bodies (NIB), and the main goal is better learning from accident. The focus on assigning blame has been recognised as a hampering factor, and mutes the will to report accident and find systemic safety learning. The European NIBs have created networks where they share relevant information about accident investigations. These networks are a good platform for sharing and increasing the knowledge on how to investigate complex accidents, such as ERTMS.

The literature on accident investigation has evolved during the last decades, and more and more scientists are recommending a systemic approach for complex accident investigation. The "old" established "sequence of events" theory, where the problem is fixed if you break one of the chains in the event, is challenged by the systemic approach. The systemic approach claims that in order to understand and learn from complex accidents the whole system, with all the interactions, must be scrutinised. By only investigating the sequence that lead to the accident, there may be a loss of learning points on how the whole system interacts and creates dangerous interactions. These dangerous interactions may be found higher up in the hierarchy than in the operating process, closer to the physical process that is being performed. If an investigation is able to find and properly explain why it is necessary to make changes at a high level, this may have a great effect on preventing future accidents. Blaming the operator or driver, and replacing him or her will do little to prevent future accidents.

The really big accidents are usually given sufficient resources and time, and the best and most experienced personnel are given the task. However most investigations are not of big accidents, but small and medium accidents and incidents. For an inexperienced investigator it can be difficult to choose the most efficient method to apply to the investigation. Some investigations can be straight forward and quite easy to explain, while others may not be able to explain down to the last detail. It is also a delicate balance to evaluate the possible safety impact recommendations from the investigations might have. A small accident or incident report might not have the impact to change management or government structures in the same way as an investigation report of a big media covered accident. Investigators of accidents know this, and adapt the time and resources used in the investigations accordingly.

The small and medium investigations are a great learning platform for gaining experience towards becoming an experienced accident investigator. A healthy focus on what safety learning is possible to achieve from the investigation, and the most appropriate method to convince the decision makers is a good start. There is no doubt that system based accident analysis methods are good tools for investigation big accidents. For small and medium accident investigation it might be to resource demanding, and the "old" methods may be sufficient to give a satisfactory result.

The introduction of ERTMS may not affect the methods used to investigate accidents, but it reminds us of some issues that have been challenging to deal with for a long time. Complex systems and software. This thesis has only demonstrated a small part of the possible approaches and methods, and there is large potential for more research on this area. As stated in the SKI report (2008) accident methods may be obsolete after five or ten years, and need to adapt to the changes in society in general. Actors who perform accident investigation should be aware of research and new methods within the discipline, and actively participate in new knowledge.

The shift to more international companies supplying ERTMS components, and those companies requiring to keep some information a business secret may cause some challenges. As the Cambrian line investigation has shown the supplier set up a replica system in a lab, and gave the RAIB access. Finding the cause of the incident or accident should be in the interest of the supplier, but there might be language problems and difficulties in understanding all functions correct with the introduction of ERTMS system.

6.2 Complex investigations

Is investigation of ERTMS any different from any other investigation involving a complex system controlled by software?

In short, no. The methods demonstrated in this thesis should work on ERTMS investigations, and so will probably many other approaches as well. Complex systems controlled by software has also been present for a long time in other branches such as space exploration, nuclear power, air transport and many other areas. Researchers have been aware of the complexity accidents may be a part of for decades, and literature on the subject has been published by several well-known researchers, as described earlier in this thesis. What might be a bigger difference is the level of recognition the different NIBs or investigating company have for the need of a different approach to complex investigations. Using old approaches where the starting point is a chain of events, and each part of the system is investigated separately might not give a good result. The NIBs must take an active approach on defining how they shall perform complex investigations, and what the required competence for the involved personnel should be. As mentioned earlier participating and contributing in networks and conferences that transfer experience on accident investigation is a good start.

6.3 Formal methods

To what extent can formal methods be used as a tool in reviewing ERTMS events?

Formal methods can be used as a defined software investigation tool, similar to metallurgical, forensic or other specialised investigations. It may also be an alternative to setting up replica computer systems in labs or other simulating methods. Because formal methods is a rigorous approach requiring use of mathematical notations, the users are forced to express requirements in a clear way. By using formal methods to express the specifications it might reveal flaws not discovered by using natural language. Specifications using natural language may contain requirements that are “obvious” for the person writing the specification, but not to the person reading it and creating the software. If the initial investigation does not reveal obvious flaws in the specification or design of the system formal methods may be a useful method. This is in line with the Joint Software Systems Safety Handbook [49] where formal methods is only recommended for a specific part of the investigation. There is little literature to support the use of formal methods to replace the whole investigation process. The initial investigation should establish whether the requirements are specified correctly for the system and if the system fulfil the requirements. These initial questions should be possible to answer by using a questioning approach, and without the investigator having expert knowledge on software. If the initial questions do not reveal any obvious problems, then experts on formal methods can be introduced to the investigation. For this purpose, the flow chart presented in chapter 4.3.3 may be used as a starting point.

Using formal methods for the development of software systems is a recognised way of ensuring high quality and resilient systems. Railway signalling systems developed in Europe requires the use of the CENELEC standards, which highly recommend the use of formal methods. Formal methods is however often characterised as hard to use and complicated. If the software system has been developed by using formal methods, this should be considered a benefit for the possibility to reuse some of this work in the investigation. However the possibility of flaws in the formal methods or their use must also be considered during an accident investigation.

The case example in this thesis was investigated by setting up a replica system, and the lack of detailed information made it difficult to demonstrate the use of a formal method. The initial questions for the investigator to answer before contacting formal expert help may be a useful guide to include in the AIBN-method, and demonstrate a systematic approach that does not need expert help at the beginning. Several investigations of software have proven that the problem often lies in the specification of the system and how the requirements are fulfilled, and not coding errors [7].

Another aspect that might also be considered is the understanding and confidence of using formal methods, as they may be hard to understand and explain. It may therefore be more reasonable to use a replica system if that is possible, as this might be an easier process to explain and accept as a tool for computer and software analysis.

6.4 Improvement of the AIBN-method

How can the AIBN-method be further developed to provide better support for the investigation of complex railway accidents?

Because the AIBN-method is a toolbox and description of recommended methods it is easy to introduce new “tools” or methods. The AIBN-method is not meant as a visual tool for the readers of the report to explain the accident. It is a systematic tool for the investigators in order to guide them through the investigation process. This is a systematic way of scrutinising the different aspects and factors that contributed to the accident, and offers guidance in finding the cause and provide safety learning. The method helps the investigator to analyse in a broad manner, and aims to reduce bias. Although the method will not be very helpful if the investigator already has decided on what the cause is and is locked to that view. The method is also a good tool for an investigation team that is familiar with the process and the accident. The visualisation of the method gives a good overview for the team as a basis for discussion on each stage of the method. By using post-it notes on a wall, or programs like Microsoft Visio, the AIBN-method is a great way of structuring and testing the issues that are up for discussion. This helps the team to focus and identify connections between the sequence of events, and risk factors at various levels in the socio-technical system. The AIBN-method already recognises that systemic methods is a tool for investigating complex accidents. However the AIBN-method only refers to other sources of information, and does not explain in detail approaches on a systemic approach for complex investigation.

The study of CAST in this thesis has demonstrated one possible systemic method for investigating a complex ERTMS incident on the railway domain, and may also be applied to investigations in other transport modes. The use of CAST does not necessarily mean that other parts of the AIBN-method may be left out. The use of the AIBN-method to explain the sequence of events in the beginning of the investigation when there is little information, and then later adding the control structure of CAST, could help to find more high level safety problems. In the beginning of an investigation it is important to understand what happened, and for that purpose the sequential approach using STEP has proven to be a useful method at the AIBN. The CAST method also includes a description of the proximate events of the accident, and the AIBN-method offers a more comprehensive way of doing this than CAST. The information found using the AIBN-method can later be used in the CAST analysis. In this thesis the CAST and STAMP theory offered more "tools" and guidance on how to analyse and visualise flaws.

The suggested steps in the CAST analysis is similar to the STPA analysis, but because CAST is retroactive it might be easier to start establishing the operating process and proximate events before establishing the hazards and control structure. In CAST the hazard is known, and in an accident investigation it is often time sensitive to start collecting volatile information as soon as possible. Volatile information can be logs, video, etc. that are automatically deleted, and interviews with witnesses should be done quickly before they are influenced by others. After the first facts collection the information can be listed up in the proximate events, and the analysis of the operating process may start. This may help understand the control and feedback structure and reveal the need for more information. Later, when the operating process is understood and facts collected, the more general hierarchy of control structure and hazards may be analysed as that stage is not as time sensitive. A suggestion would be to start the CAST analysis at stage 4 and 5, and later go to stage 1-3 before working further with stage 6-9 (see chapter 4.2 for description of the stages). This is also in line with how Leveson describes and demonstrates the use of CAST [7], where she states that there is no implication to do the steps in a different order.

Where the AIBN-method is pointing at the problem, the CAST method also offers some assistance in how to analyse the problem in more details with the models of control structure and the guidance in identifying unsafe control actions. By drawing up an abstract safety control structure it was easier to understand and think trough how the system is designed and operated in real life. The safety control structure has similarities to the V-cycle representation in EN

50126, which is a requirement for ERTMS. The CAST-method gives a better distinction between the two phases of developing the system and operating it. By refining this control structure to an appropriate detailed level, it is possible to analyse the elements in the system that did not act as expected. The next phase of analysing the elements in the control structure offered a good guidance in the way CAST is structured, with headlines focusing on safety constraints and control actions. The CAST guidance questions for context, possible mental or process model flaws is useful in order to explain why the flaw was not detected. Using the CAST method or any other systemic method does however require training and knowledge in order to use it. The efforts used by an accident investigating practitioner to understand complex methods and theories are limited due to demands on efficient investigations results, and limited time and resources to do research. Also the background of the investigator has a large influence on the preferred methods, some investigators are expert within the field they are investigating and not within accident investigations. Others are experts in safety and accident investigation, and not experts within the field they are investigating. Investigations will be affected by the individuals performing them, and the fact that investigators have their strengths and limitations. Organisations performing accident investigation must make sure the process of the investigation take into account these strengths and limitations, and ensure an acceptable result. The application of the CAST method and the STAMP theory fits well with the values of the NIBs, and will strengthen the quality of investigations. CAST is focusing on the sociotechnical control structure, and establishing the safety control structure from CAST in the AIBN-method can be helpful in lifting the focus from the technical problem to looking at the control and management problem for the technical elements.

In general the AIBN-method seems to be a better tool and guidance for an accident investigator in the start-up of an accident investigation. The CAST-method however seems to give better guidance and tools when information is already collected, and the investigation is mature to analyse the high-level hierarchy control structure and safety constraints. The AIBN-method is going into details about the accident and what happened earlier than the CAST-method, while CAST has focus on the "big lines" in the beginning. For an accident that recently happened, time is an important factor to be able to collect as much relevant facts as possible. Focusing on the events close to the accident is often more time sensitive, than looking at the development process and control structure which is information that is less time sensitive. Ideally, both methods could be used simultaneously if the investigation has enough resources. After the initial collection of facts and analysis of local safety problems, the investigation can transfer information collected via the AIBN-method to the CAST-model.

6.5 Comparison of the AIBN-method and CAST

This chapter is listing up the strengths and weaknesses for each method in table 8 and table 9, and table 10 displays a recommended combination of the two methods in an ERTMS investigation.

Table 8: AIBN-method - strengths and weaknesses

AIBN-method	
Strengths	**Weaknesses**
Useful in the early stage to establish sequence of events and finding local safety problems.	Can be challenging to analyse “high-level” systemic factor from the sequence of events. Focus is on asking why, and how the safety problem occurred. May miss important problems if is it is not in the sequence of event, or detected as a safety problem.
Focus on the accident and how to analyse “backwards”, and “up” in the hierarchy.	Harder to analyse the development factors with the AIBN-method because the focus is on operational factors from the sequence of events.
The methods used in the AIBN- framework are generally well-known and easy to learn.	
Guidance on selecting relevant factors to analyse in the investigation.	
Guidance on the generation of safety recommendations.	

Table 9: CAST - strengths and weaknesses

CAST-method	
Strengths	**Weaknesses**
Useful to analyse and find systemic safety factors	The suggested order is not so useful in the start-up of an accident investigation if the control-structure is unknown. (*A suggestion would be to start the CAST analysis at stage 4 and 5, and later go to stage 1-3 before working further with stage 6-9)*
The abstract hierarchical control structure is focusing on the life-cycle of the system, and makes a distinction between system design system operation and operating process.	Not so well-known method, and requires training in order to understand and use the control-structure, control-loops and analytical approach with scenarios.
The abstract hierarchical control structure of design and operation can be reused once it is created.	
The controlled process fits into the design and operational process, and can easily be changed in the control structure for new accidents in the same domain.	
The focus on control actions and feedback helps to analyse the relevant of the levels above the controlled process.	
Tools to help analyse the physical process and higher levels of the safety control structure, such as models of control structure, control loops, list of unsafe control actions, action analysis, scenarios to analyse elements etc.	

A combination of the AIBN-method and CAST-method is considered to give the best result in the investigation of an ERTMS accident. A green check is placed on the recommended method, and shows that the AIBN-method is recommended for the first steps and the generation of recommendations. CAST is recommended for the analytical part of the investigation, and seems to give more guidance and tools for understanding and analysing the elements in the accident. The stage where formal methods can be used as a specialised method for software analysis is marked by bold text.

Table 10: Combining the stages of the AIBN-method and CAST.

Stage	AIBN	CAST
1	Focus on the accident, what happened and who was involved. Important in order to understand the accident and find relevant areas for further investigation. ✓	More general high-level approach and focus on the systems hazards. For a NIB working in the domain these are often well known or defined.
2	Focus on identifying safety local problems during the accident, and decide how to investigate further. ✓	High-level and looking at safety constraints and requirements. For a NIB working in the domain these are often well known or defined.
3	Analysing what could have prevented the accident. ✓	Identifying the control structure. This is a demanding step, and requires a good overview on the branch where the accident happened. If this has been done previously it may be reused, and may give a benefit. ✓
4	Analysing risk factors. Guidance on areas to investigate, and elements to consider during the analysis. ***Formal methods can be a possible tool.***	Listing up the events before the accident. This is similar to stage 1 in the AIBN-method. ✓
5	Evaluating the risk factors in stage 4. This stage could be explained in stage 4 and might not be necessary as a separate stage.	Finding the contributions and ineffective controls that lead to the accident. This is similar to stage 2 in the AIBN-method, but CAST offers more assistance in graphical presentations and how to describe the problem. CAST lists four ways a control

		action can be hazardous that are useful to use. ***Formal methods can be a possible tool.*** ✓
6	Considering systemic safety factors. Rated as an important stage, and the preceding stages are leading up to the identification of systemic safety problems. ***CAST can be a possible tool.***	Analysis of elements ✓ Physical process including the physical and operational controls, potential failures, dysfunctional interactions etc.
7	Recommendations ✓	Coordination and communication ✓
8		Dynamics and changes to control structure ✓
9		Recommendations

6.6 RAIBs investigation of the ERTMS case example

How the RAIB actually investigated the Cambrian line case was not a part of the research question in the thesis. The investigation still was ongoing at the time the thesis was finalised. The final report of the investigation will be published by the RAIB. A short description with the available information is included to show that the RAIB used a different approach than those demonstrated in this thesis.

How did the RAIB investigate the complex ERTMS incident at the Cambrian line?

The RAIB does not have a similar process or method as the AIBN-method, yet they are regarded as a very competent investigative branch for railway in Europe. Their approach to investigation methods is that it is difficult to choose one of the well-known method before the facts are collected. Because the nature of collecting facts is very different from case to case, they have found that the best approach is to focus on the accident and follow the process back to the original design and approval process. During the Cambrian investigation graphical figures, event tree and a replica system of the GEST system was used during the investigation. The replica system of GEST was built by the supplier in a lab, and the tests were able to reproduce a similar conditions that lead to a fault with the TSR. By doing that is was possible to explain a flaw in the design of the GEST server. The next step of the investigation was to find the answer to why the design flaw had not been detected during the development and approval of the system. The study has not been able to follow the latest development of the investigation, and this part is therefore missing in this thesis.

6.7 Comparing results to existing results

The literature included in this thesis can roughly be divided in two parts, where the first part is more general literature on accident investigation methods, and the second part is studying and demonstrating selected methods and STAMP in particular. The literature and articles by Perrow, Rasmussen, Leveson, Sklet, Hollnagel and Speziali, Qureshi, Rausand, Underwood and Waterson has been helpful to establish the general development and status of accident investigation theory and methods. The AIBN-method is generally in line with the literature, as the main focus for the relatively new method has been to find best practice. The information about systemic methods is however limited in the AIBN-method and it is referring to literature such as Hollnagel and Speziali. According to the AIBN-method the systemic approach is a complement to and not in place of the stages in the AIBN-method. If it is difficult and complex to describe the sequence of events in stage 1, and also difficult to identify stage 2-4 it is recommended to use a systemic approach. Comparing the theory of STAMP, where the sequence of events is criticised, stage 1 on the AIBN-method is not in line with the literature of Leveson. This does not mean that the sequence of event is useless for "minor" accidents where the investigator prefer the method. In order to account for the variability and age span of the team of AIBN investigators it is regarded as reasonable to have the AIBN-method "toolbox", and gradually work towards more use of the systemic methods. Compared to the environment of a competitive business world, the methods that can prove the best results for the AIBN will probably be the preferred method.

The second part of the literature which is studying selected methods are discussed in more detail, and how the findings relate to this thesis. The analysis by Dong and Suo of the Chinese railway accident was very relevant for the CAST analysis, and the description of how they used the STAMP theory. The Chinese signalling system has several similarities to the European signalling system, and in both the Chinese and Cambrian there were similar causes to the loss. However the Chinese accident resulted in a far more tragic consequence that the Cambrian line case. Their analysis have been able to demonstrate more of the CAST-method as the official

Chinese investigation report contained more information than the Interim report for the Cambrian Line investigation. Especially the causal loops and unsafe control actions have been given more focus. This thesis has had more focus on the graphical presentation of the control structure, and introducing hazards and highlighting the control and feedback flaws in the graphical control structure presentation. This has been done in an attempt to make the control structure easier to recognise by using company logos and items representing the elements function. The original control structure consisting of only boxes, text and arrows is not very interesting to study and therefor a bit more colours and visual effects have been used to make it more interesting for the reader.

The work by Salmon, et.al in 2011 [5] is stating that the selection of accident method is more likely to be based on theoretical preference than anything else. This might also be the case in this thesis, as CAST was selected after the initial meetings with Mary-Ann Lundteigen and HyungJu Kim at NTNU where it was recommended to evaluate the use of the STAMP theory and the CAST-method, in order to study a more recent accident model. The AIBN-method is the method provided by my work place, and it is a requirement to use the method during investigations at AIBN. Also the foundation and argument of why the STAMP theory should be used, suits well with my own views. The conclusion by Salmon et.al is that for single accident investigation the Accimap and STAMP seems to most suited, while for multiple accident studies the HFACS seems to be more powerful. The AIBN-method has more similarities to Accimap than STAMP. The use of HFACS should be considered for the class investigation of AIBN reports, and may be considered for future research.

The work by Underwood, et.al. [5] suggest some factors to why the systemic methods are not widespread in use by practitioners, such as the model validation, usability, analyst bias and the implication of not apportioning blame for an accident. There seems to be a gap between how scientists and accident investigators are analysing accidents according. While scientists are preferring systemic approaches, the practitioners are using a wide range of different approaches. Some resembles the systemic approaches, while others are taking a more "try and fail" approach. There is a main difference between the practitioners and the scientists, where the practitioner must collect facts during the investigation of a resent accident where there are a lot of unknowns. Comparing scientists and practitioners (e.g. accident investigators) might not be entirely correct as they have different agendas. The scientists are often analysing "older" accidents where the facts and analysis may already be published by several parties in order to develop new methods. For the practitioner there are also many other factors to consider such as affected parties, media, short deadline, resources, business secrets, imminent law suits etc. The practitioner may have a role that involve 24 hour on-call duty, requirements to quickly attend the accident site, talk to traumatised personnel and family, and balance the political and media pressure to explain why the accident happened.

The usability of STAMP was studied at small scale field test at Cranfield University, and it was suggested that the methods usability and graphical output was highlighted as in need of improvement. The study stated that learning about STAMP and its application is not a quick process, and the participants needed multiple attempts to achieve a sufficient level of understanding. I can relate to the fact that STAMP can be a bit hard to learn, and the suggestion to improve the graphical output. Improvements to the graphical output is suggested in this thesis as mentioned earlier in this chapter. It is also worth mentioning that a STPA Handbook was published in 2018, and provides directions for those starting out with STPA. This is also relevant for some of the elements of CAST, although a handbook for CAST would be a great help for new users and investigators applying the method.

The article by Stoop and Benner published in 2015 [40] is the most critical towards the STAMP method that was found during this study. The article lists a series of 12 potential threats to the quality of CAST analysis. The article states that STAMP does not specify an accident investigation process, and that it can be problematic that the analysis rely on information from accidental occurrence reports. This is considered as an issue for unexperienced users of CAST that are using accidents investigation reports without being critical to the content of the report. This criticism is relevant, but it also applies to all information that is collected in an accident investigation. The validity of the collected information must be verified before it can be used as a fact. This thesis is investigation the use of STAMP during an investigation, and therefore the information can be evaluated easier than if the analysis rely on reports written by others. The problem with accident reports has also been recognised by Thomas and Malmquist in a paper [54] presented at the 2017 ISASI meet in San Diego. In the presentation they state that unlike scientific literature, accident reports are very rarely updated and corrected if an error is found.

6.8 Relevance of the study

This study is relevant for those who are interested in systemic investigation of complex accidents, and especially European National Investigation Bodies (NIB) that might investigate ERTMS related accidents in the future. The demonstrated methods and suggested application in this thesis can also be used for other signalling systems than ERTMS, and also for other transport modes than railway. The combination of the AIBN-method and CAST-method can be used by other transport modes such as aviation, maritime and road. For the Norwegian AIBN this study is interesting for all transport departments, as it compares the use of the AIBN-method to a systemic method. This study should also be interesting for those who are interested in the application of the STAMP and CAST-method by an experienced accident investigation practitioner. This thesis suggest some changes in the proposed steps of the CAST-method, and introduces some new elements to the graphical output. This could improve the understanding of the graphical output, and make it easier to understand and accept the CAST approach.

6.9 Reliability and validity

Reports and information about investigation of ERTMS related accidents are limited, and therefore an interim investigation by the RAIB was selected as a case example. This has made it difficult to obtain information about the investigation as the interim report contains a limited description and analysis of the accident. Using a different case example was evaluated, but there is something magical about the word ERTMS in the European railway sector that makes it easier to get more attention and interest on the subject.

The use of the proposed formal methods steps in accident investigation was not demonstrated in this thesis. Both the AIBN-method and CAST-method is exemplified in the thesis, and doing the same for formal method would have made this thesis more relevant.

Studying the STAMP theory and CAST-method without any training courses or external input proved to be difficult. The demonstration of the CAST-method would probably be better if I had more training in the use of STAMP. The CAST demonstration in this thesis mainly focuses on the control structure and analysis of elements. The causal loops and unsafe control actions should have been given more focus, and been demonstrated in the thesis.

6.10 Future research

A recommended approach for using formal methods in accident investigation was proposed in this thesis, but it was not demonstrated. This was mainly due to a lack of detailed information about the requirements for the involved system. Future research should demonstrate the use of the proposed approach for using formal method for a case example, in order to study how the different steps can be performed.

The literature points to other systemic methods which has not been studied in this thesis. In order to fill this gap it is recommended to continue the exploration of systemic methods, and expand the AIBN "toolbox" with more tried and tested methods in the future.

The review on literature on accident investigation should be conducted at least every five years. It is stated in the SKI report (2008) "*it must be expected that by five or ten years the described methods will have been partly obsolete because the nature of socio-technical systems change, and therefore accidents tend to change also*". How such a review could be regularly conducted, and by who, could be a task for future research.

Salmon, Cornelissen and Trotter recommend the use of HFACS for class investigation of multiple accidents or incidents. AIBN is mainly investigating single accidents, but are occasionally also performing class-investigations. Future research could look into the need to use different methods in class-investigations.

This thesis has focused on how digital signalling systems can be investigated if they are involved in an accident. Digitalisation technology is also used to anticipate and prevent hazards, make maintenance smarter, and improve information for both travellers and train companies. How this technology such as "Internet of things", sensors, "big data" and machine learning can be used in accident investigations would be an interesting study.

7 Conclusion

The main objective was to study how a complex accident involving the railway signalling system European Rail Traffic Management System (ERTMS) systematically could be analysed and investigated. The study is based on literature review, meetings and discussions with supervisors, the Rail Accident Investigation Branch (RAIB) and others.

The literature study is divided in two parts, where the first part is general literature on the railway system and accident investigation methods. The second part is literature evaluating selected methods and the Systems-Theoretic Accident Model and Processes (STAMP) in particular. This literature is discussed in more detail, and how the findings relate to this thesis. This include Causal Analysis based on Systems Theory (CAST) and several articles that critically evaluate STAMP and the CAST-method.

The STAMP based CAST-method is studied and compared to the AIBN-method, in order to evaluate the benefit of using CAST as a systemic approach within the AIBN framework. In addition the possible use of formal methods as a specialised software investigation tool is evaluated.

A case example from the RAIB interim report on the loss of temporary speed restriction on the Cambrian ERTMS line has been used to demonstrate the AIBN- and CAST-methods. Reports and information about investigation of ERTMS related accidents are limited, and therefore the interim investigation by the RAIB was selected as a case example. This has made it difficult to obtain information about the investigation as the interim report contains a limited description and analysis of the accident. For elements that has been analysed to demonstrate the use of the method, it should be noted that some assumptions has been made. Therefor it is important to stress that the official investigation result is presented by the RAIB in their final report, and may not be in line with the results of this thesis.

Formal methods has been evaluated as a possible software investigation tool, similar to metallurgical, forensic or other specialised investigations. A flowchart and a series of questions is proposed to guide the investigation to systematically start a process towards the possible use of formal methods. This should help the investigation to narrow down the scope of the software investigation, and may reduce the initial need of expert help in the beginning.

A combination of the AIBN-method and CAST-method is considered to give the best result in the investigation of an ERTMS accident. For the control-structure part of the CAST-method the thesis has introduced more elements to visualise the actors and hazards to improve the graphical output. The AIBN-method and CAST-method has several similarities, but also proved to have different areas of strengths and weaknesses. At the start of the analysis it was easier to use the AIBN-method while the CAST-method was better as more information was collected and understood. To ease the use of CAST in the start-up of investigations this thesis therefore proposes a switch in the steps that the CAST-method is normally set out to follow. The strength of the AIBN-method is that it helps the team to focus and identify connections between the sequence of events, and risk factors at various levels in the socio-technical system. However when analysing the system development aspects of the case example, the CAST-method gave a better framework for analysing these factors in relation to the operational factors. The CAST-method also has more tools to guide the user in the analysis of both technical and human elements, than the AIBN-method. The AIBN-method is a framework that offers great freedom to choose the appropriate method, but this also limits the details in the guidance material.

The result of this study demonstrates that the CAST-method adds value to the framework of the AIBN-method, and that formal methods are a possible tool for investigation software. It is therefore recommended to include guidance material on the CAST-method and the formal method approach as possible tools in the framework of the AIBN-method.

8 Bibliography

[1] Accident Investigation Board Norway, "Report on abnormal signal observation at Atna station Rørosbanen 6 January 2015," Accident Investigation Board Norway, Lillestrøm, 2016.

[2] Bane NOR, "Norge får Europas mest moderne jernbane: Bane NOR digitaliserer for 20 milliarder,," 2018. [Online]. Available: http://www.banenor.no/Nyheter/Nyhetsarkiv/2018/norge-far-europas-mest-moderne-jernbane-bane-nor-digitaliserer-for-20-milliarder/.

[3] J. S. Erik Hollnagel, "Study on Developments in Accident Investigation Methods: A Survey of the ”State-of-the-Art.," Swedish Nuclear Power Inspectorate, Stockholm, 2008.

[4] Salmon, "Systems-based acident analysis methods: A comparison of Accimap, HFACS and STAMP," *Safety Science*, no. 50, pp. 1158-1170, 2012.

[5] P. &. W. P. Underwood, "A critical review of the STAMP, FRAM and Accimap systemic accident analysis models," in *Advances in Human Aspects of Road and Rail Transportation, Chapter: 39*, CRC Press, 2012, pp. 385 - 394.

[6] European Parliament, Council of the European Union, "Railway Safety Directive," 2004. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32004L0049&from=EN.

[7] N. G. Leveson, Engineering a safer world, Cambridge, Massachusetts: Massachusetts Institute of Technology, 2011.

[8] European Commission , "ERTMS - History of ERTMS," [Online]. Available: https://ec.europa.eu/transport/modes/rail/ertms/general-information/history_ertms_en.

[9] European Commission, "Communication from the Commission to the European Parliament and the Council on the deployment of the european rail signalling system ERTMS/ETCS," 2005. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:52005DC0298.

[10] European Commission., "ERTMS - Work Plan of the European Coordinator," European Commission, Brussels Belgium , 2015.

[11] EUROPEAN COMMISSION, "Delivering an effective and interoperable European Rail Traffic Management System (ERTMS) – the way ahead," EUROPEAN COMMISSION, Brussels, 2017.

[12] European Commission, "The countries," 2019. [Online]. Available: https://ec.europa.eu/transport/modes/rail/ertms/countries_en.

[13] European Commission , "ERTMS - What is ERTMS?," [Online]. Available: https://ec.europa.eu/transport/modes/rail/ertms/what-is-ertms_en.

[14] UNISIG, "ERTMS - Signaling levels," [Online]. Available: http://www.ertms.net/?page_id=42.

[15] European Commission, "ERTMS - Specifications and Legislation," [Online]. Available: https://ec.europa.eu/transport/modes/rail/ertms-european-rail-traffic-management-system/ertms-specifications-and-legislation_en.

[16] European Parliament, "Directive 2008/57/EC of the European Parliament and of the Council of 17 June 2008 on the interoperability of the rail system within the Community," 17 06 2008. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32008L0057.

[17] European Commission, "2014/897/EU: Commission Recommendation of 5 December 2014 on matters related to the placing in service and use of structural subsystems and vehicles under Directives 2008/57/EC and 2004/49/EC of the European Parliament and of the Council Text with EEA rel," 5 12 2014. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32014H0897.

[18] European Parliament, "Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union," 11 05 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016L0797.

[19] European Commission, "Commission Regulation (EU) 2016/919 of 27 May 2016 on the technical specification for interoperability relating to the 'control-command and signalling' subsystems of the rail system in the European Union," 27 05 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016R0919.

[20] CENELEC, "European Standards Organizations (ESOs)," [Online]. Available: https://www.cenelec.eu/aboutcenelec/whoweare/europeanstandardsorganizations/index.html.

[21] EN50126, "Railway Applications: The specification and demonstration of Reliability, Availability, Maintainability and Safety," CENELEC, International Electrotechnical Commisssion, IEC, 1999.

[22] EN50128, "Railway applications: Communication, signalling and processing systems, Software for railway control and protection systems," CENELEC, International Electrotechnical commission (IEC), 2011.

[23] EN50129, "Railway applications: Communication, signalling processing systems, Safety related electronics systems for signalling," CENELEC, International Electrotechnical Commission commission (IEC), 2003.

[24] European Union Agency for Railways, "Report on Railway Safety and Interoperability in the EU 2018," European Union Agency for Railways, Luxembourg, 2018.

[25] E. U. A. f. Railways, "European Rail Accident Information Links," [Online]. Available: https://erail.era.europa.eu/.

[26] M. W. Albert, "Undersøkelse av komplekse ulykker i den digitaliserte jernbanesektoren," Norges teknisk-naturvitenskapelige universitet (NTNU), Trondheim, 2018.

[27] Accident Investigation Board Norway, "Methodology," 2019. [Online]. Available: https://www.aibn.no/About-us/Methodology.

[28] N. G. L. a. J. P. Thomas, "STPA Handbook," Nancy Leveson and John Thomas, 2018.

[29] Partnership for Systems Approaches to Safety and Security (PSASS), "Partnership for Systems Approaches to Safety and Security (PSASS)," 2019. [Online]. Available: http://psas.scripts.mit.edu/home/.

[30] C. Perrow, Normal accidents: Living with high risk technologies, New York: Basic Books, Inc., 1984.

[31] J. Rasmussen, "Risk management in a dynamic society: A modelling problem.," *Safety Science 27,* pp. 183-213, 1997.

[32] S. Sklet, "Comparison of some selected methods for accident investigation," *Journal of Hazardous Materials,* pp. 29-37, 13 April 2004.

[33] N. Leveson, "A New Accident Model for Engineering Safer Systems," *Safety Science,* no. 42, pp. 237-270, 2004.

[34] Z. H. Qureshi, "A review of accident modelling approaches for complex critical," Technical report DSTO-TR-2094, Defence Science and Technology Organization, Edinburgh, Australia., 2008.

[35] M. Rausand, "Risk assessment: theory, methods, and applications," John Wiley & Sons, Inc., Hoboken, New Jersey., 2011.

[36] P. C. M. a. T. M. Salmon, "Systems-Based Accident Analysis Methods: A Comparison of Accimap, HFACS, and STAMP," *Safety Science, 50,* pp. 1158-1170, 2011.

[37] T. Hardy, "Software and system safety: promoting a questioning attitude," in *Proceedings of the Australian System Safety Conference - Volume 145*, Brisbane, Australia, 2012.

[38] T. L. Hardy, Software and System Safety : Accidents, Incidents, and Lessons Learned, Bloomington, United States: AUTHORHOUSE, 2012.

[39] P. a. W. P. UNDERWOOD, "Accident analysis models and methods: guidance for safety professionals," Loughborough University, Loughborough, 2013.

[40] J. S. a. L. B. Jr, "What do STAMP-based analysts expect from safety investigations?," *Procedia Engineering,* no. 128, pp. 93-102, 2015.

[41] Rail Accident Investigation Branch, "Interim Report - Loss of speed restrictions on the Cambrian line 20 October 2017," Rail Accident Investigation Branch, Department for Transport, Derby UK, 2018.

[42] A. Dong, "Application of CAST and STPA to Railroad Safety, MIT Master's Thesis," 05 2012. [Online]. Available: http://sunnyday.mit.edu/safer-world/Airong-thesis.pdf.

[43] Dajiang, "A System Theoretic Analysis of the "7.23" Yong-Tai-Wen Railway Accident," 04 2012. [Online]. Available: http://sunnyday.mit.edu/train-accident-suo.doc.

[44] Railway Traffic Accident Investigation Team, "7 · 23 ” Wenzhou Special Railway Traffic Accident Investigation Report," Ministry of Emergency Management of the People's Republic of China, 28 12 2011. [Online]. Available: http://www.chinasafety.gov.cn/gk/sgcc/tbzdsgdcbg/2011/201112/t20111228_245242.shtml.

[45] U.S. Department of Energy, Washington D.C., DOE Handbook Accident and Operational Safety Analysis Volume I: Accident Analysis Techniques., Washington D.C.: U.S. Department of Energy, Washington D.C., 2012.

[46] Transportation Safety Board of Canada, *Guide to Investigation for organizational and management factors - 2nd Edition.,* Transportation Safety Board of Canada, 2014.

[47] Australian Transport Safety Bureau (ATSB), *Safety Investigation Guidelines Manual – Analysis. Version 1.07,* Australian Transport Safety Bureau, 2015.

[48] J. P. T. Nancy G. Leveson, "STPA Handbook," MiT (PSASS), Massachusetts, 2018.

[49] U.S. DEPARTMENT OF DEFENSE, "Joint Software Systems Safety Engineering," Naval Ordnance Safety and Security Activity, 2010.

[50] ERTMS Solutions, "ERTMSFormalSpecs now completed !," 27 3 2018. [Online]. Available: https://www.ertmssolutions.com/press/ertmsformalspecs-now-completed/. [Accessed 2019].

[51] openETCS, "European Train Control System (ETCS) - Open Proofs - Open Source," [Online]. Available: http://openetcs.org/. [Accessed 2019].

[52] ITEA, "openETCS," [Online]. Available: https://itea3.org/project/openetcs.html.

[53] Nancy Leveson, Writer, *Engineering a Safer and More Secure World.* [Performance]. MiT, 2011.

[54] T. a. Malmquist, "Partnership for Systems Approaches to Safety and Security," 2017. [Online]. Available: http://sunnyday.mit.edu/Thomas-Malmquist-ISASI.pdf.

[55] T. Hardy, "Software and System Safety," 2012.

9 Attachments

Annex A – Terje Sivertsen - Formal methods in Bane NOR (translated from Norwegian)

Annex B – Terje Sivertsen - Bane NOR as a competent customer (translated from Norwegian)

Annex C – Flowchart of the process of using formal methods in software investigation, enlarged

Annex D – AIBN-method, enlarged

Annex E – CAST control structure, enlarged

9.1 Annex A - Authored by: Terje Sivertsen.

This text is originally written in Norwegian and translated to English for use in this thesis.

Norwegian experience with formal methods

The railway signalling system NSB-94 is Bane NOR's proprietary software-based signalling system. The system is based on Bane NOR's relay-based signalling system (NSI-63 and later), but the interlocking logic is implemented in PLC software instead of relays.

The software design for NSB-94 systems is specified through the functional and design specifications. These consist mainly of Boolean equations that define the functions (variables) to be calculated, along with a specification of the calculation order. The equations in the function specification are implemented almost directly in program code. It is relatively easy to see the relation between the equations and the program code, which facilitates the verification that the program code is a correct implementation of the function specification.

PLS is microprocessor-based but has functionally and logically many similarities with traditional relay-based systems. One of the explanations for the great prevalence is the possibilities this has given for a smooth transition from old to new technology. This was also an important factor when the National Rail Administration around 1990 introduced the use of PLC in signalling systems, first for less critical functions (NSB-87) and later also for the system's safety related functions (NSB-94).

A PLC program is written in an imperative programming style that conceptually associates logical conditions with the setting of switches, which in turn reflects the similarity with relay-based systems. The logical conditions are expressed as Boolean values, based either on outside input or on stored data. The setting of switches consists in sending Boolean values out to the outside world in the form of currents which are optionally used to set physical relays used for controlling external components.

The logical structure of the equations in the function specification, and the way these are encoded in the PLC, has facilitated so-called formal verification of the software in the NSB-94 facilities, based on a representation of the function specification and the program code in a formal notation based on mathematical logic. This verification has been twofold in that it is verified:

- that the functional specification meets specified, functional safety requirements, and
- that the program code is a correct implementation of the function specification.

Together, these verifications result in the program code meeting the safety requirements. By dividing the verification in this way, several alternative implementations of the same feature specification can be verified by performing only other parts specifically for each implementation. This has practical significance not least in the case of changes and corrections to the program code.

The formal verification is made possible by establishing formal mathematical models of safety requirements, functional specification and program code, and using a suitable analysis tool to verify relationships between them. In order to facilitate this, the infrastructure manager prepared at the beginning of the 2000s a document that formulated all safety-related functional requirements that should be made to the NSB-94 facilities. Formal verification of these facilities, according to the principles described above, has been carried out on behalf of the infrastructure manager by the Swedish company Prover, based on a patented method.

One of the advantages of the described formal verification approach is that methodological analysis of the functionality of a system and the implementation of this functionality are differentiated. This can be exploited directly in connection with investigations of accidents and incidents where safety issues cannot be excluded in the software of the system concerned.

If it is suspected that the specified functionality has safety weaknesses, the survey can initially analyse the actual specification. One current approach is:

1. Formulate safety requirements it is expected that the specification meets and which functionally contradicts the relevant situation, in the sense that if the safety requirement is fulfilled, the relevant situation cannot arise.
2. Examine whether the safety requirement has already been verified fulfilled by the specification.
3. If the safety requirement is not already verified, a formal verification is made that the specification meets the safety requirement.

The method is in accordance with what is done with the actual provision of the system, and can therefore be carried out with the same methodology. If safety deficiencies are not detected in the specification itself, it is natural that the investigation focuses on the program code that implements this. One current approach is:

1. Check if the specification has already been verified fulfilled by the program code.
2. If the specification is not already verified, a formal verification is made that the program code meets the safety requirement.

Again, the same methodology can be used as during the procurement of the system. From this sketch of the procedure we can conclude among other things the following:

- If formal verification has already been carried out for the procurement of the signalling system in question, it is well arranged for the use of formal verification also with any investigations after the system has been put into use.
- Formal verification in any accident investigations can follow the same methodology as in obtaining the system.
- If, during the procurement of a signalling system, it was verified that the program code meets the specification, and the specification and program code have not been changed later, it is natural to focus on any safety deficiencies in the specification.

This procedure can in principle also be followed for other types of systems than the NSB-94, including older relay-based plant types. Instead of basing the models on the functional specification and the program code for the facility, it will then be based on the relay schemes and their physical implementation.

In general, the question of the applicability of formal methods for investigating incidents and accidents can be answered by asking if formal methods could have been used in the procurement of these systems. As shown above, there are good reasons to expect the same methods and approaches to be used in both cases.

At Bane NOR, chief engineer Terje Sivertsen has carried out an independent R&D work with the aim of establishing an alternative methodology based on his own developed tool HALDEN Prover (Halden Algebraic Language and Design ENvironment Prover) and the specification language HALDEN ASL (Algebraic Specification Language). HALDEN Prover is a non-commercial tool that supports a number of activities related to this, including automatic evidence in the verification of specifications, design and program code. In this work, Sivertsen looked at the application possibilities for formal methods in various parts of a system's lifecycle, represented by signalling systems of the type NSB-94. The research questions in this work have attempted to answer whether formal methods can contribute to:

- implementing the CENELEC standards in such a way that the entire RAMS process is supported and not just individual activities;
- integrating the various processes, activities and techniques in the RAMS process;
- raising the integrity of the RAMS process by also formalizing parts of the process not usually supported by such methods;
- making verification more explicit and explicit;
- improving the traceability of requirements through the various life cycle phases;
- making verification more effective, both for generic applications, for specific applications and for changes thereto; and
- improving existing processes related to the development and safety demonstration of the railway's safety facilities.

How and to what degree the research work is capable of answering these research questions lies beyond the present thesis, but the questions indicate the type of issues Bane NOR has looked into more closely in the question of the application possibilities for formal methods.

9.2 Annex B - Authored by: Terje Sivertsen.

This text is originally written in Norwegian and translated to English for use in this thesis.

Bane NOR as a competent customer

In connection with the acquisition of signalling systems, Bane NOR bases itself on a distribution of responsibility between the customer and the supplier that is reflected in EN 50126. This means that the customer and the supplier have the main responsibility for different parts of a system's life cycle, where the customer will normally have the main responsibility for the life cycle phases up to validation of system requirements and later from system acceptance and onwards. The supplier, in turn, will have the main responsibility for the part of the life cycle that is based on the validated system requirements and proceeds to the validation of the system itself. In addition, the supplier will naturally be involved later in connection with maintenance, in the form of error correction, improvements, etc.

The need for expertise on the customer side will of course be particularly important where the customer has the main responsibility, for example in connection with the risk assessments that must be carried out in order to determine the safety requirements for the system. This competence must be understood from the customer's overall responsibility for operational safety. This responsibility means that the customer is able to determine the requirements that various systems must fulfil in order for the customer to be able to fulfil this responsibility in a satisfactory manner.

However, the customer's competence needs should not be limited to the life-cycle phases in which the customer has the overall responsibility. Being a competent customer also means being able to follow up the supplier to uncover any shortcomings in the systems delivered. Such expertise will be important in order to be able to judge whether the systems in question are suitable for use in their intended environment. This means, among other things, the possibility of being able to uncover whether the supplier has misunderstood the customer's requirements and expectations. During the development, problems may also arise where clarifications between Bane NOR and the supplier are necessary, for instance in cases where one of the parties wishes to deviate from the system requirement specification. Such clarifications will typically require assessments of whether the deviations are acceptable, which in turn may require a revision of previously performed verifications, for example against Bane NOR's rules and requirements or against the analyses carried out during the risk assessment process which were used as the basis for establishing the system requirement specification.

The need to be a competent customer can be linked, among other things, to the establishment of the requirement specification the customer enters into the market with. This specification is intended to express the customer's requirements and wishes for the procurement, and has significance primarily for the choice of supplier and system type. The fact that the specification is used as the basis for the offer gives Bane NOR a good negotiating position with the supplier. The supplier has offered to deliver a system that meets Bane NOR's requirements, and Bane NOR will thus have a better basis for negotiating any changes in price and delivery time related to deviations from these requirements. This presupposes, however, that the requirement specification to the greatest possible extent meets criteria for precision, clarity, unambiguity and other matters important to ensure agreement between the customer and the supplier when it comes to the interpretation of the requirements.

Based on EN 50126, being a competent customer will also be reflected in how verification and validation are performed in the different life cycle phases. For software, this means, first, that the vendor must demonstrate that the software development and securing processes effectively detect potential safety-related errors. Furthermore, the customer (Bane NOR) must carry out a risk assessment at the overall railway system level, verify that this has been satisfactory with regard to being able to establish any safety requirements, and verify that the safety requirements have been handled further in the process.

The distribution of responsibility between the railway operations and the supplier is reflected through a corresponding split of responsibility for verification and validation. It is therefore natural that both parties have designated responsibilities for these activities. Although safety is one project, two parties are responsible for each part of the process. Compliance with the CENELEC standards therefore implies that a Verifier and Validator have been designated both by the railway company and the supplier, and that it can be referred to, for example, "Bane NORs verifying". Understanding that it is about "one project" is also important for how these roles coordinate their tasks across the organizational boundaries. This applies not least in connection with the validation of the system requirements.

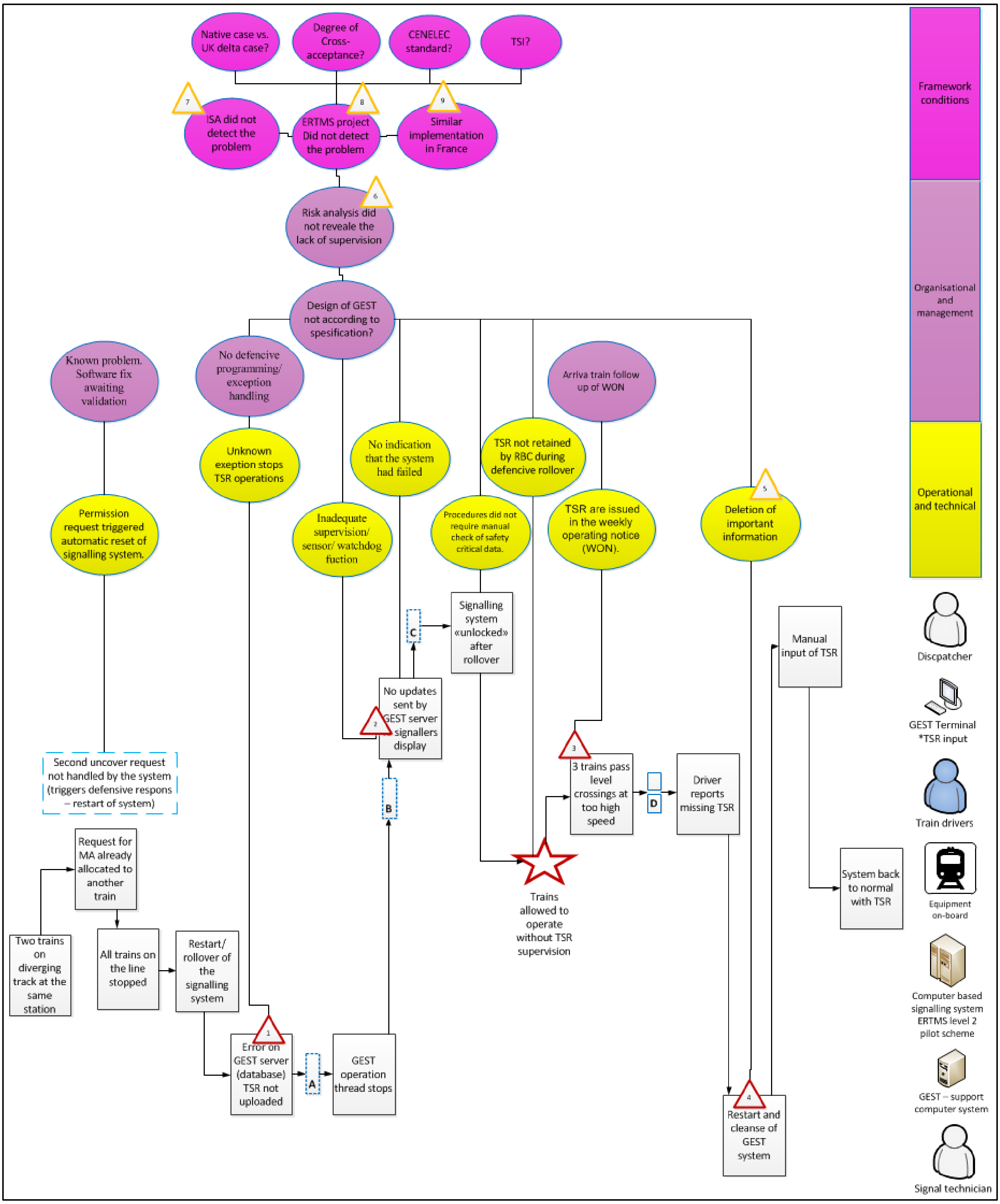
Being a competent customer is also reflected in connection with so-called acceptance testing, which is performed to check that the acceptance criteria are met. This generally does not include the tests that the supplier performs as part of its development process, but can be carried out by the supplier under the customer's supervision upon agreement. Acceptance testing can be considered as verification in the sense that it is performed to verify the fulfilment of claims. Acceptance testing is usually based on specified requirements and tests, supplemented when needed with ad-hoc tests.

The use of the role Validator in Bane NOR's projects must be seen in conjunction with both the validation tasks under Bane NOR's responsibilities and with the necessity of dealing with the validations performed by the supplier. According to their respective areas of responsibility, Bane NOR and the supplier will normally emphasize their validation activities differently. As Bane NOR's projects are to follow up the suppliers to ensure that an acceptable system is provided, the projects must be able to assess the validations carried out by the suppliers. Often, the most appropriate will be that Validator in Bane NOR's project performs these assessments as part of their validation. Bane NOR's Validator will thus both carry out their own validations and evaluate others', related to the entire life cycle of the system. The principle is the same if this role is taken care of by different people through the life cycle of the system.

Due to the wide field of validation activities Validator either to carry out or evaluate, Bane NOR's Validator will need expertise on more than the activities for which Bane NOR has the main responsibility. In this way, Validator will be better equipped to answer the questions that have to come up through the system's life cycle, and thus contribute to Bane NOR acting as a competent customer. This competence can prove crucial to ensure that both Bane NOR and the supplier perform the validation activities that are necessary and that they are carried out in a manner that provides a sufficient basis for acceptance of the delivered system.

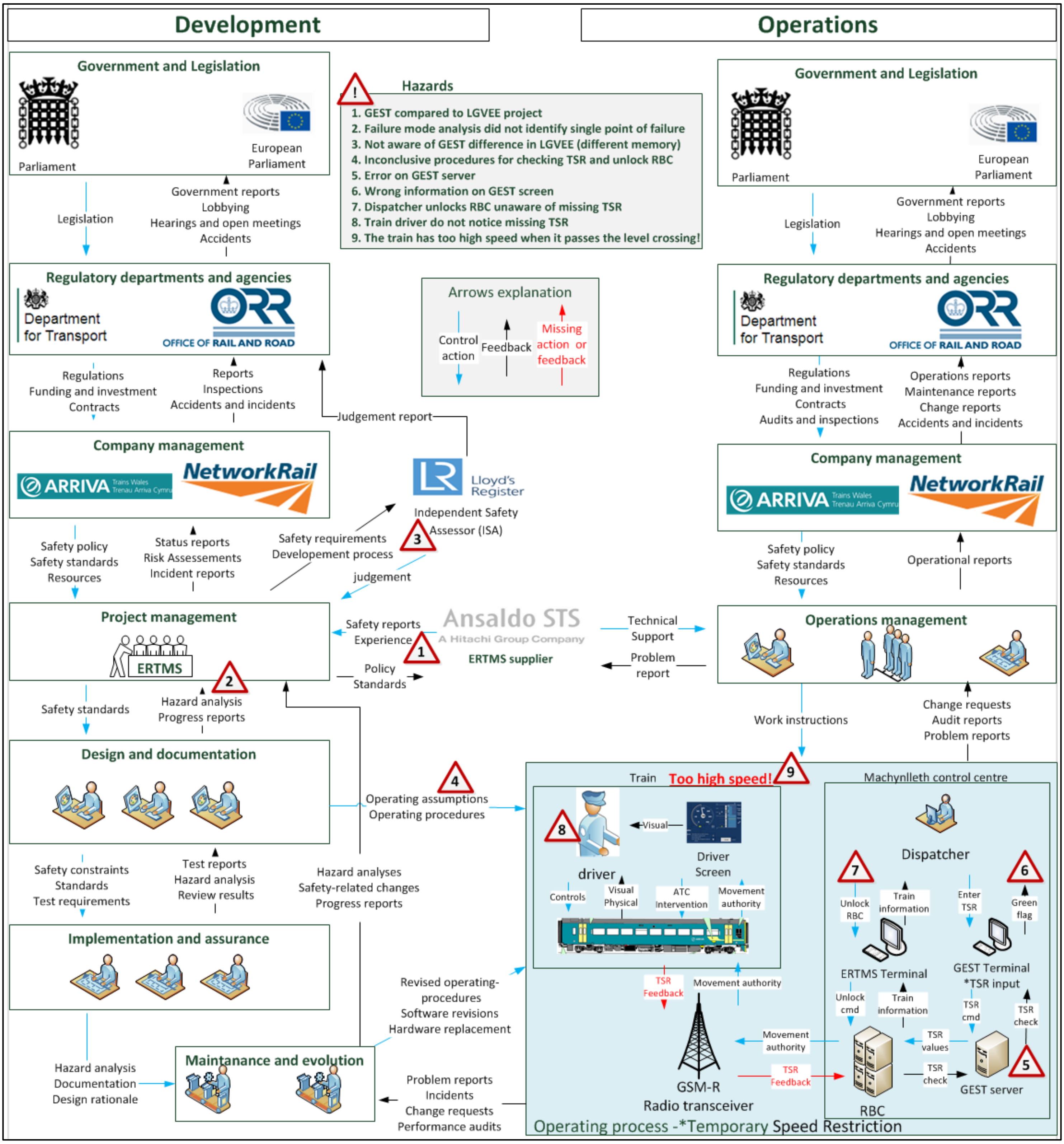
9.3 Annex C – AIBN-method large picture

AIBN-method


Native case vs. UK delta case?
Degree of Cross-acceptance?
CENELEC standard?
TSI?
Framework conditions
7
ISA did not detect the problem
8
ERTMS project Did not detect the problem
9
Similar implementation in France
6
Risk analysis did not reveal the lack of supervision
Organisational and management
Design of GEST not according to spesification?
Known problem. Software fix awaiting validation
No defencive programming/ exception handling
Arriva train follow up of WON
No indication that the system had failed
TSR not retained by RBC during defencive rollover
Unknown exeption stops TSR operations
Operational and technical
Permission request triggered automatic reset of signalling system.
Inadequate supervision/ sensor/ watchdog fuction
Procedures did not require manual check of safety critical data.
TSR are issued in the weekly operating notice (WON).
5
Deletion of important information
Signalling system «unlocked» after rollover
C
Manual input of TSR
Discpatcher
No updates sent by GEST server signallers display
2
GEST Terminal *TSR input
3
3 trains pass level crossings at too high speed
D
Driver reports missing TSR
Train drivers
Second uncover request not handled by the system (triggers defensive respons – restart of system)
B
Trains allowed to operate without TSR supervision
System back to normal with TSR
Equipment on-board
Request for MA already allocated to another train
Two trains on diverging track at the same station
All trains on the line stopped
Restart/ rollover of the signalling system
Computer based signalling system ERTMS level 2 pilot scheme
1
Error on GEST server (database) TSR not uploaded
A
GEST operation thread stops
GEST – support computer system
4
Restart and cleanse of GEST system
Signal technician

9.4 Annex D – CAST control structure large picture

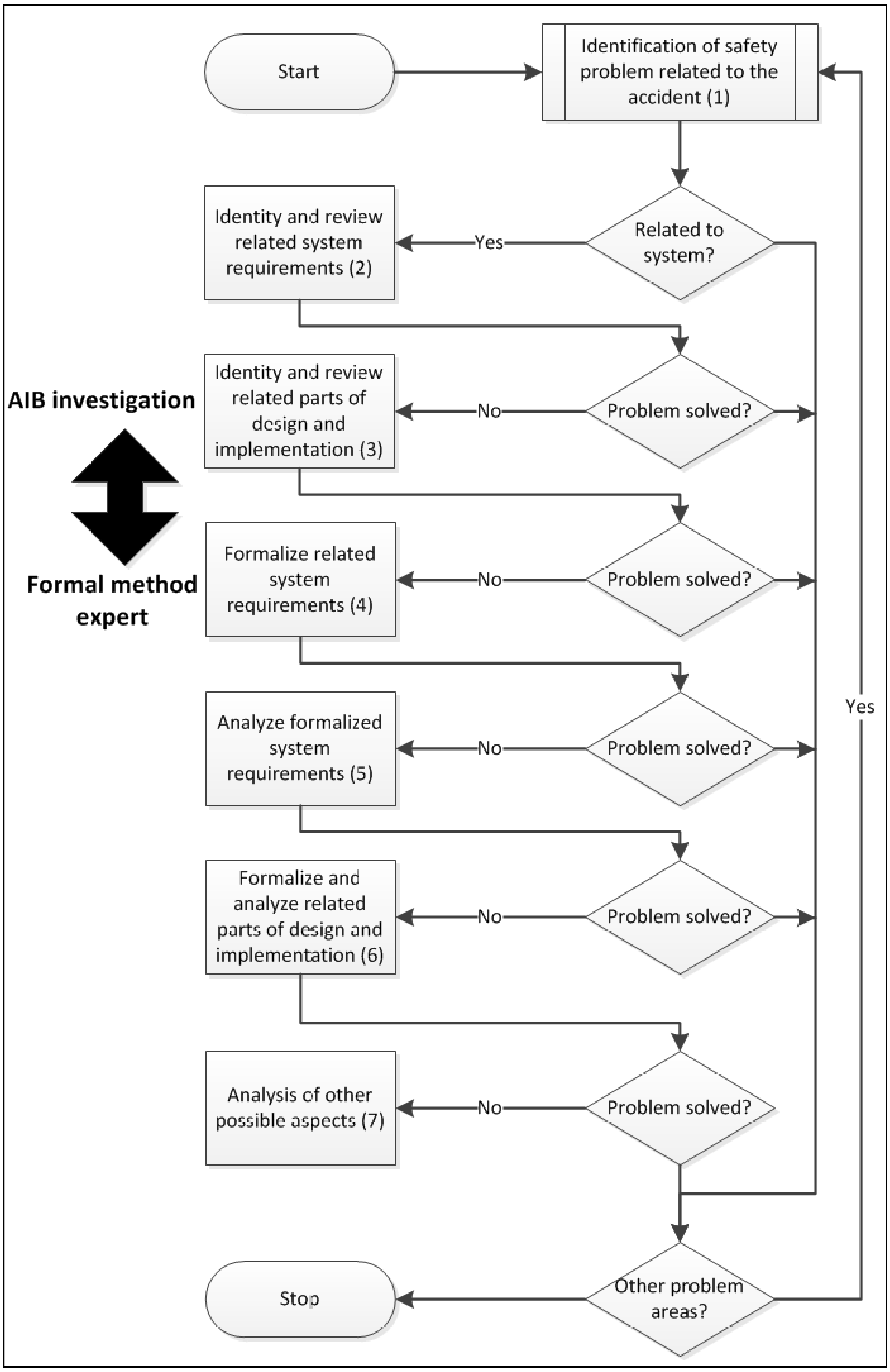
CAST control structure


Hazards

1. GEST compared to LGVEE project
2. Failure mode analysis did not identify single point of failure
3. Not aware of GEST difference in LGVEE (different memory)
4. Inconclusive procedures for checking TSR and unlock RBC
5. Error on GEST server
6. Wrong information on GEST screen
7. Dispatcher unlocks RBC unaware of missing TSR
8. Train driver do not notice missing TSR
9. The train has too high speed when it passes the level crossing!

9.5 Annex E – flow chart formal method large picture

Flowchart of the process of using formal methods in software investigation


Start
Identification of safety problem related to the accident (1)
Related to system?
Yes
Identity and review related system requirements (2)
AIB investigation
Formal method expert
Problem solved?
No
Identity and review related parts of design and implementation (3)
Problem solved?
No
Formalize related system requirements (4)
Problem solved?
No
Analyze formalized system requirements (5)
Yes
Problem solved?
No
Formalize and analyze related parts of design and implementation (6)
Problem solved?
No
Analysis of other possible aspects (7)
Stop
Other problem areas?

NTNU
Norwegian University of
Science and Technology