J.C. Aantjes

System reliability analysis of interactions between ETCS, train drivers and dispatchers, demonstrated by STPA

Master Thesis
Construction Management & Engineering

System reliability analysis of interactions between ETCS, train drivers and dispatchers, demonstrated by STPA

By

J.C. Aantjes

in partial fulfilment of the requirements for the degree of

Master of Science
In Construction Management & Engineering

This project is proposed as my master thesis at the Delft University of Technology
in cooperation with ProRail.
to be defended publicly on the 29th of September, 2022 at 5 PM.

Thesis committee
Prof. dr. ir. P.H.A.J.M. van Gelder (chair), Delft University of Technology
Prof. dr. R.M.P. Goverde, Delft University of Technology
Ir. W.M.T. Mennen, MBA, ProRail
Drs. G.M. Verduijn, ProRail

An electronic version of this thesis is available at http://repository.tudelft.nl/
Cover image: Two combined trains on Utrecht central station. Source: Julian Aantjes, 2022

Preface

This thesis concludes my studies in Construction Management and Engineering at the Delft University of Technology. Writing this thesis was like climbing a mountain to achieve a master's degree on the summit of my study. The journey started with a good preparation of the climb, a suitable subject of interest was selected, conversations were started and documents were written for the journey kick-off. I had no experience with similar climbs that were about the hazard analysis technique STPA or about the railway transport system. The inexperience made the terrain more difficult to walk through, but also more educational.

The thesis journey was executed individually, but thankfully there were a number of people who guided and supported in my journey. I would like to thank my company supervisors Gertruud Verduijn and Wendi Mennen for the weekly encouragements, the helpful feedback and the trust in my research. I found the contact very pleasant. In addition, I would like to thank my other colleagues at the ERTMS Programme Management for all the lunch walks and laughs during my time at the office. A special thanks goes to Ton Harteman who helped me a lot with research specific information.

I'm grateful for the supervisors of the TU Delft. I would like to thank Pieter van Gelder and Rob Goverde for their support and detailed academical and textual feedback on my thesis. The meetings were meaningful and constructive, those meetings made me improve the quality of my work throughout the process.

Last but not least, I could not reach the summit of this journey, without the support of my wife, family and friends that had to listen to me talking about the struggles of graduating and the created passion for the railway transport system. While writing this preface, I can look down to the walked path, and see all the dead ends I walked in and the help I got to proceed. After all, the views for reaching the summit were fully worth it and I will continue with another journey.

Enjoy reading.

Julian Aantjes   Delft, 2022

Summary

The Dutch railway transport system is a system of systems and also a sociotechnical system that will migrate to a radio-based signalling standard ERTMS (European Rail Traffic Management System). ERTMS will influence the train drivers and dispatchers the most, especially due to the introduction of the signalling and control element of ERTMS: the European train control system (ETCS). A reliability requirement for the migration towards ERTMS obligates to demonstrate that the reliability of the system stays the same or improves. Reliability can be quantified if all the possible risks are known, but identifying risks with traditional models is insufficient, because they do not capture the complexities and dynamics of socio-technical systems.

The hazard analysis technique 'systems theoretic process analysis' (STPA) is a promising technique to sufficiently identify hazards that models the system in a control structure and searches systematically for hazards. The main research question of this thesis is: 'To what extent can STPA be applied to identify risks and determine the system reliability of interactions between ETCS, train drivers and dispatchers?' What are the risks caused by those interactions and how can STPA be applied for an effective risk assessment are the two research objectives.

This is researched by doing a desk research about the change that ERTMS will bring, the way reliability is demonstrated in the railway transport system and how STPA can be applied in the railway transport system. After that, STPA is applied for analysing the procedure for combining two trains that arrive from opposite directions. And lastly, three in-depth interviews are conducted to reflect on STPA and investigate how STPA can be implemented in an organisation.

STPA consists of 4 structured steps. First the analysed system is described and the purpose of the analysis is set. The system is modelled in a control structure in the second step, this structure illustrates the control actions (the downward facing arrows) that the controller performs on the controlled process, the upward facing arrows are feedback and the horizonal arrow is a communication channel. The figure below illustrates the developed control structure for the analysed procedure. In this structure, 4 different actors are present, the drivers, the dispatcher, the trackside system (this concerns all the (sub)systems that are available for the dispatcher) and the train systems (this concerns all the (sub)systems that are available for the driver). The third step of STPA is to identify unsafe control actions with guided words. 27 unsafe control actions are identified for the 8 control actions that are present in the control structure. The last step of STPA is to identify loss scenarios that could lead to the unsafe control actions, those were formulated with system experts.

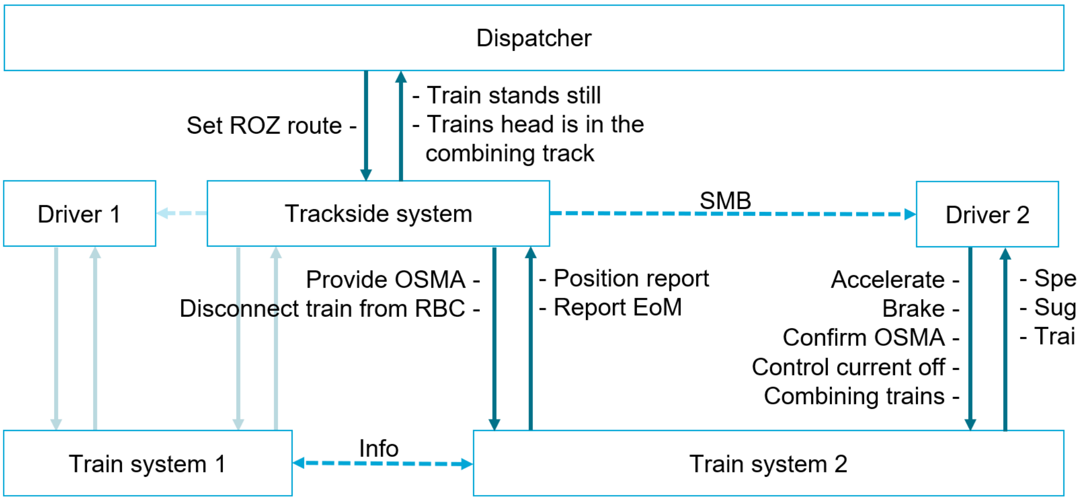


Figure: Control structure of the procedure for combining two train that arrive from opposite directions.

The desk research and this research demonstrates that STPA is completer and more thorough in identifying hazards than the tradition hazard analysis technique ‘failure mode effect and criticality analysis’ (FMECA). In this research, STPA identified 70 loss scenarios in the analysed procedure (compared to 4 issues identified with FMECA), those hazards ranged from missing or inadequate feedback mechanisms to inconsistent process models of the train drivers or dispatchers. STPA identified besides technical failures also design flaws in the procedure and unsafe interaction between the ETCS, train drivers and dispatchers.

Besides the conclusion that STPA turned out to be more complete and thorough in identifying hazards, another advantages of STPA is that performing STPA is very structured and not superficial. An identified disadvantage of STPA is that the method stops immediately after the hazards are defined. Determining the probability of occurrence and the impact expressed in train delay minutes can result in prioritization of the hazards and a better risk assessment.

To conclude, this research recommends applying STPA for complex systems where multiple controllers are involved. An STPA expert, someone who has experience with applying STPA in different projects, is a key to successfully implement STPA in an organisation.

Table of contents

List of figures

List of tables

Definition of terms

ERTMS Programme Management	Organisation that is responsible for directing the implementation of ERTMS in the Netherlands.
Hazard	A system state or set of condition that has the potential to lead to a loss.
Loss	Something unacceptable to the stakeholders
Reliability	1 minus the probability of failure (R=1-F)
Risk	Potential (negative or positive) effect of an event, determined by the probability of the event multiplied by the impact when it occurs.

List of abbreviations

ATB-EG	Automatische Treinbeïnvloeding - Eerste Generatie (Dutch ATP system)
ATB-NG	Automatische Treinbeïnvloeding - Nieuwe Generatie (Dutch ATP system)
ATP	Automatic Train Protection
DMI	Driver Machine Interface
EoA	End of Authority
EoM	End of Mission
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
ETIS	ERTMS Train Information System
FME(C)A	Failure Mode, Effects, (Criticality) Analysis
FSMA	Full Supervision Movement Authority
IXL	Interlocking
LS	Loss Scenario
NTC	National Train Control
OS	On Sight
OSMA	On Sight Movement Authority
RBC	Radio Block Centre
ROZ	Driving On Sight (Dutch: Rijden Op Zicht)
SB	Stand By
SD	System Dynamics
SL	Sleeping
SMB	Stop Marker Bord
STM	Specific Transmission Module
STPA	Systems Theoretic Process Analysis
TSI	Technical Specifications for Interoperability
UCA	Unsafe Control Action

1.

Introduction

Signalling is crucial for train drivers due to the inability to swerve with a train and because the driver can't oversee the distance needed to come to a safe standstill. Signalling systems for railways have changed a lot since the train was first used. When the first railway lines were introduced, where multiple trains would drive over, no signalling systems were used to indicate if a railway was clear of other trains. Between 1830 and 1860, men were employed to signal with hand gestures how long ago another train has passed at that point. From 1841, so called semaphores were introduced to replace the hand gestures with a signal and train dispatchers made use of telegraphs to indicate if a train had left a section of a railway line. From the 1920s optical signals were introduced and electric circuits could indicate if a segment of a railway line was occupied by a train (Goverde, 2022). After World War II, European countries introduced automatic train protection (ATP) systems to increase the safety of the railway (Britannica, n.d.). These protection systems compare the actual train speed with the permitted speed. The permitted speed is indicated by lineside signalling (ERA, 2008). In other words, it supervises the train movement and ensures that the given movement authority is respected, this authority is indicated by lineside signals. Over the time, the signalling systems changed and currently some ATP systems in different parts of the world have been changed to a radio-based signalling standard ERTMS (European Rail Traffic Management System) (Unife, 2022).

1.1. ERTMS in the Netherlands

In the Netherlands, multiple ATP systems are used. Most main railway lines use the ATP system ATB-EG (automatische treinbeïnvloeding - eerste generatie), while most secondary lines use ATB-NG (automatische treinbeïnvloeding - nieuwe generatie) and a few lines are already equipped with ERTMS. The term new generation in ATB-NG may suggest that ATB-NG is an improvement on ATB-EG, but ATB-EG and ATB-NG are two different systems and not an upgraded version of each other.

ATB-EG and ATB-NG cooperate with the block signalling system NS'54. ATB-EG/NS'54 uses lineside signals and coded track circuits or balises that communicate the target speed limits to the trains. The ATP systems automatically intervene with an emergency brake intervention if the supervised speed is exceeded. In 1971 all passenger lines where equipped with a train detection system (track circuits or axle counters) to enable automatic block signalling. Some of the rail tracks are still equipped with the oldest track circuit cabling and those are on its technical end-of-life and need to be replaced (ERTMS Programme Management, 2019a; van den Top, 2007).

ATB-EG is limited to provide only 5 speed authorities (40, 60, 80, 130 and 140 km/h) with the highest enforceable speed of 140 km/h and only interferes with brakes supervision if train speeds are above 40 km/h. ATB-NG supervises every speed below 200 km/h in steps of 10 km/h and can also supervise speeds between 200 km/h and 300 km/h in steps of 20 km/h, but those high speeds are not applied in the Netherlands. While under ATB-EG, a signal is continuously sent to the train via coded track circuits, ATB-NG sends information via beacons at intermittent points on the infrastructure. There are two types of beacons used, the first one (block beacon) informs about the current applicable speed limit, the second (intermediate beacon) informs about the speed limit at the next block beacon. ATB-NG trainborne equipment calculates the required braking curve to the next signal and enforces an emergency brake if the braking curve speed is exceeded after a warning (ProRail, 2019).

The ATB systems have functioned well, but it does have limitations and drawbacks. The parliamentary committee Kuiken on rail maintenance and innovation, concluded that the current analogue automatic train protection system ATB-EG cannot deliver the desired performance for the 21st century train infrastructure (Kuiken, 2012). The Dutch parliament decided a national replacement of the ATB-EG and ATB-NG system by ERTMS before 2050 (Tweede kamer, 2019). Also, the EU forbids to upgrade legacy systems, unless a modification is deemed necessary to mitigate safety related defects in its system (EU, 2006).

Capacity increase

Besides the demands of the EU, a higher capacity of passenger rail transport is needed. Railways experience an increase in demand for passenger rail transportation. NS, a Dutch railway undertaking increased its overall mobility market share from 9.1% to 10.1% in the years 2010 till 2017, despite the reduction in amount of train track use (NS annual report, 2019). The Dutch railway system is already the most intensively used railway system in Europe, with 50.600 train kilometres per track kilometre in 2018 (CBS, 2009; Europese commissie, 2021), and one of the most intensively used in the world. On some corridors a capacity utilization is used that is above the international advised norm (UIC, 2004). ProRail expects an increase of 30 to 40% more train travellers by 2030, compared to the 1,5 million daily train users in 2019, so the capacity needs to grow even further (ProRail, 2020).

Increase of capacity can be met by improving or expanding the infrastructure or by improving the signalling system. ERTMS is seen as an improved signalling system, compared to the ATB-EG. The alternative of expanding the infrastructure is less preferable, because it is very costly. Implementing ERTMS level 2 will not directly ensure that more trains can run, but the robustness of the timetables will increase by more margins in the design and operation of the timetable. With ERTMS speeds above 140 km/h can be authorized, unlike in ATB-EG. But implementation of the increase speed is also dependent on other factors than the train protection system, such as the runway alignment, the rolling stock itself or the noise production.

ERTMS programme

ERTMS will be deployed in the Netherlands for 4 reasons: the technical end-of-life ATB-EG system components, European policy with obligations, need for digitization in the railway transport system and the benefits that can be achieved from roll-out (ERTMS Programme Management, 2019b). An ERTMS programme has been developed to replace the legacy ATP systems by ERTMS. With the implementation, 5 policy goals are drafted, to achieve benefits in safety, interoperability, speed, capacity and reliability (ERTMS Programme Management, 2019a; Mansveld, 2014).

ERTMS makes the step from analog to digital, it uses wireless communication between the train and the infrastructure. The position of the train is determined by an onboard odometry module and balises on the track. The train receives movement authority from the trackside and a dynamic speed profile including braking curves is computed over the route, until the end of authority. The allowed speeds are displayed on a driver-machine-interface (DMI) inside the train. If speed instructions are not followed, the system intervenes by brake intervention of the train (van der Weide et al., 2022). ERTMS is a uniform standardised train communication and safety system that can replace the fragmented national systems. It is not a product, but a specification, the industry must come up with products that meet the specification and are compatible. Cross-border interoperability and signalling procurement is the main political goal of ERTMS (Tessédre, 2004). ERTMS aims to improve the interoperability, safety, capacity, reliability, maintainability and competitiveness of the rail network in Europe

(Flammini, 2006; Unife, 2021a). The transition from the current automatic train protection systems in Europe toward the ERTMS is shown in Figure 1.

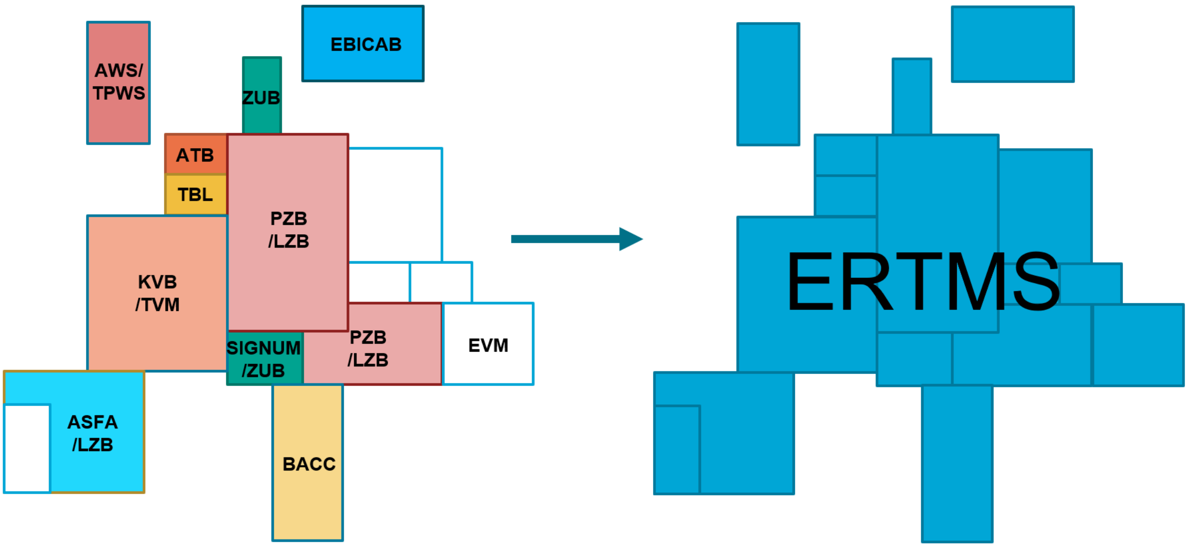


Figure 1: Simplified figure of the transition from the different national automatic train protection systems to a single European railway system (redrawn from ERA, 2017)

The ERTMS can be deployed in different levels and the Netherlands chose to go for the European train control system (ETCS) level 2 (ERTMS Programme Management, 2019a). Level 2 indicates the application level of ERTMS, the differences between the levels are briefly explained in section 2.1.

Implementation of ERTMS in the Netherlands will change technical systems in train and track, but will also significantly influence operational processes for train drivers and dispatchers. The ERTMS programme scope is diverse and will include the following points (ERTMS Programme Management, 2019b):

- ERTMS level 2, baseline 3, release 2 implemented on seven lines[1], see Figure 2.
- (Retro)fit more than 1300 equipment units.
- More than 60 user processes are added or modified.
- Approximately 200 different user-roles are influenced by ERTMS.
- 15000-18000 users are impacted, which need around 45000 days of training.

The changes to ERTMS are made to the existing railway system, a so-called brownfield. Figure 2 presents the geographic scope of the ERTMS programme.

[1] The lines: ‘Hanzelijn’ and ‘Noordelijke lijnen’ were later added to the scope. The Hanzelijn will be converted from a dual signalling line to ERTMS level 2 only (ministry of infrastructure and water management, 2021)

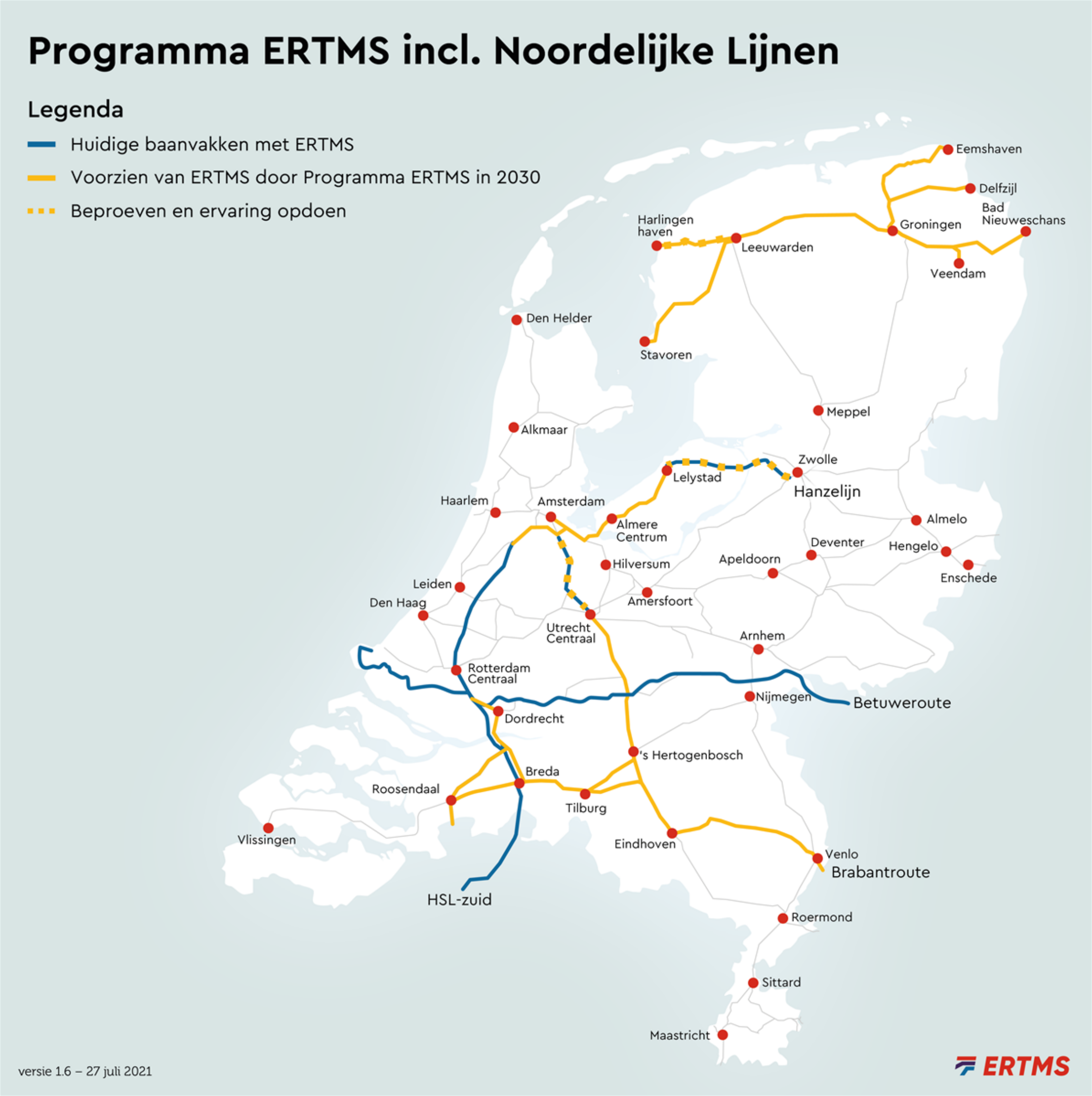


Figure 2: ERTMS programme roll-out in 2030 (ERTMS, 2021)

1.2. Problem description

The Dutch railway transport system consists of components that can be considered as systems in itself, those system components operate together and independently for a shared purpose. This is called a 'system-of-systems' (Hall-May & Kelly, 2005). Besides being a system-of-systems, the railway transport system is also a sociotechnical system. The system cannot be segregated into just a social (people, processes and culture) and technical aspect (technologies, infrastructure and tools), because those are interwoven and not separate components (Kleiner, 2006).

The migration towards ERTMS will cause major changes for the railway transport system, with changes in the social and technical aspect. Al lot will change, in particular for the train drivers and dispatchers. The operational processes and procedures for them will change, for example, the movement authority information is moved from outside the cab (with trackside light signalling) to inside the cab (with a driver-machine-interface). ERTMS will change the interactions and interconnectedness between technology, processes and people. This will also remove, add and change risks in the railway transport system and therefor change the reliability of the transport system.

The ERTMS Programme Management has the obligation toward the ministry of infrastructure and water management to demonstrate that the reliability of the whole transport system stays the same or becomes better after migration to ERTMS (ERTMS Programme Management, 2019c). This demonstration is not yet fully done. To get more support for the commissioning of ERTMS from the various affected companies, the demonstration of the system reliability is also important.

The migration toward ERTMS has many improvements compared to the legacy Dutch ATP systems, but there is no proof that it will be more reliable. Because ERTMS is a socio-technical system, system reliability is also influenced by human action. Examples of human factor issues are the allocation of attention, driving styles, mental workload, route knowledge and trust in automation (Young et al., 2006; Buksh et al., 2013). The human factors, like actions executed by the train driver must be included when the reliability of the railway system is demonstrated (Smith et al., 2012). Rosberg et al. (2021) found 28 publications about the influence from ERTMS on the drivability for train drivers. Research is already done about what the impact is from ERTMS on the train drivers and how this will influence the reliability. The social side of the migration to ERTMS is researched with different methods and different conclusions have been made (Rosberg et al., 2021). A problem that is not yet fully addressed is the reliability and the risks that are influenced by the behaviour and interaction of multiple components in the integrated railway transport system ERTMS. Examples of components are: the train driver, the driver-machine-interface, the train, the rail infrastructure and the train dispatcher.

Identification of the possible risks is necessary to demonstrate the reliability of the transport system. The identification of risks in a system-of-systems may require other techniques than to identify risks form a single system, such as a train engine. Simply combining the risks of different system components will not automatically lead to a complete set of risks for the whole system, new risks occur in the interaction between the different system components (Leveson, 2012). Multiple risk analysis techniques are sufficient for identifying risks for a system component, but the same risk analysis techniques are not necessarily sufficient to identify the risks in a system-of-systems (Dabekaussen, 2017).

More than 100 risk analyses techniques are suggested in the literature. All those different techniques have the same principles (identify causes, consequences, safeguards and recommendations), but they differ in how these principles are approached. The context of the different risk analyses differs mainly in 1. Analysis of a single technical system or 2. Analysis of complex systems (like systems-of-systems or socio-technical systems). Traditional/sequential methods, tools or models for risk analyses (like HAZOP, Fault-Tree analysis and FMECA) are analyses in context 1 and are not sufficient for the analysis of complex systems (Meyer & Reniers, 2016). Qureshi (2007) adds that the traditional models are important to understand how accidents arise, but they are unable to capture the dynamics and complexities of modern socio-technical systems. De Bruijn et al. (2018) also recognized that the commonly used risk analysis technique Fault-Tree analysis is ineffective for the modelling of interactions between the different system components of ERTMS.

The railway transport system is both a socio-technical system and a system-of-systems. It is a requirement to demonstrate that the reliability stays the same or improves by introducing ERTMS. ERTMS will remove, add and change risks in the system, but the overarching problem is that identifying those risks with traditional risk analysis is insufficient.

1.3. Scope

To demonstrate the reliability of the transport system, risks should not only be identified by traditional risk analysis, but also by more modern risk analysis. Because no individual analysis model is able to capture all the complexities in a socio-technical system (Underwood & Waterson; 2014). An example of a promising modern hazard analysis is Systems Theoretic Process Analysis (STPA).

STPA is a hazard analysis technique that is based on Systems-Theoretic Accident Model and Processes (STAMP). STAMP is developed by N.G. Leveson and is an accident modelling framework founded on basic systems theory concepts, rather than reliability theory. It sees safety more as a control problem rather than a failure problem. The framework conceptualises socio-technical systems and sees accidents as something involved in complex dynamic processes with multi-layered control loops and structures. So not only as chains of directly related events, like traditional accident causalities models do (Leveson, 2012). The STAMP framework provides the foundation for the hazard analysis STPA. STPA is a useful hazard analysis to analyse complex systems which can have accidents that result from component failures, design flaws or unsafe interactions (Leveson, 2012), so it can be used for the complex systems in ERTMS which has many interactions. The reliability risks of ERTMS are then caused by interactions of components with unsafe control actions due to inadequate control loops. STPA can find those inadequate control loops.

Compared to other (traditional) hazard analysis, STPA is a more applicable analysis for the railway system, because ERTMS is a complex system (with many actors) where other hazard analysis approaches are less suitable due to the different feedback/circulating loops in ERTMS. It is also a proactive analysis to identify unknown unknowns in the development process of ERTMS, before it is implemented on more tracks in the Netherlands. STPA includes in its analysis also the used software and human interference, which are both present in ERTMS. A benefit of using STPA is that the definition for accident goes beyond human death or injury, it can also include more minor incident, like a train that is a few minutes delayed. Lastly, it also documents the difficult to find system functionalities in the complex systems. Compared to other traditional analyses (e.g. FTA, FMECA, HAZOP), STPA found more causal scenarios and requires less resources like time and money (Leveson & Thomas, 2018). A disadvantage of STPA is that the method executer should be more open-minded than with traditional methods, because more causal scenarios are identified and must be analysed (Bensaci et al. 2018).

STPA models the complex interactions that occur in socio-technical systems, but without making complex analysis. It therefore is a promising way to find unidentified hazards due to ERTMS introduction. STPA is already applied to parts of the railway transport system (Dong, 2012; Li et al., 2021; Ouyang et al., 2010; Wang, 2018), STPA is also applied to the Dutch railway transport system (appendix I), but not yet to demonstrate the reliability of the railway transport system with ERTMS. The focus in this report will be on the use of STPA, to research the risks in the interactions of the transport system with ERTMS.

The problem will be further scoped by only looking at the operational side of system interaction risks, those are more dynamic and less predictable than the technical risks. In the operational side of the transport system, the train driver and dispatcher are interacting with ETCS and play a crucial role. The focus lays at passenger trains, so freight trains are out of scope. This scoping is made because the user processes differ between these two and the ERTMS Programme Management can more easily reach drivers of passenger trains. Applying STPA is done by choosing one specific user process.

Because the Dutch ministry of infrastructure and water management obligated to demonstrate the reliability, this research focusses on the Dutch railway transport system. This research is also done in cooperation with the ERTMS Programme Management, this organisation is directing and making the frameworks for the realization of ERTMS in the Netherlands. Knowledge about implementation is shared to improve this research and to provide for a better evaluation of STPA.

The roll-out of ERTMS is done with ETCS level 2, this level will be the only considered level of ETCS. Dual signalling is also out of scope, dual signalling is implemented on some railway lines in the Netherlands, these tracks have both ETCS and ATB-EG/NS'54 signalling. With dual signalling other risks occur, for example a wrong interpretation due to the integration of two systems. These dual signalling risks are already identified in a report by ERTMS pilot Amsterdam-Utrecht (2015). ATB-NG will be out of scope, so ERTMS is not compared with ATB-NG and the transitions between those systems are left out.

The focus of this research will be on the application of STPA for identifying risks in the interactions of the Dutch railway transport system. With a further focus on the operational aspect, where train drivers, dispatchers and ETCS interact with each other in ERTMS level 2.

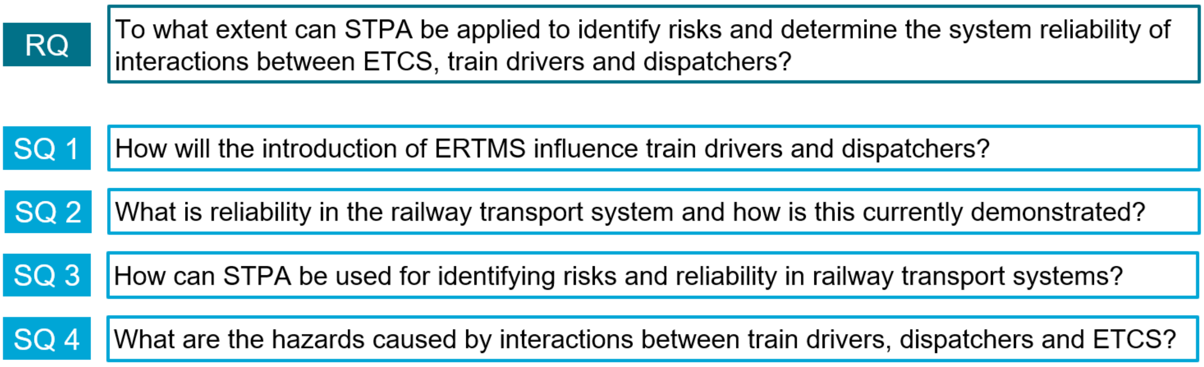
1.4. Objectives

This research has two clear objectives. The research is meant to provide a deeper insight into the application of STPA for identifying risks due to implementation of ERTMS in the current railway system (a brownfield). The first and main objective is therefor to demonstrate if and how STPA can be used by the ERTMS Programme Management. This means that a demonstration will show how relevant or impractical the analysis is. To see what kind of expertise is needed to apply the promising technique STPA for an effective approach of risk assessment.

The second objective is to determine the risks due to interactions between ETCS, train drivers and dispatchers. With those risks, the reliability on railway-system level can be more substantiated and the applied risk assessment will be more adequate.

1.5. Research questions

The research question (RQ) flows out of the problem description and objective. And a few sub-questions (SQ) are formulated to contribute to answering the research question.



RQ	To what extent can STPA be applied to identify risks and determine the system reliability of interactions between ETCS, train drivers and dispatchers?
SQ 1	How will the introduction of ERTMS influence train drivers and dispatchers?
SQ 2	What is reliability in the railway transport system and how is this currently demonstrated?
SQ 3	How can STPA be used for identifying risks and reliability in railway transport systems?
SQ 4	What are the hazards caused by interactions between train drivers, dispatchers and ETCS?

Figure 3: Research questions

1.6. Methodology

To answer the research questions a desk research, STPA and in-depth interviews are executed. The methodology to answer the questions in the different chapters is illustrated in Figure 4, where the arrows present the streams of information. The figure indicates that the desk research functions as a starting point for the method STPA and the in-depth interviews.

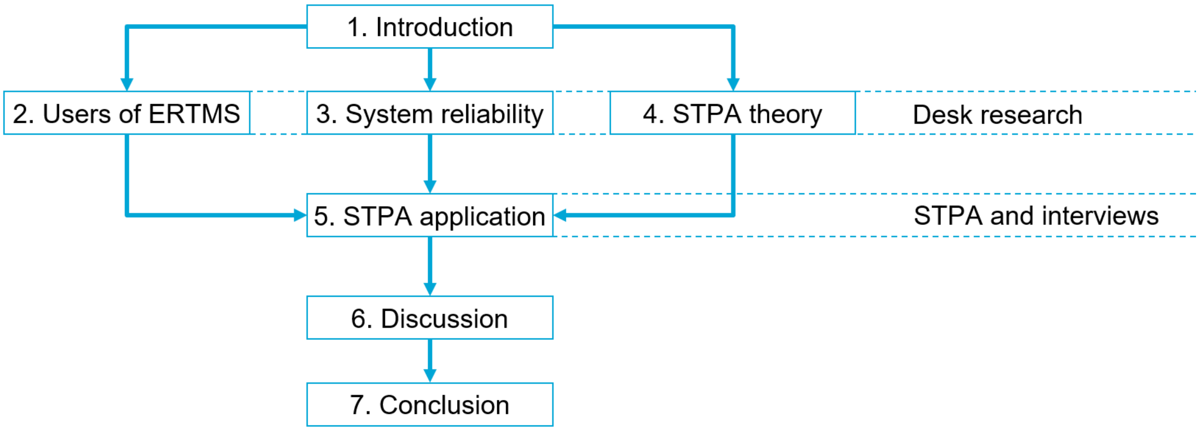


Figure 4: Illustration of methodology used in different chapters

Desk research

The desk research answers the first three sub-questions in the first three chapters after this introduction. The information is gathered by literature review and reports made available by the ERTMS Programme Management.

The literature review was divided into three separate reviews, namely: a review for the changed user processes with ERTMS, reliability of railway transport systems and searches about the usage of STPA. The three reviews were performed in the same manner. First a database search was conducted in the databases of ScienceDirect and Google Scholar for a broad scope. A combination of different search words are entered, for example: ERTMS, ETCS, reliability/reliable, risks, driver, dispatcher, human factors, STPA and STAMP. Key words operators (AND/OR) are applied to select relevant articles, this is further narrowed down by taking the number of citations into account.

More relevant literature was gathered by using a 'snowballing' process (Wohlin, 2014). With this process a key document is picked out of the already found literature and the bibliography of this document is consulted for finding more relevant literature. The search was limited to publications written in English or Dutch. The literature selection took place on different levels, first a rough selection was made by reviewing the title to decide if the literature was relevant for this study. The next level of selection was reviewing the abstracts and again the relevance of the literature was checked, the last level was reading through all the relevant literature.

Besides the literature review, reports from the ERTMS Programme Management were made available to provided better insight in the current reliability assessment, railway standards and insight in the change in Dutch user processes for the train drivers and dispatchers.

STPA

The method STPA is used to provide an answer for sub-question 4. STPA is applied on a case study and with the help of system experts the method is applied. How the STPA method works is described in chapter 4 and how it is executed is described in chapter 5.

In-depth interviews

The in-depth interviews are a qualitative research technique, those interviews are conducted with experts who have experience in applying STPA in the Dutch railway transport system. Those experts are selected by purposive sampling. The in-depth interviews are used to complement the desk research. Further explanation about the followed strategy and the method used for the interviews is described in chapter 5.

1.7. Report structure

The body of the report is structured with chapters that each answer a sub-question. With the different chapters, the main research question can be answered: 'To what extent can **STPA (chapter 4)** be applied to **identify risks (chapter 5)** and determine the **system reliability (chapter 3)** of interactions between **ETCS, train drivers and dispatchers (chapter 2)**?'.

Chapter 2 provides an overview of the different levels of ERTMS and explains the architecture of ERTMS level 2. The change from the current ATB-EG/NS'54 system to the new ERTMS system and the specific changes for train drivers and dispatchers are described to answer the first sub-question.

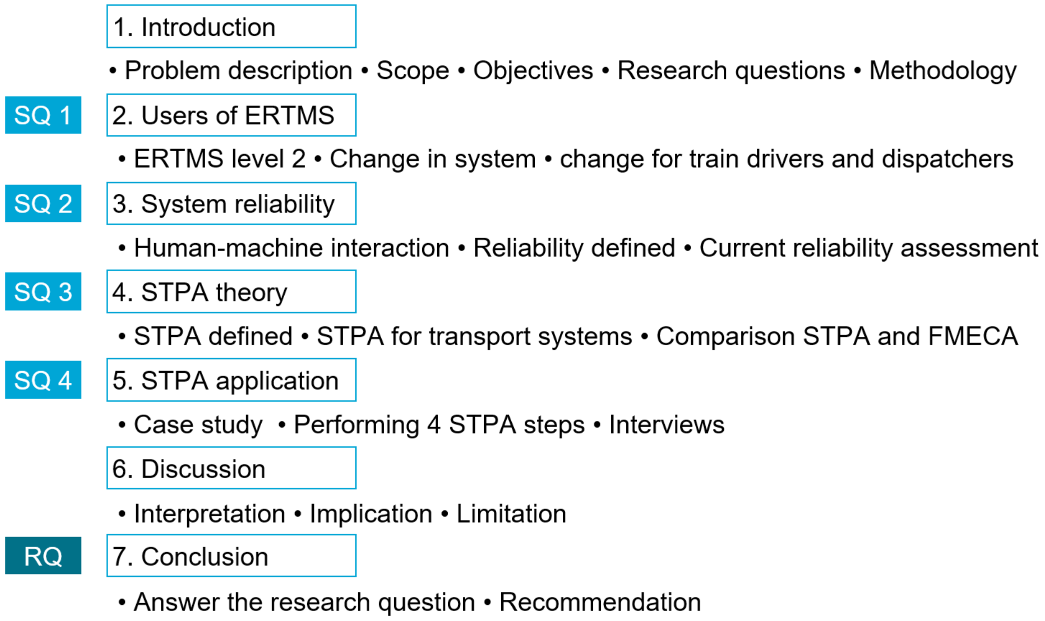
Chapter 3 focuses on the system reliability of the railway transport system, how this is defined and how currently the reliability is assessed for ERTMS, this chapter starts with a small explanation of the human-machine interactions that influence the reliability.

STPA is further introduced in chapter 4, a literature review presents the set up for a STPA and the literature review presents how STPA can be used for transport systems. The theoretical benefits of STPA are shown and compared with FMECA.

With the information gathered in the previous chapters, chapter 5 applies STPA on a chosen user process as case study and interviews are conducted to gather experiences of people who applied STPA in the railway transport system. This chapter answers the last sub-question.

The discussion and conclusion reflect on the research and the result are interpreted, implications and limitations are stated, the research question answered, and recommendations are made for further research.

The report structure with corresponding research questions is illustrated in Figure 5.



1. Introduction

• Problem description • Scope • Objectives • Research questions • Methodology

SQ 1 — 2. Users of ERTMS

• ERTMS level 2 • Change in system • change for train drivers and dispatchers

SQ 2 — 3. System reliability

• Human-machine interaction • Reliability defined • Current reliability assessment

SQ 3 — 4. STPA theory

• STPA defined • STPA for transport systems • Comparison STPA and FMECA

SQ 4 — 5. STPA application

• Case study • Performing 4 STPA steps • Interviews

6. Discussion

• Interpretation • Implication • Limitation

RQ — 7. Conclusion

• Answer the research question • Recommendation

Figure 5: Outline of research with corresponding research questions

2.

European Rail Traffic Management System (ERTMS)

How will the introduction of ERTMS influence drivers and dispatchers?

This question will be answered in this chapter and will be done by starting with a small overview of the different levels in ERTMS. The first section will dive deeper in the architecture of ERTMS level 2, the level that will be implemented in the Netherlands. Following sections will discuss the change from ATB-EG/NS'54 to ERTMS and the changes for train drivers and dispatchers due to the introduction of ERTMS.

2.1. ERTMS architecture

The automatic train protection (ATP) systems are developed to prevent collisions and derailments in case of driver failure. ERTMS is broader than only an automatic train protection system, in ERTMS four layers are found. Namely, the European Operating Rules (EOR), the European Traffic Management Layer (ETML), the European Train Control System (ETCS) and the Global System for Mobiles – Railway (GSM-R).

EOR provides the operational regulations for usage of ERTMS. The ETML is a traffic control information system and is not yet developed. GSM-R is a data and speech communication carrier on specific frequencies, used for information exchange between train and traffic control centres. ETCS is the signalling element of the system and is divided in two components, on board (European vital computer, odometry module, driver machine interface, euroradio module) and trackside components (balises, radio block centre (RBC), line side electronic unit (LEU)) (Smith et al., 2012; UIC, 2015; EC, 2006; van den Top, 2009).

ERTMS levels

ERTMS/ETCS has three levels of technical operation. The first level, level 1, uses track mounted balises (Eurobalises) to transmit discontinuous information from the track to the train and is designed as an add-on for the already available lineside signals and train detectors. The balise transmits information about the movement authority and track description. The ETCS in the train calculates the dynamic speed profile and the braking curves. And train detection (like axle counters or track circuits) is needed to notify the interlocking that a track is free or occupied. Level 1 is functionally comparable with ATB-NG.

Level 2 has the same safety and interoperability benefits of level 1, but it uses GSM-R to transmit information to and from the train, this is bi-directional continuous communication where train position reports are transmitted from the train to a radio block centre and movement authority is given from the radio block centre to the train. In level 2, the train driver sees all the relevant driving information on its driver machine interface (DMI) and lineside signals are unnecessary. The balise is used to transmit location information to the train. Interlocking is still notified by train detection systems and the movement authority is provide by the RBC. The ETCS in the train still calculates the dynamic speed profile and the braking curves.

Level 3 is still in a conceptual phase and the big difference with level 2 is that trackside train detection systems are no longer required, because level 3 includes train integrity monitoring that monitors the completeness of the train. This allows the division of track sections (where only one train can enter) in virtual blocks or moving blocks. Balises have the same function as in level 2. (Smith et al., 2012; Unife, 2021b).

Figure 6 provides a visualisation of the three different levels of ETCS.

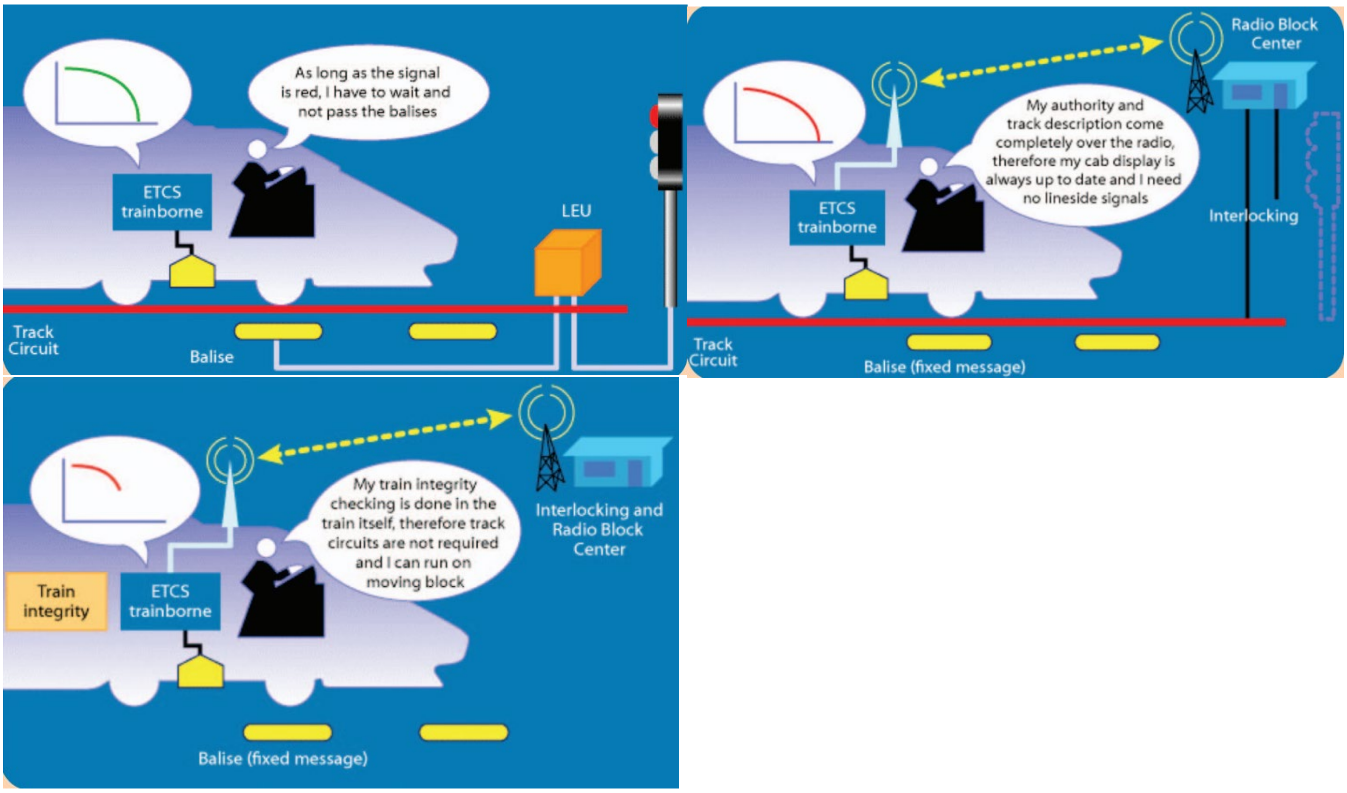

As long as the signal is red, I have to wait and not pass the balises
ETCS trainborne
LEU
Track Circuit
Balise
Radio Block Center
My authority and track description come completely over the radio, therefore my cab display is always up to date and I need no lineside signals
ETCS trainborne
Interlocking
Track Circuit
Balise (fixed message)
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: Level 1: left up. Level 2: Right up. Level 3: left down (Unife, 2021b)

Besides the 3 levels of ERTMS, a level 0 and level NTC is recognized. Level 0 is used on routes without ETCS trackside equipment. There is no automatic train protection and a train driver reads its movement authority from available outside signalling. Those signals are controlled by train detection. Level NTC (national train control) makes use of a specific transmission module (STM) as an extension to the ETCS onboard equipment. This module translates the information of national ATP systems into the ETCS. In this manner a train equipped with ETCS on-board can drive on tracks without ETCS trackside. An overview of the different levels is displayed in Table 1.

Level	Small overview
Level NTC	Train is equipped with ETCS onboard, including a national STM Infrastructure has national signalling and ATP Information from ATP is presented on ERTMS DMI
Level 0	Train is equipped with ETCS onboard, but there is no ETCS trackside No ATP available
Level 1	No lineside signals, but still train detection in tracks Fixed blocks/sections Eurobalises have location and movement authority information
Level 2	No lineside signals, but still train detection in tracks Fixed blocks/sections Communication via GSM-R, Eurobalises are mainly position markers
Level 3	No lineside signals, no train detection in tracks Virtual blocks or moving blocks (possible due to on-board train integrity monitoring) Communication via GSM-R, Eurobalises are mainly position markers

Table 1: ERTMS levels

Level 2 architecture

As previous defined, the architecture of ETCS has 2 sub-systems, ETCS trackside and ETCS on-board. Those sub-systems, the connections and interactions between sub-system components are visualized in Figure 7. The visualization gives an overview and is based on the visualizations made by the ERTMS Programme Management (2019d), Flammini et al. (2014), van Es (2017) and ERA (2016a). The Dark blue blocks/components in Figure 7 are components that are not official ETCS elements but they are elements that interact with ETCS. The figure is not complete, certain details have been omitted.

The connecting lines between the different components have different interface specifications and those interfaces are defined by the European Union Agency for Railways (ERA, 2016a). Interface specifications are for some interfaces just functional (FIS) and some are besides functional, also form and fit specified (FFFIS). FIS gives a general definition of what information in which format should be transmitted over the interface. FFFIS includes also the definition of the communication protocols and the physical layer.

Besides ETCS trackside and on-board, other trackside systems are present. The interlocking (IXL) is one of them, but no interoperability requirements are established. The train dispatcher communicates with the interlocking and the radio block centre via a traffic control system (TCS). The interactions between the driver and DMI and between the train and the train interface unit (TIU) are specified in an interface specification. The GSM-R module for railways provides bidirectional data communication between RBC and on-board units via GSM-R. GSM-R voice enables the train driver to speak with the train dispatcher who is responsible for the area where the driver is currently driving. It also ensures that emergency calls are sent to the correct train(s). With GSM-R data, information is exchanged between trackside and train.

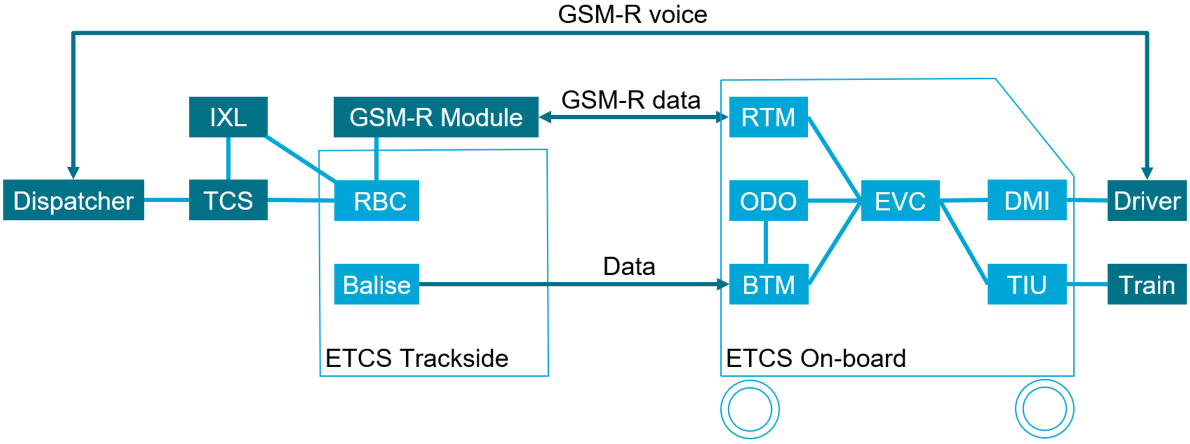


Figure 7: ERTMS/ETCS level 2 architecture model

The main tasks of the ETCS trackside are: calculating the movement authority, the monitoring of train movement and data transmission. Balises and the radio block centre (RBC) are the main components. A small description is given in Table 2.

Name	Component	Description
RBC	Radio block centre	Computer based communication system for safety and it controls train separation. It interacts with the interlocking information from the IXL and gives movement authority.
Balise	Eurobalise	Point position marker that transmits data (telegrams), standalone device, comes in pairs for reliability and to tell the direction the train is moving

Table 2: Trackside components

The main tasks of the ETCS on-board are: communication with the trackside and providing safe movement. Table 3 describes the different components of the ETCS onboard.

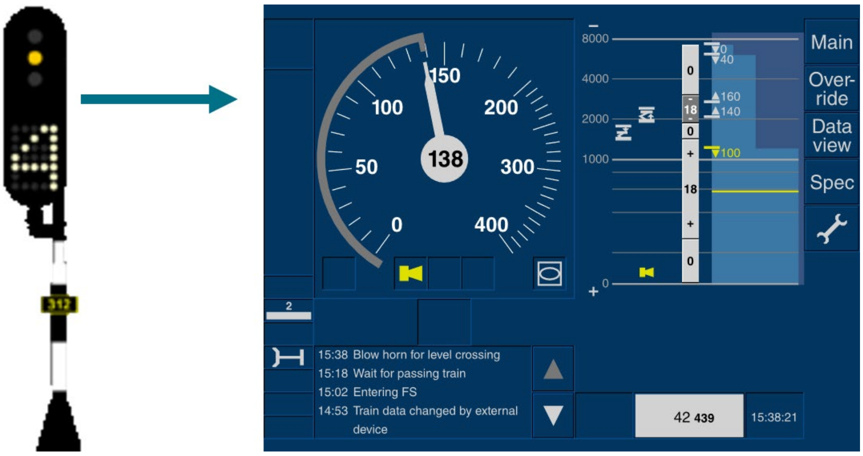
Name	Component	Description
BTM	Balise transmission module	Antenna that reads the telegram send by the balise.
DMI	Driver machine interface	European standard touchscreen that provides the info for driving (actual speed, maximum speed, what needs to change).
EVC	European vital computer	Core of the system and is connected to the other systems, for example the train interface unit that controls the brakes and traction. The primary function is to compute the dynamic speed profiles for the current movement authority.
ODO	Odometer	System to determine the speed and travelled time, to calculate the position of the train since the last balise.
RTM	Radio transmission module	Provides bidirectional data interface with the trackside on GSM-R network and via EuroRadio protocols.
TIU	Train interface unit	Bidirectional interface between the EVC and other train devices.

Table 3: On-board components

2.2. From current automatic train protection toward the ERTMS

The current mostly used train protection system in the Netherlands consist of the automatic train protection system ATB-EG and the block signalling system NS’54. ATB-EG supervises if the allowed speed steps are not exceeded, the speed steps that are supervised are 40, 60, 80, 130 and 140 km/h. Those speeds are communicated via coded track circuits in the rails to the train cab and a movement authority is given via signal aspects shown by lineside color light signals. ATB-EG does not supervise speeds under the 40 km/h, therefore an upgrade of ATB-EG was developed (ATB Vv) and equipped in many places of the railway network (ERTMS Programme Management, 2019a).

With ERTMS level 2, the automatic train protection system is made more modern and the signalling is transferred to on board on a touchscreen in the train cabin, so light signalling along the track can be removed. The communication between train and track becomes digital with GSM-R. ETCS on-board informs how far the train is allowed to drive and which speeds restriction are present and will occur in the given route. ETCS on-board also calculates and supervises a dynamic speed profile with braking curves. The braking curves are computed for all allowed speeds with the train specific characteristics and applied to the current speed. With ERTMS, any speed can accurately be supervised. An illustration of the in-cab driver machine interface is seen in Figure 8 on the right side of the arrow.



15:38 Blow horn for level crossing
15:18 Wait for passing train
15:02 Entering FS
14:53 Train data changed by external device

Figure 8: From light signalling along the track (left) to in-cab signalling with a driver machine interface (right) (de Vries, 2016).

ERTMS might also result in less malfunctions in signalling and the train detection systems. Light signals along the track are removed, so these signals cannot fail anymore. The train detection systems are still required in ERTMS level 2, to ensure the interlocking that a track is clear. But under ERTMS, the train detection system can switch from track circuits to axle counters. Under ATB-EG the track circuits cannot be replaced by axle counters, because coded track circuits are needed to communicate the speed steps. Axle counters are cheaper, installed flexible, require less maintenance, is more reliable and less sensitive for weather conditions (Theeg and Vlasenko, 2009). With axle counters, the so-called rust driving is something of the past, because track circuits need to be driven by at least 20 axles every 24 hours to be reliable, this is not the case for axle counters.

The migration from ATB-EG and ATB-NG to ERTMS will be done by replacing it on a line-by-line basis. So there is not a big-bang where many lines are changed simultaneously (ERTMS Programme Management, 2019a). The strategy of the roll-out resembles a so-called inkblot, a few main lines in different regions are chosen and new ERTMS sections are connected to those lines. Another strategy is called the patchwork strategy, where lines are replaced because they are on their technical end-of-life. This strategy is partly applied by adding the northern lines, but also there an inkblot strategy is applied. Van der Weide (2017) concluded that an inkblot strategy is the most appropriate roll-out strategy if operational and human factors are considered.

As already briefly mentioned, ERTMS aims to provide more cross border interoperability in Europe, improve the national and international train traffic safety, better speed supervision, increase in capacity, more operational punctuality and flexibility, less trackside equipment, enabling more European competition between railway signalling component manufactures, reduce maintenance costs and enable more chances to develop rail related technologies.

A deeper dive in the advantages of capacity increase and more safety due to less signals passed at danger will be further discussed in the following sections. The migration toward ERTMS will also influence the train drivers and dispatchers in particular. Section 2.3 goes further in depth in what changes for the drivers and dispatchers (ERTMS Programme Management, 2019a).

Less signals passed at danger

With NS'54 block signalling, color signals are placed alongside the tracks, a signal can order 3 basic aspects: green (clear and proceed), yellow (caution, reduce speed to 40 km/h, expect stop), red (stop, danger, don’t go beyond this point). Optional speed indicators next to the color signals can indicate the target speed limit. In this conventional block signalling system, the infrastructure is divided in blocks with train detection systems (track circuits or axle counters) and each block is guarded with a signal. The length of a block, also the distance between two signals, is based on the train with the poorest braking performance that could achieve a certain speed reduction in the available distance (van den Top, 2007). The meaning of a yellow signal is sometimes ambiguous and the infrastructure layout is sometimes placed in a manner that it is not obvious for the driver to predict the distance to the next red signal, this may lead to a signal passed at danger (SPAD) (Onderzoeksraad voor de Veiligheid, 2005). A SPAD is highly undesirable, because the track section behind the signal may be in use for other purposes or a switch may be destroyed.

With ERTMS, the lineside signalling is replaced by cab signalling and a modern ATP, which is aware of the movement authority and the speed restrictions until the End of Authority. Equipment onboard of the train calculates and supervises a detailed dynamic speed profile. If a train driver exceeds the allowed speed, the ETCS onboard warns and intervenes with a brake intervention if needed. Signal passed at danger are no longer possible under full supervision (van den Top, 2009).

Capacity increase

Capacity utilization can improve in multiple ways after applying ERTMS, this is mainly caused by the in-cab signalling with speed supervision for all speeds and continuous braking curve supervision, the capacity increase depends on how conservative the braking curves are computed. A combination of different functionalities increases the capacity utilization further. Examples of those functionalities are given by Goverde (2012):

- Train specific braking curves that provide effective distance-to-go braking, causing gain in follow-up time.
- Shorter blocks, also available due to train specific braking curves (rather than at the beginning of a block) and the placement of blocks is no longer restricted to where electronical signals can be placed.
- More effective overtaking, due to shorter minimum headway time.
- Higher section speeds possible to supervise within a block.
- Supervising all the speeds, especially the speeds between 80 km/h and 130 km/h that are not supervised by ATB-EG.
- More flexibility in positioning the blocks, even just before a switch is possible due to cab signalling.

The main changes from ATB-EG/NS'54 to ERTMS are the in-cab signalling with braking curve supervision and speed supervision of all speeds. This will benefit among others: more capacity and more safety on the railway network.

2.3. ERTMS influencing the train drivers and dispatchers

The train drivers and dispatchers notice the most from the transition toward ERTMS and they frequently and directly interact with ERTMS. The train drivers will interact with the ERTMS functionalities in the rolling stock for a large part of their work. The dispatchers will mainly get more and changed functionalities due to ERTMS. This section will discuss the changes for train drivers and dispatchers due to the introduction of ERTMS. First the train drivers are discussed.

2.3.1. Train drivers

The train driver controls the train equipment to carry out train rides, shunting work and recover minor malfunctions. The driver's activities change due to ERTMS introduction, because the infrastructure and the equipment changes. Drivers need different skills than driving under ATB-EG, the driver becomes more an operator of a computer system. ERTMS is perceived as more difficult for some drivers, due to the more complex troubleshooting, the English terminology and the processing of screen information (ERTMS pilot Amsterdam-Utrecht, 2015).

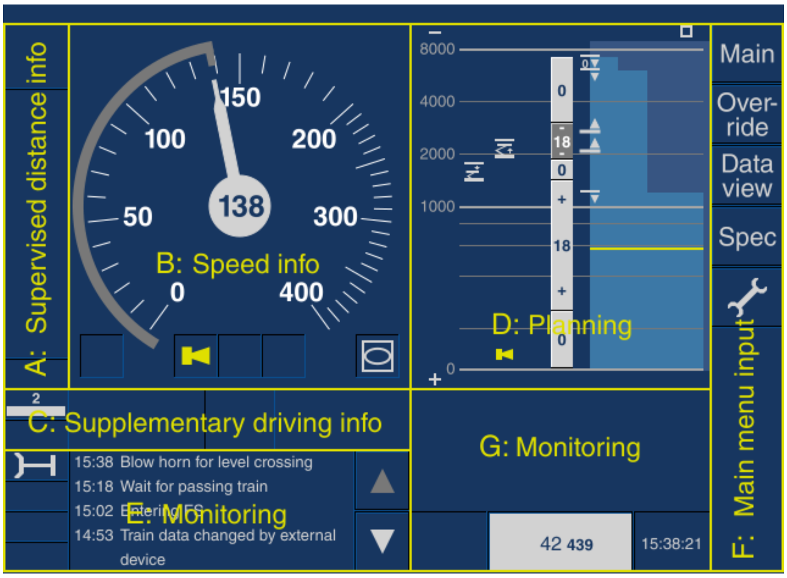
The biggest change for the driver is the shift of movement authority information, this was first outside with color light signals and now in-cab on the driver machine interface. The visual focus of the driver will therefor shift from outside to inside and the driver's attention on events outside the cabin reduces (Naghiyev et al., 2014). Besides the shift of focus, the workload, the procedures and the communication styles change. The current drivers need training to deal with those changes (Zeilstra et al., 2016). The job requirement and consequently the selection procedures will also change due to ERTMS. The competences change, because the driver becomes more reactive on what the DMI displays and proactive with the increase of available information. Drivers are demanded to have more technical insight, computer skills and the ability to change faster (Brandenburger et al., 2017). The rest of the section elaborates about the changes in human-machine interactions and the change in workload.

Human-machine interactions

The driver is affected by ERTMS in human-machine relationships, namely due to the driver's desk with its driver machine interface (DMI). The drivers perform their tasks in the driver's cab which contains the driver's desk. Drivers drive different train types with different driver's desk layouts (ERTMS Programme Management, 2019d). During a train ride, the driver can encounter different technical systems in the infrastructure, for example the change in ATP systems and different energy supplies. The driver should therefor switch from systems used on its driver's desk. This transition can be extra demanding if the infrastructural situation is complicated due to slopes or curves in the track (van der Weide, 2017).

The interaction with the signalling will change drastically as previous said. The introduction of in-cab information on the DMI causes head down driving. The driver that normally drives with route knowledge must now concentrate on the displayed messages, which alters the focus of the driver (Porter, 2011). Van der Weide (2017) researched how much train drivers look outside and concluded that they look 75,3% of the time outside if they drive under ATB-EG and 39,3% under ERTMS. A risk of looking less outside is missing important information like damaged overhead contact lines, unsafe objects on and near the tracks or ETCS marker board (Rosberg et al., 2021). An advantage for the driver is that he can read the displayed information at any moment and not only when the train passes a light signal (Van den Top, 2009).

The driver machine interface is the operating interface of ERTMS in the train. The DMI shows more information than the ATB-EG equipment does, for example the movement authority, a planning of up to 32 km of the track ahead and exact allowed speeds based on braking curves. Information must also be entered via the DMI, which was not necessary for ATB-EG equipment (van der Weide, 2017). The planning displayed on the DMI can be compared with the existing driver advisory system TimTim from the NS, this system is appreciated by drivers (Spoor Pro, 2022). Figure 9 displays a DMI with a small explanation of the different sections.



15:38 Blow horn for level crossing
15:18 Wait for passing train
15:02 Entering FS
14:53 Train data changed by external device

Figure 9: Example of a Driver Machine Interface with the different sections highlighted in yellow (de Vries, 2016).

There are also issues identified for the DMI, the screen visibility can be lacking due to sun glare and a too dark screen. The converse is also reported, a too bright screen during the night. The DMI icons have also caused issues, because drivers found them to small or similar (Smith et al., 2012). Human error can be the result of such issues.

Workload

A literature review from Rosberg et al. (2021) demonstrated that the mental workload of train drivers due to transitioning to ERTMS is in some situations reducing and, in some situations, increasing. The increase is caused by complex speed profiles and transitions between conventional signalling systems and ERTMS. The decrease is caused by the clear brake announcements of the DMI and the increase of available driving information. Different studies show that staying alert may be more challenging due to the decrease of external stimuli (Rosberg et al., 2021). Risks are introduced if a long period of decreased external stimuli occurs, drivers could become less aware of situations where intervention is needed (Hamilton and Colford, 2003).

Before the train driver starts driving, a Start of Mission (SoM) is performed. The preparation before driving consumes a bit more time in ERTMS, because train data (category, length, brake percentage, maximum speed) must be entered in the DMI and ATB-EG has no comparable process. The manual entry of data is danger sensitive, when for example a wrong braking percentage is filled in, a wrong braking curve will be calculated. The likelihood of error can be reduced by automatically uploading the safety critical data and the driver should only check and accept the uploaded data (Porter, 2011). This is implemented in the scope document for ERTMS implementation in the Netherlands (scope-id: S-076) (ERTMS Programme Management, 2019e).

During normal driving operation, ETCS supports processing of information much more than ATB-EG does. ATB-EG does not continuously supervise the driver to drive gradually to a certain point with a required speed. ETCS does this and supports by first giving warnings on the DMI if a required speed is trespassed and brakes if the speed is still not reached, those driving errors are always corrected, because provided information is more precise than in ATB-EG. This makes the workload lower while driving in full supervision mode and compared to ATB-EG (van der Weide, 2017). The decreased workload is also concluded in a workshop executed for train drivers by van der Weide et al. (2017). The drivers who had experience with ERTMS on the lines Betuweroute and HSL-Zuid mentioned that there is a lower workload and less external stimuli, this made staying alert harder.

Increase in mental workload is caused by technical failures. With NS'54 block signalling the light signals can fail and in ERTMS other technical failures can occur, for example a loss of contact with the radio block centre, the ETCS onboard equipment or the balises. Correcting the malfunctions in ERTMS will be done by procedures, called user processes. These user processes are not executed often, so train drivers have limited experience with them. More information about user processes is given in chapter 5. When the processes from ERTMS are compared with ATB-EG, then it can be concluded that the user processes of ERTMS requires more actions. The procedures are increased and different due to the applicable regulations (van der Weide, 2017). And under ATB-EG it is often already clear to users whether a failure is caused by failure in the train or in the infrastructure, but with ERTMS it is in most cases much more difficult to determine where the cause of the failure must be found.

Change	Explanation
Perception of signals	Visual focus shift from outside (line signalling) to in-cab (driver machine interface). A reduction of time looking outside from 75,3% to 39,3%.
Communication	Communication via GSM-R equipment standardized by ERTMS.
Available information	Increase in information available for the train driver (e.g. a braking curve and a planning of the track ahead).
Preparation	The DMI requires to fill in more information (the train protection mode and train data).
Reacting to signal aspects	The DMI shows the braking curve, so the driver is guided with when and how much he should brake. More detailed information can now be read on the DMI.
Procedures after failure	Extra and different actions required

Table 4: Main changes for the train drivers that transition toward ERTMS

2.3.2. Train dispatchers

The train dispatcher facilitates and directs safe movement of trains over an assigned route, for which they can adjust routes. The tasks of the dispatcher are influenced by the introduction of ERTMS, mainly due to new and adapted procedures and functionalities. The impact on the tasks of the dispatcher is significant in normal operation and in case of technical failures in the transport system.

Under ATB-EG, the train dispatcher gives specific written orders for safety critical messages, the procedures for those written orders will change and some will be added under ERTMS. The written orders are called European instructions in ERTMS. European instructions are instructions that describe how certain procedures are carried out (EU, 2015). An example of a new European instruction is getting permission to continue driving after an automatic emergency braking, as described in user process 37 (ProRail, 2022c).

The malfunctions and its behaviour are also different in ERTMS, the dispatcher therefore needs different knowledge and skills when operating in ERTMS areas and when communicating with the train driver (ERTMS Programme Management, 2019d). The workload of the dispatcher increases slightly under ERTMS, this is concluded after execution of a pilot in the Netherlands. This is mainly caused by the increase in actions that are required by fault handling. An example of a malfunction is the increase of communication losses between train and RBC due to GSM-R failure, this leads to stranded trains (ERTMS pilot Amsterdam-Utrecht, 2015).

More information about the changes for dispatchers in the Netherlands was not found in scientific literature or public available documents. The rest of the information found in this section was gathered by reviewing intern documents from ProRail and the ERTMS Programme Management.

Implementation of ERTMS results in the change that there is no difference anymore between operable infrastructure elements on station areas and on the ‘open track’ (in between station areas), both will be operable by the train dispatcher. In the conventional system, many open tracks have automatic signals that operate via automatic block systems and thus, no routes are set by the dispatcher. The dispatcher is under ERTMS responsible for giving movement authority to the trains on all the operated infrastructure. This results in an increase of information.

Under ERTMS, much more information is available about the current condition of the train than under the current system. Some information is directly available on the screen of the dispatcher, such as the status of the connection to the radio block centre and the kind of movement authority the train is given. Other information can be made available if needed, information such as the exact position or speed of the train. So the train dispatcher has a better view on what a train driver experiences. When a deviation on the planned timetable occurs, then the dispatcher has a better situational awareness and the dispatcher has more insight in possible causes of the deviation and the location of the train.

Besides the extra available information, the dispatcher can also intervene more and in real-time. Real time intervention is necessary if a defect in the track or an unsafe situation around the track is reported. In the conventional system, the dispatcher must warn each train individually with an instruction, usually a speed restriction. With ERTMS, the dispatcher can enter a temporary speed restriction digitally and this is directly processed in the maximum permitted speed of all the trains on and to a specific track, this will lead to a changed dynamic speed profile for the applicable trains. Besides the speed restriction, the dispatcher can also withdraw movement authorities of a specific train or more trains on a specific track or area, this is necessary if a dangerous situation occurs. Under ATB-EG it is not possible to set such restrictions automatically for every train that passes a certain location for a certain moment. The change is also beneficial for train drivers, because they can continue look at the DMI and there is less risk of missing speed restriction signs.

ERTMS gives also indirectly new functionalities: clearing residual routes and resetting axle counters. In events of unplanned turning movement or malfunctions, parts of a route sometimes remain unintentionally set, causing the inability to drive on that track by other trains. Under ATB-EG, an asset manager must remove the residual route manually. When axle counters are used, removing residual route can be done digitally by the dispatcher. With the possibility to reset axle counters, the dispatcher can digitally reset the axle counter in case of errors of the axle counter. Axle counters are not a part of ERTMS, but ERTMS makes it possible to replace tracks circuits by axle counters, so the added functionality is indirect.

Change	Explanation
More operable infrastructure	Added operability on open tracks (previously operate via automatic block systems).
More available information	Increase in information about the trains, what gives more situational awareness (location, speed, kind of movement authority, connection with radio block centres).
Other intervention possibilities	Enter temporary speed restrictions or withdraw movement authorities digitally to directly process it for all the relevant trains.
Indirect added functionalities	New functionalities, like clearing residual routes and resetting axle counters.

Table 5: Main changes for the train dispatcher that transition toward ERTMS

3.

Reliability in the railway transport system

ERTMS influences the reliability of the railway transport system, this thesis focuses on how the reliability is changed by the interactions between ETCS, train drivers and dispatchers. Chapter 2 concluded with a summary of the main changes for the train drivers and dispatchers, due to the transition toward ERTMS. Those changes will also influence the reliability of the transport system.

Chapter 3 answers the second sub-question of this thesis. It explains what is meant by system reliability and how the reliability of interactions between ETCS, train drivers and dispatchers is currently demonstrated. By explaining how system reliability is defined, it can be examined how STPA can contribute to demonstrate the system reliability in the next chapter. By explaining how the reliability is currently demonstrated in the ERTMS Programme Management, the current method can be compared to STPA, this comparison is elaborated in chapter 4.

The focus of chapter 3 is first on what system reliability is. The first section gives a system reliability definition that demonstrates the relationship between risks and reliability and what information is relevant to describe the reliability. The second section focuses further on how the system reliability of the railway transport system is influenced by human-machine interactions. In those interactions, human error can occur due to the limitations of human information processing. The last section will elaborate on the currently applied reliability assessment for interactions between ETCS, train drivers and dispatchers by the ERTMS Programme Management.

3.1. System reliability

To demonstrate the railway transport system reliability, the system reliability must first be defined. This section discusses the different ways to define system reliability, a few preconditions to demonstrate the system reliability, the reliability requirement, failure categories and the importance of risk analysis.

System reliability defined

The complex system ERTMS should operate reliable, where the reliability of the system aims to fulfil the function of the system. System reliability focuses on the probability and impact of potential failures of a system function, so the system can operate as intended (Rausand, 2004).

When a system component is only technical, it is delivered with a certain level of reliability (expressed in terms of mean time between failures (MTBF)) and when the component is properly maintained (expressed in mean time to repair (MTTR)), than the required availability of the component can be expected to be achieved. Availability=MTBF/(MTBF+MTTR). The terms MTBF and MTTR are often expressed in hours. However, reliability and availability of a technical system component is something completely different compared to reliability on railway transport system level, because it is a system-of-systems and a socio-technical system.

Vromans (2005) points out in his research on the reliability of railway systems that reliability measures are generally described with Mean Time Between Failures and a percentage of completed processes in a system. Vromans describes that in the case of a railway system, the system is reliable if the trains are run as planned. This means that passenger trains and freight trains are at the right stations at the scheduled time, punctuality is therefore of importance. The difference between arrival times in operation and the scheduled arrival times must be minimized for a reliable railway system.

The European Committee for Electrotechnical Standardization (CENELEC) develops and publishes European standards in the area of electrical engineering. CENELEC developed the standard EN 50126, which elaborates about the specification and demonstration of reliability, availability, maintainability and safety (RAMS) for railway applications (CENELEC, 1999). This standard is made mandatory by the Technical Specifications for Interoperability related to the Control-Command and Signalling (TSI CSS). The TSI CSS is obligatory to follow when ERTMS is implemented, this specification is developed by the European Union Agency for Railways (ERA, 2016b). The standard EN 50126 includes, besides specifications for reliability demonstration, also specifications for availability, maintainability and safety. Those other terms are connected to reliability, but are not discussed in detail in this thesis. EN 50126 defines reliability as following: 'The probability that an item can perform a required function under given conditions for a given time interval' (CENELEC, 1999).

In this thesis, the reliability is formulated in a slightly different manner, to make it more operable and to clearly demonstrate reliability. Namely, 1 minus the probability of failure: R(t)=1-F(t), as illustrated in Figure 10. R(t) stands for the reliability over time and F(t) stands for the cumulative probability of failure over time. The probability of failure and the reliability are opposites (Aven, 2017).

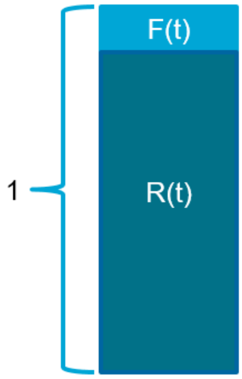


Figure 10: R(t)=1-F(t)

Preconditions to demonstrate system reliability

To determine the probability of failure of a system, an unambiguous description of the concept of failure for the system must be drawn up, the so-called failure definition. The failure definition is linked to the function of the system and can be subdivided in fault categories and rate of occurrence. The fault categories demonstrate the effect of a failure.

A reliable system can be obtained by precautions: prevention of deviations and failures or controlling the consequences of deviations and failures. Prevention of all failures is impossible for a socio-technical system, therefor the control of consequences of a failure is essential.

The EEIG ERTMS Users Group (1998) described two preliminary RAM related outputs that are important for the reliability analysis. Namely, system identification, and failure conditions. The railway system must be identified, this has to be done by describing the system architecture, system interfaces (as is already partly done in section 2.1: ERTMS architecture), the boundary limits and the operational conditions. Examples of operational conditions are location, time of the day, foreseeable deviations, weather conditions and train type. The failure conditions describe the failure of the system and the different fault categories.

Reliability requirement

ETCS has as goal to supervise the movement of trains, to ensure that they are running safe on the railway network (EEIG ERTMS Users Group, 1998). The goal of the railway system is to carry out the entirety of activities for the movement of people and/or goods by rail (ERTMS Programme Management, 2021a). System reliability contributes to this function by minimizing the probability and impact of failure in the system. As already explained, the railway system is reliable if the trains run as planned (Vromans, 2005). Delay of a train can result in a loss of transportation goal by not moving people and/or goods by rail on time.

The ERTMS Programme Management described the requirements for the railway system, one of those is a reliability requirement, which can be read in the following text box.

> ***Reliability requirement:***
> *'The operational impact of disruptions in the transport system, expressed in train delay minutes, should remain the same or decrease as a result of the addition of ERTMS to the transport system, with as reference value the infrastructure and the same equipment and the prevailing operational conditions, as before the addition' (ERTMS Programme Management, 2021b).*

The reliability requirement is set for the overall transport system level, so not for only a sub-system/component level. The requirement talks about the 'train delay minutes' and not about passenger delay minutes. From a risk-based point of view, passenger delay minutes are more relevant, because it also takes consequences of delay in terms of numbers of passengers into account. Passenger delay minutes concerns the loss of travel time for the passenger compared to the planned timetable for station-to-station travel time. But the ERTMS Programme Management does not have direct influence on the number of passengers and the planned timetable, but only on the operational impact. The operational impact is about the cumulative number of minutes of delay of trains that are affected as a result of a disruption (ERTMS Programme Management, 2019c).

The operational impact is composed of three aspects: disruption frequency, functional recovery time, impact on train traffic per disruption. The disruption frequency is about how often a disruption occurs that affects train traffic. Functional recovery time is about the needed time to functionally remove a disruption, so the train traffic runs normally again. The impact on train traffic per disruption is about the number of trains that ultimately experience hindrance, due to the disruption. The recovery time is depending on the location, what time it is and the control and corrections of train driver and dispatcher. A disruption during rush hour in station Utrecht Central has generally more impact on train traffic than a disruption during night-time on a little used track (ERTMS Programme Management, 2019c).

ERTMS Programme Management can influence the operational impact in four manners: 1. Changing some system components and changing the system architecture 2. Adjusting user interactions and user processes 3. Arranging the management of added components and the overall system 4. Add functionalities to better control and correct the railway system (ERTMS Programme Management, 2019c).

Adjusting user interactions and user processes is done by designing the user processes and the user interfaces. The human-machine interactions will change, so the user processes and interfaces must change accordingly. If the processes and interfaces are illogical, then the number of human errors and thus the number of disruptions can increase (ERTMS Programme Management, 2019f). Sallak et al. (2015) concluded that train drivers and dispatchers have the highest impact on the reliability of ERTMS, so the human errors should be considered if reliability is assessed. The railway standard EN 50126 elaborates on which parameters could influence human errors. Examples of how human information processing capabilities can be influenced are: The density, rate and quality of transferred information, human training and human support in decision making (CENELEC, 1999). Because the train driver and dispatcher have the highest impact on system reliability, the focus of this thesis is on the interactions of those users with ETCS.

The reference value in the reliability requirement is relative to the transport system without the ERTMS. The bottom value of reliability is the reliability of the transport railway system before the addition of ERTMS, with the same equipment and prevailing operational conditions, like train kilometers. This is called the GAMAB principle (an abbreviation for the France phrase: Globalement Au Moins Aussi), which stands for the principle that a changed system offers a level of risk that is globally at least as low as the original system (CENELEC, 1999). The ERTMS Programme Management uses the term stand-still principle, but it has the same meaning as the GAMAB principle.

94,4% of the train rides on the main rail network (HRN) in 2021 had no delay or less than 5 minutes delay. And 1,9% of the train rides on the main rail network (HRN) in 2021 had a delay of more than 15 minutes (Prorail, 2022a). These percentages of train punctuality can be misleading, because it does not minimise train delays. It will rather lead to concentrating the delays on one train or cancel a train that already passed the 5 minutes or 15 minutes threshold (van den Top, 2010). The given percentages are not fully representative to use for the reliability of the railway system before ERTMS is implemented, but it can be illustrative for a quick comparison with a reliability percentage after ERTMS is implemented on many tracks.

The reliability requirement appoints that disruptions in the transport system are expressed in train delay minutes. Those disruptions are a variable set that differ between ATB-EG and ERTMS. Some new disruptions are possible to occur, some cannot occur anymore and other disruptions will change. The different possible disruptions must be identified, before a failure category can be attached to the disruption.

Failure categories

Failure categories categorize the effects of a failure. Those categories and their definitions can differ, as is demonstrated in this section. The standard EN 50126, the EEIG ERTMS Users Group and the ERTMS Programme Management have their own definition for their failure categories. The definitions do not contradict and help each other to understand the different failure categories. In this thesis, the definitions from the ERTMS Programme Management are used, because those are the most quantitative and can contribute to quantifying the risk.

EN 50126 defines three failure categories for reliability in the railway transport system. These categories differ in the severity of the failure: significant, major or minor. Table 6 demonstrates the definitions of those categories.

Failure Category	Definition defined in EN 50126
Significant (Immobilising failure)	A failure that: prevents train movement or causes a delay to service greater than a specified time and/or generates a cost greater than a specified level
Major (Service Failure)	A failure that: - must be rectified for the system to achieve its specified performance and - does not cause a delay or cost greater than the minimum threshold specified for a significant failure
Minor	A failure that: - does not prevent a system achieving its specified performance and - does not meet criteria for Significant or Major failures

Table 6: Reliability failure categories defined in EN 50126 (CENELEC, 1999)

The EEIG ERTMS Users Group (1998) defined the different failure categories in a different manner, their categories are specifically described for ERTMS. Namely, an immobilising failure will cause 2 or more trains to switch to on sight mode. A service failure will cause 1 train to switch to on sight mode and/or it causes a nominal performance reduction of one or more trains. A minor failure is described as a failure that results in an unscheduled maintenance. (EEIG ERTMS Users Group, 1998). The ERTMS Programme Management defined the failure categories more applied to the reliability requirement and the definition for the different categories is made more quantitative as described in Table 7. The threshold values for the different categories are 3 train delay minutes and 10 train delay minutes. The 3 minutes value is chosen because delays that are shorter than 3 minutes are not included in loss of punctuality reports. The 10 minutes value is chosen because delays of more than 10 minutes will likely influence other trains, this number is based on expert judgement.

Failure Category	Definition defined by the ERTMS Programme Management
Significant	A failure causing a service delay lasting longer than 10 minutes
Major	A failure causing a service delay lasting between 3 and 10 minutes
Minor	A failure causing a service delay lasting less than 3 minutes

Table 7: Reliability failure categories for trains, defined by the ERTMS Programme Management (ERTMS Programme Management, 2019g).

Not all failures will cause service/train delay minutes, those disruptions are still not desirable, because it can lead to more workload for the train driver or dispatcher. The disruptions that do not cause delay are categorized as a minor failure.

Risk analysis

The obligatory RAMS standard EN 50126 from CENELEC addresses via general guidelines, techniques that evaluate system dependability for critical control systems, like ETCS (CENELEC, 1999). The standard suggests qualitative and quantitative methods for risk analysis. Qualitative methods mainly provide insight into how a system will behave and in what ways it will fail, while quantitative methods provide insight into how likely a particular failure will occur. EN 50126 suggest mainly traditional risk analysis methods ('fault tree analysis', 'failure mode effects criticality analysis' and 'hazard and operability analysis'), but those techniques are inadequate for assessing the complex interactions in railway transport system, as explained in the problem description of this thesis. The proposed techniques are only suggestions and therefore not obligatory to use. Other techniques, like STPA, are also possible to use for the risk analysis. The standard also prescribes that the reliability analysis should include a human machine interface analysis. No suggestion for this analysis is given and STPA can be applied for this analysis. Barnatt and Jack (2018) concluded that railway industry guidance does generally not mention STAMP or STPA. Instead, they refer to more general and more established risk analysis methods.

The reliability of a system can be demonstrated by identifying the various risks that affect the reliability requirement. Different risk analysis can contribute for identifying the risks and quantify the probability and severity. In this thesis it is investigated whether STPA is a relevant addition for identifying risks and not just whether it is a relevant replacement of current risk analysis.

> *Reliability of a system is expressed as 1 minus the probability of failure. In the reliability requirement for ERTMS, the failure event is defined whether train delay takes place or not. Failures can be classified in failure categories expressed in the extent of delays (in minutes) and identified through risk analyses.*

3.2. Reliability influenced by human-machine interactions (human error)

ERTMS is a sociotechnical system where humans interact constantly with the components of ETCS. With the introduction of ERTMS, human-machine interactions will even be more interwoven. The operational use of the equipment will change a lot for the train drivers and dispatchers. This section is about the ironies of automation, the resistance to change, human error and human information processing. These topics are related to the interactions between the train drivers, dispatchers and ETCS and will influence the reliability of the whole railway transport system. The Ironies of automation, the resistance to change and human error are all negatively influencing the system reliability. The information (indirectly) presented by ETCS to the train driver and dispatcher is processed in a certain way and a model for human information processing is illustrated at the end of this section. The feedback loops presented in this model can also be linked to the feedback loops that are present in the control structure model, which will be explained in chapter 4, for executing the STPA.

Ironies of automation

The introduction of ERTMS will make the train driver and dispatcher better informed and more supported in executing their tasks, this might lower the workload for a train driver/dispatcher if the circumstances are normal. Increase in workload is often seen as a concern, in contrary to a decrease in workload. But a decrease can lead to distraction and boredom and is even so a concern, also known as the homeostasis principle (Muttram, 2018; Wilde, 2014). This example can be seen as an irony of automation. The switch to ERTMS will not cause more system automation, but it makes the train driver and dispatcher more informed and supported in the already existing automatic train protection system. An example is the train speed that is still manually controlled by the train driver, but the speed supervision is better and more accurate.

Other ironies of automation in human-machine interactions are: automation will cause a loss of awareness and skills from the operator in the system and the operator will only monitor the automation tool. Automation is only possible if the operator is in the control loop in case the automation fails to function, the so called out-of-the-loop performance problem. Unforeseen tasks are often not automated and manual intervention is required for the more difficult tasks (Bainbridge, 1983). Those ironies of automation might become more present by implementing ERTMS and it might influence the reliability of the railway transport system negatively.

Resistance to change

Changing the automatic train protection system might cause resistance by the affected people. Møller et al. (2019) researched the operational readiness of successful ERTMS programmes. They learned from the implementation of ERTMS in Denmark that the introduction of ERTMS created resistance among some employees. Managing the changes for a smooth handover toward ERTMS operation requires proactive and dedicated management and leadership. Ambassadors of ERTMS are created by involving the different users, these ambassadors will create confidence in the change. The benefits and necessity of the change should be explained elaborately, so the users of ERTMS feel proud towards the change and they can understand that the change will benefit them in the long run. The last point that Møller et al. addresses is the importance of responding to the fear of being made redundant by introducing the new system. This can be done by good communication, listening to the fears and making a retention policy. The fear of being made redundant by ERTMS is primarily not a justified fear, but the digitalization in ERTMS may make it easier to facilitate the next grade of automation (e.g. more easy facilitating ATO) and make the train operation more automatic.

If train drivers and dispatchers change from driving under ATB-EG and NS'54 to driving under ERTMS or vice versa, then they need mitigation against repetitive behaviour they were used to under the other signalling system (Muttram, 2018). Training is crucial to change the behaviour. Action-oriented training is preferred over a learn-by-heart training and the training set up should represent the operational reality as close as possible to make the training more effective Møller et al. (2019).

Human error

Human error gained acceptance as a probable cause for accidents since the early 1960s (Hollnagel, 1992). Li et al. (2019) concluded that human error is most commonly seen as the main cause of accidents in railway systems. Models for identifying those human errors started to be developed in the 1970s, those models displayed how human information processing and decision making occurred (Hale and Hale, 1970). Rasmussen (1983) made a skill, rule and knowledge model (SKR-model). This model explains that humans first tend to perform tasks in an automated skill-based level, skills are routine actions, requires little conscious effort and is the automatic mode of operation. If this cannot be done, then mental rules are used to react on the task, this starts after conscious choices of a rule or procedure. If this also cannot be applied, then the task is performed on knowledge, where an analogy with another system is made or other abstract knowledge is used. The probability of human errors is the highest for knowledge based actions and the lowest for skill based actions. Hinzen (1993) quantified the human error of skill based activities on 1:1000, rule based on 1:100 and knowledge based on 1:10. This was debunked by Kirwan (1994), by explaining that the change of human error can vary from 1:50000 to 1:1, depending on the circumstances rather than the difference of skill, rule or knowledge decision. Nevertheless did the institution of railway signal engineers (IRSE) research about the quantification of human error by train drivers under a certain level of stress, this is summarized in Table 8, showing the parabolic shape of the human error probabilities as a function of the level of stress. Neuropsychology research confirms the different described phenomena in the SRK-model by assigning different brain areas for each decision type (Klein 2006). The probability of human error is likely to change due to the transition toward ERTMS, because the proportions in skills/rules/knowledge based decision making will change, especially in the early stages of change.

Human behaviour	Stress due to too low demands	Optimum level of stress	Stress due to excessive demands
Based on skills	2/1000	1/1000	2/1000
Based on rules	2/100	1/100	2/100
Based on knowledge	2/10	1/10	2/10

Table 8: Quantification of the probability of human error per action, based on the SKR-model and the level of stress (IRSE, 1996).

Human information processing

How humans process information, is modelled by Wickens (1984) by presenting the different psychological processes that are involved in human-machine interactions. The processing of information (light blue arrows) goes through different stages before a task is performed, this is modelled in Figure 11. Each stage requires attention and mental resources, attention is needed to understand the information, as illustrated with the dashed arrows originating from the attention/resources. Attention and mental resources determine where the focus of a person goes to in its (system) environment. Information from our environment is processed first in our senses, the sensory processing, the information is stored for a short time in our short term sensory story (STSS). The amount of information that is made available from our sensors is abundant, as illustrated with 3 arrows between the sensory processing and the perception stage. Our attention selects the input from our sensors, this is seen in the most left dashed arrow from the attention/resources oval. For train drivers this can be done by directing the eye toward the lineside signalling or driver machine interface, because eye movement and attention relate to each other (Posner, 1980). The selected information goes to the perception stage, here the information is interpreted and given a meaning. Interpretation can be done by recognizing tasks, experiences or intentions from the past, those experiences are stored in the long-term memory, this is illustrated in the figure by adding arrow originating from the long-term memory to the perception stage and just before this stage. The next stage is response selection, this is skill, rule or knowledge based, as described before in the SKR-model from Rasmussen (1983). After the response selection, the response is executed and the feedback loop is closed by the interaction with the environment.

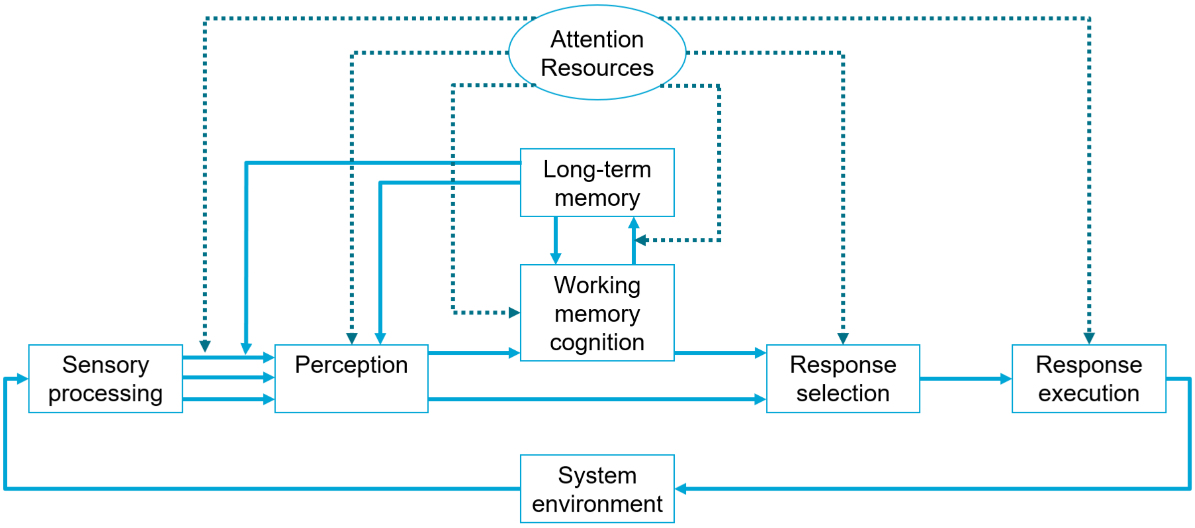


Figure 11: Human information processing model (redrawn from Wickens et al., 2016)

There are a few limitations to the information processing in the human-machine interactions, also in the railway transport system. Train drivers need to select what they give attention, not everything in the environment can be selected, our senses should first detect the signal, before it can be processed. The perception of the information can be difficult if the information is complex and uncertain for the driver. The selected response can be unsuitable because the available information is limited and the rules and protocols do not suit the situation. Lastly, the execution of the response can vary and cause execution errors.

3.3. Current reliability assessment for interactions between ETCS, train drivers and dispatchers

This section elaborates on the use of a failure mode effect and criticality analysis (FMECA). This analysis is suggested by the standard EN 50126 as a risk analysis. FMECA will be explained and the implementation for reliability assessment is discussed. FMECA is compared with STPA in section 4.3, the limitations of FMECA will therefore be discussed in that section.

FMECA is an analyses technique for system reliability and risk analysis that identifies potential failure modes (FMs) of all the system components, their criticality and their effects on system performance. FMECA can be used in the early design phase of a system and reliability analysis can be performed with this technique (Rausand et al., 2004). Another commonly used analysis technique is the qualitative analysis FMEA, it identifies the failure modes and its effects, without identifying the failure mode criticality. FMECA is more quantitative and prioritizes the failure modes via risk priority numbers. The risk priority number demonstrates the criticality and is derived from the multiplication of 3 parameters, the severity, the probability and the detectability of a failure mode (Kiran, 2017).

Sharma et al. (2005) developed a systematic approach for performing a FMECA. Step 1: Identify the system and its system components. Step 2: display the relationships of the system components in a functional block diagram. Step 3: Determine all the potential failure modes for every system component and their interactions, then determine the causes, the effects and criticality on the system and system components. Step 4: Determine how failures are identified and how the risk can be mitigated. FMECA is a bottom up approach/inductive procedure where analysis starts with identifying potential failure modes, those failure modes can lead to a cause of an undesirable event.

Current reliability assessment

The ERTMS Programme Management needs to assess the reliability of the whole railway transport system. The human error of train drivers and dispatchers will influence the reliability of the system and those errors have to be identified to analyse. Currently no official document about reliability assessment for interactions between ETCS, train drivers and dispatchers are set by the ERTMS Programme Management. In 2018 a draft was made for human error assessment in the railway transport system (van Vliet, 2018). This draft was not made final, but will be summarized in this section to demonstrate how the human errors would be identified if its analysis would take place at the moment. The analysis was also executed in 2018, but it was done with slightly outdated user processes.

The analysis is developed to identify the impact of human errors on the reliability of the transport system with ERTMS. This is done by using a series of failure mode effect and criticality analyses (FMECA). A FMECA is executed by starting to identify each user action in a user process. In total, there are 65 user processes which describe the behavioural chain of interactions between train drivers, on-board system, trackside system and train dispatchers (ProRail, 2021). Those processes demonstrate how to operate in normal situations (think of departing, splitting, combining, shunting or turning), in disrupted situations, during calamities or when driving over infrastructure that is currently under maintenance. For each user action, the FMECA describes which failure mode can occur. Subsequently, the failure cause and failure effect/event of those failure modes are described. The next step is to describe the handling after the failure effect occurred. Finally, the criticality is demonstrated by attributing a fault category to the failure mode, as defined with train delay minutes in Table 7. The in FMECA identified failure modes, the failure effect and the handling of the effects is then displayed in a bowtie diagram.

The required information for the FMECA is preferably gathered via empirical data of observed failure modes, but is usually gathered via structured expert judgements from train drivers and dispatchers. This means that the identified failure modes are logically reasoned or already known by the experts. Unknown/new failure modes for the experts are therefor probably not included in the FMECA.

The focus of the suggested analysis is on the difference between ERTMS and ATB-EG/NS’54, this is elaborated by adding a column in the FMECA that explains the increase or decrease of train delay minutes due to the implementation of ERTMS in the transport system. The suggested analysis does not include the probability of a failure mode occurring, so the reliability of the railway system is not made quantitative. The determination of how failures are identified is also not included, but this is mentioned as process step 4 in the systematic FMECA approach, developed by Sharma et al. (2005).

A PRISMA-Rail method is applied to assess what kind of mitigation measures can be taken to reduce the change or impact of failure. PRISMA stands for Prevention and Recovery Information System for Monitoring and Analysis. The PRISMA method is originally designed to build up a quantitative database of failures, which would be classified, analysed and from which conclusions can be drawn regarding optimal improvement measures. The PRISMA-Rail method is a generic approach for analysing failures in the railway transport system and developed by Van der Schaaf and Wright (2005). The method classifies the failure modes by using a root cause taxonomy. The taxonomy classifies the root cause into a limited set of abstract classes. First by classifying a failure as a technical, human operator or organisational failure. Those failure are then further classified, for example, the human operator failure is further divided into the SKR-model of Rasmussen (1983), explained in section 3.1.

Failure classification enables the ERTMS Programme Management to identify dominating recurring causes underlying a failure. The different failure classifications suggest different mitigation measures. Examples of mitigation measures are: redesign the technical system, improve procedures, improve information/communication or changing the training (van der Schaaf & Wright, 2005).

Table 9 demonstrates the suggested FMECA table framework. The failure handling includes prevention and mitigation (failure probability and consequence) measures. The table is missing categories like 'problem owner' and 'planned completion date for failure handling', which are common in FMECA tables.

User process	User action	Failure mode	Failure cause	Failure effect	Failure category (PRISMA)	Difference between ATB-EG/NS'54 and ERTMS	Failure handling

Table 9: FMECA table framework used for current reliability assessment in user processes (van Vliet, 2018)

The limitations in the use of FMECA, like not identifying certain types of risks, are described in chapter 4. This chapter will describe which benefits traditional risk analysis and especially FMECA miss, compared to STPA.

4.

Systems Theoretic Process Analysis (STPA)

As described in the scope of this thesis, Systems Theoretic Process Analysis (STPA) is a system-based hazard analysis method based on the Systems Theoretic Accident Model and Processes (STAMP). STAMP is an accident causality model that is in turn based on system theory (Leveson, 2012). STAMP is an alternative to the linear chain of failure events model which is at the basis of traditional risk analysis methods like fault tree analysis or FMECA. Appendix A demonstrates the need of STAMP as an alternative accident model over the traditional model, because current software-intensive sociotechnical systems became too complex to model it with just linear models. Leveson (2004) argues that methods based on chain of events models do not account for system accidents (accidents that result from interactions between sub-systems), human errors (humans that change their behaviour as was not described) and social and organisational factors.

The developments of ERTMS increased the coupling and complexity of the railway transport system. System theory demonstrates that explanation of accidents in complex systems cannot simply be reduced to system components, because of the interactions between the different system components. So, when doing a hazard or risk analysis, the railway transport system must be considered as a whole (Wang, 2018). STPA does look at this bigger picture and this hazard analysis method will be discussed in this chapter.

This chapter will answer the third sub-question: How can STPA be used for identifying risks and reliability in railway transport systems? This will be done by explaining the 4 STPA steps in the first section, the next section demonstrates how STPA is already applied to railway transport systems and the last section compares STPA with the currently used FMECA method.

4.1. STPA steps

STPA is a hazard analysis technique. Those techniques identify hazards, their causes and their consequences. With this information, risks in a system can be determined and mitigation/elimination measures can be taken for those hazards (Ericson, 2005). Hazard analyses investigate accidents before they occur (Leveson, 2004). With STPA hazards are identified that are caused by: human error, design errors, system interactions, software, missing design requirements, flawed assumptions and social, management and organizational factors (Thomas, 2021). STPA identifies hazardous scenarios in the whole system and not only in the electro-mechanical sub-systems (Leveson, 2012).

STPA consists of 4 primary steps, built upon system engineering basics. 1) Define the purpose of the analysis. In this first step, a definition of the system and its boundaries are given and the losses and hazards are defined which are aimed to be prevented. 2) Build a control structure model of the system. This model captures the interactions and the functional relationships in a system while using feedback control loops. This model can first be made at an abstract level and may eventually be made with more details. The model conceptualizes both the functional and structural model of a sociotechnical system. Appendix C Illustrates a few examples of a control structure. 3) In the control structure model the control actions are analysed, to examine how they could cause an in step 1 identified loss, unsafe control actions are identified by using keywords. 4) Determine how the unsafe control actions could occur by identifying causal scenarios or factors (Leveson & Thomas, 2018). The 4 steps are illustrated in Figure 12.

The scenarios and the identified unsafe control actions can be used for drafting mitigation or elimination measures, additional requirements, making recommendations for design and developing key indicators of risks (Leveson & Thomas, 2018).

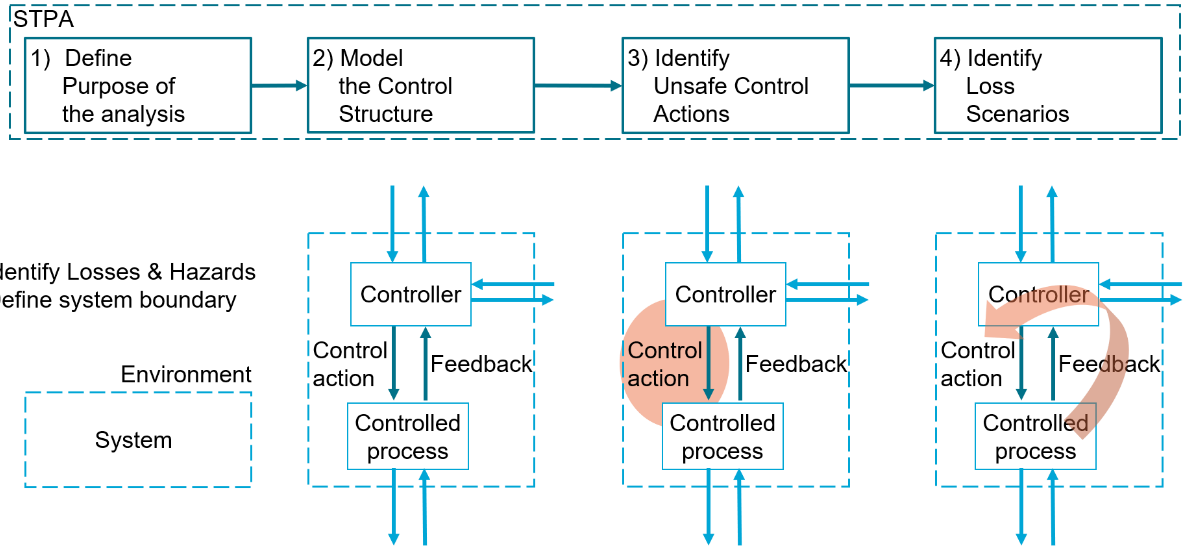


Figure 12: 4 STPA steps with graphical representation (redrawn from Leveson & Thomas, 2018)

Appendix B elaborates more on the execution of the different steps.

4.2. STPA applied for railway transport systems

STPA is gradually accepted and seen as supplementary to other hazard analysis techniques, the analysis is recognized by academics and cited for dealing with complex systems like the railway transport system (Patriarca et al., 2022). A systematic review from Zhang et al. (2022) included 121 publications about STAMP, eight of those papers used STAMP techniques in the railway transport system. This section will focus on the use of STPA applied in the railway industry, to learn from publications how STPA can be implemented and what lessons were learned. A STPA example is given to make the analysis more tangible and to give an idea of the different STPA steps.

Ouyang et al. (2010) was one of the first to make us of STAMP in the railway industry, it validated the usability of STAMP for analysing the railway transport system. Read et al. (2019) validated that STPA can be applied for hazard analysis in the railway industry, an control structure was made and analysed of the entire sociotechnical railway system in Australia. Dong (2012), Kawakami (2014) and Bugalia et al. (2020) identified causal factors with STAMP techniques, that were not already mentioned in railway accident reports.

Currently, the practical application of STPA in the railway industry is mostly still in the trial stage or in academic papers, this makes it difficult for risk managers to process the STPA results into clear leading indicators (Li et al., 2021). A leading indicator can act as a warning sign and identify where weaknesses in a system appear, so accident prevention measurements can be taken. Li et al. (2021) indicates that converting the STPA outcomes into practical interventions (like leading indicators) requires a broad understanding of the system, otherwise it may not be comprehensive.

The rest of this section illustrates examples of how STPA is executed in the railway transport system. Those examples show which different system-level hazards and corresponding constraints are chosen. And a reference is made to the related control structures in appendix C, so the first two steps of STPA are made clearer with given examples. The first described example also elaborates about which unsafe control actions and loss scenario are identified. More examples of unsafe control actions and loss scenarios are given in the referenced literature.

Examples of STPA executed for a train control system

A book by Wang (2018) discusses, among other things, different safety analysis methods of train control systems. STPA is introduced as a better suitable hazard analysis than traditional analyses for the increased complexity in train operation control systems. An example STPA is executed by analysing the handover of radio block centres (RBC) in the Chinese train control system (CTCS-3). The CTCS-3 is an equivalent to level 2 ETCS. The steps described in the STPA handbook (Leveson & Thomas, 2018) are followed, so it follows the structure as also described in appendix B.

Wang (2018) selected a system-level hazard: 'trains exceed the limitation of speed/distance in the process of Handover RBC'. The system-level safety constraint correspondents to the hazard: 'the CTCS Level 3 Train Control System should prevent the train from exceeding the safe limitation of speed/distance in the process of Handover RBC'. Step 2 of STPA is to model a control structure, this is shown in Figure 13. This figure is a good illustration, but it is not made entirely according to the STPA guidelines, because it is not entirely hierarchical drawn up (e.g. the entity 'train' should be located under 'driver') and the feedback mechanisms and control actions must be made more specific (e.g. 'input' can changed in acceleration or braking). 11 examples of unsafe control actions are identified (step 3 of STPA). For instance, 'The handover RBC did not send an MA shortened command to the vital computer in the case of an emergency occurred in the received RBC area when the train runs to the handover boundary' The corresponding safety constraint for the unsafe control action is: 'In an emergency, the RBC should be able to correctly send the MA shortened command.' The last step of the analysis is to identify the scenarios that can result in the unsafe control action. An example of a loss scenario is: 'The control algorithms of handover RBC are improper, and it believes that it is unnecessary to shorten MA for the route information in process model', 7 other scenarios are identified for this one unsafe control action.

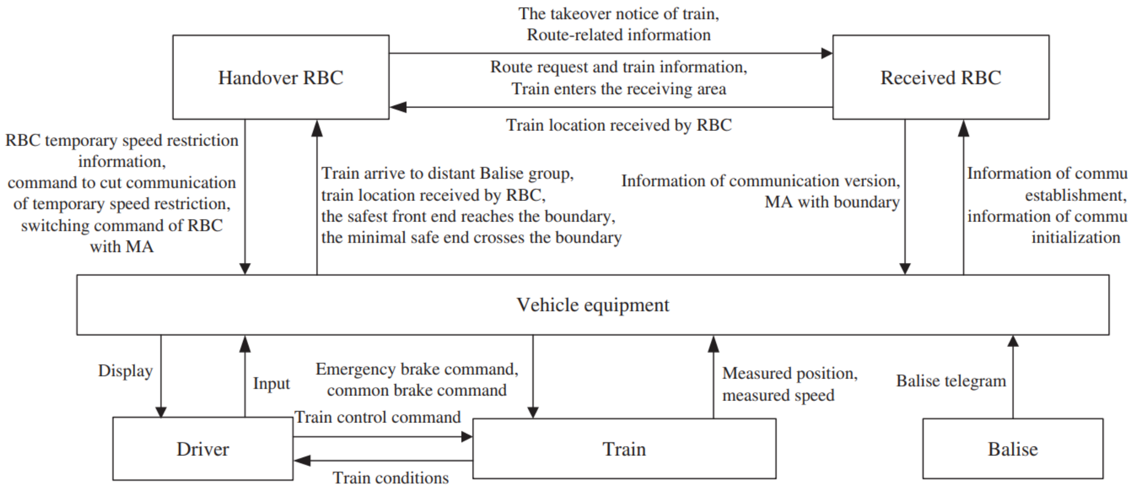

The takeover notice of train,
Route-related information
Handover RBC
Route request and train information,
Train enters the receiving area
Received RBC
Train location received by RBC
RBC temporary speed restriction information,
command to cut communication of temporary speed restriction,
switching command of RBC with MA
Train arrive to distant Balise group,
train location received by RBC,
the safest front end reaches the boundary,
the minimal safe end crosses the boundary
Information of communication version,
MA with boundary
Information of communication establishment,
information of communication initialization
Vehicle equipment
Display
Input
Emergency brake command,
common brake command
Measured position,
measured speed
Balise telegram
Train control command
Driver
Train
Balise
Train conditions

Figure 13: Control structure of RBC handover (Wang, 2018).

Li et al. (2021) also executed a small STPA with analysing a shunting procedure as example. The chosen system-level hazard is 'exceeding the speed limit' and the control structed is modelled in Figure 31, in appendix C. Appendix C illustrates general control structure and railway control structure examples, to demonstrate how others have modelled the control structure for different purposes in a railway system.

Ouyang et al. (2010) looked at the overarching sociotechnical railway transport system, including the laws and regulations for the railway industry. STPA is executed and the chosen system-level hazard is 'derailment of the train'. The corresponding safety constraints are 1. trains must run within limited speed, 2. the correct limited speed must be known for the train drivers. The control structure is illustrated in Figure 35.

Dong (2012) executed a STPA applied to the communication based train control (CBTC) system. The CBTC system provides continuous bidirectional train-to-wayside data communication, it determines the train location and it performs vital functions. The system goals (specified with a G) are: G-1. Perform safely a close headway between trains G-2. Provide automatic speed protection G-3. Provide automatic passenger protection. The overarching goal of Dong is to provide a safe and on time transportation over rails. Dong focusses on the safety, this thesis focusses on avoiding train delay minutes (in a safe manner).

Losses (specified with a L) are defined by Dong (2012) as: L-1. Train derailment L-2. Passenger injury caused by train doors L-3. Train collision with train/structure/highway vehicles/work crews/work trains. The system-level hazards (specified with a H) that follow from the defined losses are: H-1. Violate the principles of interlocking protection [linked to L-1] H2. Hazard caused by door opening [linked to L-2] H-3. Train over speed [linked to L-1 and L-3]. The relevant control structure is modelled in Figure 38. With the control structure and the system-level hazards defined, the last two steps of STPA are executed by identifying the unsafe control actions and the loss scenarios.

4.3. (Dis)advantages of STPA compared to the current FMECA technique

The traditional accident models (where FMECA is based on) suggest that sociotechnical system accidents are caused by events like human action or equipment failure. But accidents in those complex systems do not simply result from one trigger event, but from complex phenomena (de Carvalho, 2011). Just describing a complex system accident as a sequential chain of events is inadequate, as further explained in appendix A.

In the scope of this thesis, a few advantages of STPA over traditional hazard analysis are mentioned. Leveson and Thomas (2018) described a few other advantages in their STPA handbook. For instance the availability of involvement of human operators and software in the analysis. This ensures that the analysis includes all the different possible causal factors for losses. The STPA handbook also explains in chapter 3 how the analysis can be integrated into a system engineering process, like the one used by the ERTMS Programme Management. STPA can already be applied during early concept analysis, this will result in safety constraints and requirements that help designing a safe system.

FMECA and STPA both end up with causal scenarios/factors for accidents, but how those are derived is different. This can be seen in the difference in approach in appendix b and section 3.3. The different approaches cause different results and have different (dis)advantages. The two analyses are also based on different theories, STPA is based on system theory and FMECA on reliability theory.

This section compares the hazard analysis techniques STPA and FMECA, because FMECA is the currently used method to analyse hazards for user processes, as described in section 3.3. STPA can be a replacement or addition to the FMECA. This section will describe the (dis)advantages of STPA, compared to FMECA. The difference between deductive and inductive is first described, then other differences are discussed, the completeness of the different methods is described and the section ends with the main method trade-offs.

Deductive/inductive search technique

FMECA is an inductive (forward/bottom-up) search technique and described in the standard: NEN-EN-IEC 60812:2018. The technique starts with the lowest component level and from there different failure effect of the whole system are identified. STPA starts with defining the system-level losses and hazards first and then search for unsafe control actions, so it is a deductive (backward/top-down) search technique. STPA identifies how a hazard could occur. STPA uses a functional control structure model and FMECA uses a physical component diagram.

The deductive search technique is in theory more efficient than the inductive technique, because only hazardous situations are explored with the deductive search. With an inductive search, not all findings result in hazardous situations, this makes STPA take less time and effort than FMECA (Fleming et al., 2013). Unlike inductive search, deductive search can identify combinations of initial events that may lead to a hazard (Pawlicki et al., 2016).

Complex systems involve design errors that can cause accidents. With design errors, no system component fails, because the component does what its meant to do. With the inductive technique FMECA those errors are not identified, because the components are executed as intended. The deductive STPA technique does find design errors, because it does not treat safety as a system component failure, but as a system control problem (Leveson, 2004).

FMECA compared to STPA

The difference between deductive and inductive search technique is an example of the difference between FMECA and STPA. When FMECA and STPA is compared with each other, many other differences are identified, which will be described in this section.

The results from FMECA are more quantitative than the results from STPA. STPA is developed to identify hazards, but not to quantify the probability or impact of those hazards. Identifying the rate of occurrence and the severity of risks that may result from a hazard can be determined after the 4 STPA steps are executed, this can help prioritizing which elimination/mitigation measurements are needed (Patriarca et al., 2022).

STPA can identify causal scenarios, instead of only identifying causal factors (like in FMECA). It is harder to identify causal scenarios, than causal factors. The most common mistake made in executing STPA is to not identify causal scenarios, but only individual causal factors (Leveson and Thomas, 2018). Examples of individual causal factors are: sensor failure, delayed feedback mechanism or loss of input. Listing those causal factors alongside the scenarios context can easily result in overlooking indirect/non-obvious causal factors that can lead to hazard or unsafe control actions. Interactions between and combinations of different factors are also more easily overlooked (Ericson, 2005). When only causal factors and no causal scenarios are identified, then the STPA becomes more like a FMECA (Leveson and Thomas, 2018).

Identifying causal scenarios makes the analysis of STPA more challenging. Executing STPA is a bit more complex, if compared to FMECA. The needed control structure model in STPA is difficult to construct and verify by non-experts of the analysed system. System experts have more difficult in identifying the causal scenarios of a hazard in STPA, than identifying the causal factors of a hazard in FMECA (Sulaman et al., 2019). FMECA is more easily understood, because it uses a worksheet structure what needs to be filled in. The next section describes the completeness of the analysis techniques with the amount and the kind of hazards that are identified.

Completeness of the analysis techniques

In the desk research executed for this thesis, two papers and a master thesis were found that researched the completeness of STPA results, when specifically compared to FME(C)A results. The master thesis executed a case study in the automotive industry (Martinez, 2015) on an electric power steering system and the authors of the STPA handbook, Leveson and Thomas, were the supervisors for this research. One paper executed a case study in the pharmaceutical industry (Pawlicki et al., 2016), with the analysis techniques demonstrated on a new online adaptive cranial radiosurgery procedure. Leveson was a co-author of this research. The other paper was developed without involvement of the STPA developers, this paper also executed a case study in the automotive industry (Sulaman et al., 2019) on a forward collision avoidance system.

The two papers and master thesis included interactions with other components and the analysed systems included hardware, software and human interference. The papers and thesis concluded that STPA can find more causal scenarios/factors than FME(C)A and that the structured process of STPA result in a more complete hazard analysis. STPA is compared to FME(C)A and STPA is described as the more effective hazard analysis technique.

Martinez (2015) identified with STPA, 121 causes of hazards in the automotive industry. And 83 hazard causes were identified with FMEA. Those causes are subdivided in 5 causality categories: Engineering design, component failure, (lack of) correspondence, interaction and physical degradation. STPA has significant more causes in the engineering design category (STPA: 47 causes, FMEA: 28 causes) and the interactions category (STPA: 32 causes, FMEA: 13 causes), compared to FMEA. All the identified causes found with FMEA in this study were also identified by STPA. Some of the STPA identified causes were more general, so those cover the more in detail causes that were identified by FMEA (Martinez, 2015).

The research by Pawlicki et al. (2016) identified 472 causes of hazards with STPA and 132 causes of hazards with FMEA in the pharmaceutical industry. This research also divided the causes in causality categories and more causes were found by STPA in all the categories, especially the causes that involve interactions of hardware, software and people. Pawlicki et al. (2016) mentions that, even though STPA identified more causes of hazards, there could be hazards that are still not identified. There is no way of validating if a hazard analysis is complete. A hazard analysis is always subject to the analysts limitations and things like the available time (Pawlicki et al., 2016).

Sulaman et al. (2019) concluded without the involvement of the STPA authors that there is a significant difference between the causal factors that are identified by STPA and FMEA. The identified causes by STPA cover more aspects and are described in more detail. The more detailed description of causes is mainly due to the use of keywords in STPA step 3 that identify unsafe control actions. STPA identified in particular more component interaction hazard causes.

Sulaman et al. (2019) mentions the difference in focus in the two methods. STPA is mainly stronger in identifying the causal factors/scenarios of hazards. FMEA is mainly stronger in risk assessment of identified failures by calculating the risk priority number. Sulaman et al. (2019) concludes by emphasizing that the two different methods complement each other in this study.

Method trade-offs

Choosing between techniques that are based on chain of events (like FMECA) and STPA is a trade-off between the number of identified causes for hazards and easy to use of the technique. Chain of events techniques oversimplify the causes of accidents and is less thorough, because they exclude complex interactions between system components (Leveson 2012).

A judgement about the usability of a technique is subjective, every analysis technique has different strengths and weaknesses. No single technique can be usable for every analyst, because the needs of the analyst differ (Underwood & Waterson, 2014). Underwood and Waterson (2014) mention a more general trade-off than Leveson (2012), namely the trade-off between thoroughness of the analysis technique and the number of resources made available for the analyses. Examples of resources are: time and money. It is justifiable to do a hazard analysis as thorough as possible, because the cost and time to executing the analysis are small in comparison to investigating an accident or changing the system if it is already in use (Underwood & Waterson, 2014).

A hazard method can be chosen based on the available resources, but also on the usability of the method or a way of thinking that suits the analyst better (Underwood & Waterson, 2013). An analyst can prefer FMECA over STPA, because the analyst is used to do hazard analysis with FMECA and is unfamiliar with executing STPA. Because STPA is relatively a new hazard analysis, far fewer people are experts in STPA.

It is impossible to identify all hazards in a complex system or fully eliminate human errors, so not with STPA either (Leveson, 2015). STPA can be used complementary with FMECA, meeting the advantages of both analyses.

Main advantages of STPA over FMECA: involvement of human operators and software in the analysis; identify design errors; more complete/thorough in identifying causal scenarios/factors

Main disadvantages of STPA over FMECA: no quantitative results; more complexity due to the making of a representative control structure and finding causal scenarios; less used in practice

5.

STPA application

The railway transport system, its reliability and the hazard analysis technique STPA are discussed in the previous chapters. This chapter answers the sub-question: ‘What are the hazards caused by interactions between train drivers, dispatchers and ETCS?’ This question will be answered by applying STPA in a case study. The interactions between ETCS, train drivers and dispatchers are described in user processes, where the different actions are explained to perform a certain procedure, such as starting up a train. The user processes are in line with the technical specifications for interoperability for operation (EU, 2019). For the case study, one of the user processes is chosen to analyse. Analysing more user processes consumes more time. When the results show that STPA is capable of providing relevant (new) results, STPA can be used for more user processes, but this is due to the time-consuming actions out of the scope of this thesis.

The user process: ‘Combining two trains arriving from opposite directions with movement authority’ is chosen. This process is selected out of the 65 described user processes, because it is executed in normal operation, frequently occurring and is relatively complex due to the many interactions.

The first section describes the user process for the case study. Section 5.2. up to and including section 5.5 execute STPA, as described in appendix B. To execute step 2 (section 5.3) and step 4 (section 5.5) of the STPA, two separate workshops are organised to obtain relevant results. The last section explains how STPA can be practically implemented within a railway organisation, this is done by conducting three interviews.

5.1. Description of chosen user process

The user process of combining two trains that arrive from opposite directions and have movement authority is labelled as user process 48 in the user processes document drawn up for ERTMS level 2 (ProRail, 2022c), illustrated in appendix D. The process is also expressed in words in an operational concept description for the start of commercial operation with ERTMS level 2 (ERTMS Programme Management, 2022). Combining is connecting two trains into one train. This user process describes the procedure for combining trains that come from opposite directions on a location set up as a combining track (Dutch: combineerspoor).

> *User process 48:*
> *Combining two trains arriving from opposite directions with movement authority*

Combining trains is carried out relatively often with a regular passenger train. Many trains are lengthened before rush hour, by combining shunting trains. The process can also be carried out after an unplanned event, for example if a defective train has to be towed away.

This user process assumes that the first train has full supervision movement authority (FSMA) when driving into the combining track. A second assumption is that the second train is in front of the stop marker bord (a blue square with orange arrow) and has FSMA with End of Authority (EoA) at the stop marker bord (SMB). A third assumption is that the combined train departs in the direction in which the second train arrived.

Figure 14 illustrates a situation sketch of the user process. The figure includes the two trains in yellow, the combining track in grey, the five stop marker bords alongside the track and under the track an illustration is given of the different ETCS driving modes and speed profiles. Appendix D illustrates with a behavioural chain how different actors are involved in the process and it takes Figure 14 as an example to go through the process. The process is also expressed in words under the figure. Figure 7 in section 2.1 already illustrated an architecture model of ERTMS level 2, the actors in user process 48 are illustrated in the figure as: dispatcher, ETCS trackside, ETCS onboard and driver.

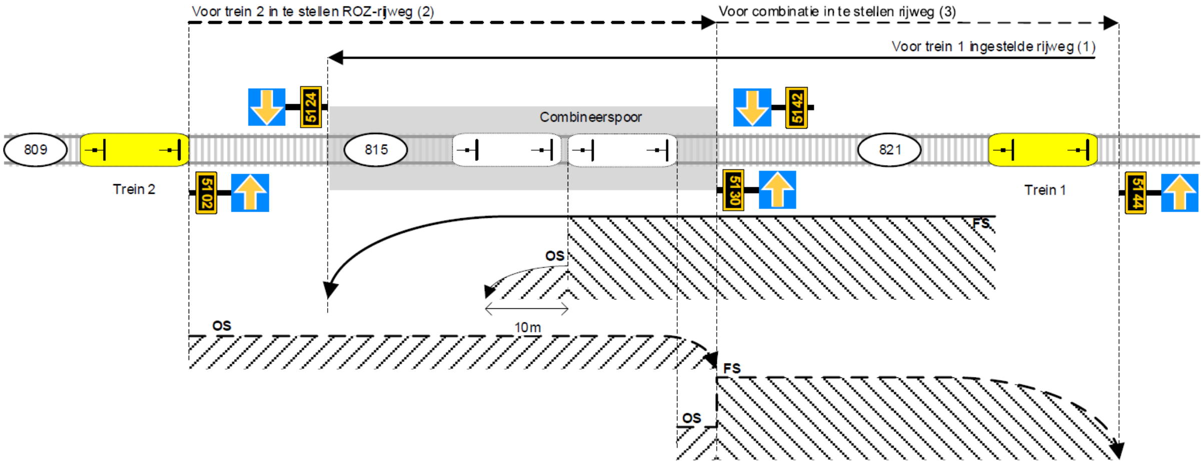

Voor trein 2 in te stellen ROZ-rijweg (2)
Voor combinatie in te stellen rijweg (3)
Voor trein 1 ingestelde rijweg (1)
Combineerspoor
5124
5142
809
815
821
Trein 2
Trein 1
5102
5130
5144
FS
OS
OS
10m
FS
OS

Figure 14: User process 48 example illustration: Combining two trains arriving from opposite directions with movement authority (ProRail, 2022c).

In the user process, different operation modes in ETCS are used which define the movement authority: full supervision (FS), on sight (OS), stand by (SB) and sleeping (SL). In FS mode, the train is fully guarded by ETCS and track information is present in the ETCS on-board equipment. In OS mode, the train is limited guarded by ETCS and the drivers drives by sight. The track might be occupied by another train and the maximum permitted speed in the Netherlands is 40 km/h. The train drivers determines the correct stop position. In SB mode, ETCS monitors that the train remains stationary. SL mode is used in cabs with no train driver, because the train is operated from another cabin.

Train 1 (the yellow train on the right of the figure) has full supervision movement authority (FSMA) and travels to the combination track. When train 1 has come to a standstill, a ROZ (driving on sight) route can be set by the train dispatcher for train 2 in the combine track (where train 1 is already present). The ETCS trackside system checks whether train 1 is actually standing still by checking the position report of the train, no ROZ route is set for train 2 if train 1 is not standing still. If train 1 is standing still, then the ROZ route is set and the full supervision movement authority is converted to on sight movement authority (OSMA) to a few meters before the current train 1 position. The train driver of train 1 confirms the movement authority by clicking on an on sight logo in its DMI. After the ETCS trackside system has determined that the movement authority of train 1 has been adjusted to on sight, train 2 receives an on sight movement authority that ends at the end of the combining track.

The driver of train 2 also confirms the switch to on sight mode and then drives the train visually to a distance suitable for coupling from train 1. After that, the trains can be coupled. An end of mission is performed in both trains, before or after coupling, because the operated cabins are located in the middle of the combined train, the combined train cannot be run from either cabin. By performing an end of mission, the cabins go into stand by mode. The mode automatically switches from stand by mode to sleeping mode if the control current (Dutch: stuurstroom) is connected. Now a driver will perform a start of mission for the combined train in the cabin in front of the train and depart according to another user process (user process 1).

The order in which the two trains are coupled can differ, the trains in the explanation and figure above can also be exchanged with each other, so train 2 can also start the user process from the left side of the illustration in Figure 14.

A main point for attention for the train dispatcher is that the ROZ route can only be set after the ETCS trackside system has detected a standstill of the train on the respective track. A main point for attention for the train driver of train 1 is that the full supervision is shortened and converted in on sight movement authority. A main point for attention for the other train driver is that the train automatically switches to sleeping mode if the trains are combined.

The main differences between the user process under ERTMS and the user process under ATB-EG/NS’54 are the ETCS modes are introduced in ERTMS. Under ATB-EG/NS’54 is confirming the ROZ route not applicable. Under ERTMS the user process is applied with ETCS equipment (ETCS on-board and ETCS trackside) which is new for the train driver and dispatcher.

Identified hazards with FMECA

FMECA is applied on this user process, following the steps described in section 3.3, compiled by van Vliet (2018). With a group of train drivers and dispatchers all the user processes are analysed with FMECA, so also for user process 48. The focus of this FMECA was on identifying the impact of human errors on the reliability of the transport system with ERTMS. Only hazards caused by the train driver or dispatcher are identified, so no hazard are identified related to the electro-mechanical sub-systems in ERTMS.

The analysis identified 4 issues: 1. The dispatcher applies a normal route instead of a ROZ route. 2. The train driver does not confirm the on sight movement authority within 5 seconds and starts driving. 3. The first train drives too far and drives out of the combining track. 4. Combining trains fails, because the train driver of train 2 stopped the train too early.

From the 4 issues, 3 of them were issues that were already identified in other user processes, before user process 48 was analysed. Issue 1 was identified in the first analysed user process. Issue 2 in the second and issue 4 was identified in tenth user process.

The results of the FMECA were looked up and written down after all the steps of STPA (in the next sections) were executed. So the results of the FMECA did not influence the process of applying STPA and identifying the loss scenarios.

5.2. Step 1: Define purpose of the analysis

The first step of STPA is to define the purpose of the analysis, this is done by identifying the system-level losses, the system-level hazards and system-level constraints.

A loss involves something of value and is unacceptable to the stakeholders. Examples of stakeholders are train passengers and railway undertakings. An example of what they value is that the transportation is provided on time and safe. When the value is translated into a loss, examples of losses are loss of transportation goal or loss of life/health/customer satisfaction.

The Loss will be based on the reliability requirement formulated in section 3.1. A loss in reliability of the railway transport system is a goal loss. The railway transport system function is to carry out the activities for the movement of people and/or goods by rails, this should be done safe and on time. The research question of this thesis is about how the system reliability can be determined by applying STPA, so the chosen loss is a loss of transportation goal. This can be expressed in train delay minutes, as already substantiated in section 3.1. The transportation goal loss can be caused in many different ways.

To define the system-level hazard, the system and its boundaries must be identified. The analysis of STPA is performed on the user process described in section 5.1. The system in which this user process occurs is the system described in section 2.1 in Figure 7. The system includes the interactions between ETCS, train driver and the dispatcher, so the system does not include the whole sociotechnical railway transport system which includes the system development actors and regulatory agencies. Inside these system boundaries, the ERTMS Programme Management has some control. Setting system boundaries over the part of the system where one has some control is advised by the STPA handbook (Leveson & Thomas, 2018).

The system-level hazards are defined by identifying the system states/conditions that can lead to a loss. A system-level hazard refers to the whole system, will lead to a loss in a worst case environment and describes a state or condition that needs to be prevented. The system-level hazards used for executing the STPA on user process 48 are:

- H-1: Train stands still or does not run at the best operational speed (that is permitted)
- H-2: Relevant movement authority is not given or adhered to

Examples of safety constraints corresponding to the system-level hazards are:
SC-1: If a train does not run or does not run at the best operational speed, than this must be detected and measures must be taken to prevent further standstill or slow movement (H-1).
SC-2: A train must not unintentionally pass the issued movement authority (H-2).
SC-3: If a train unintentionally passes the issued on sight movement authority, the system must detect this and take measures (H-2).
SC-4: The appropriate authorization must be given if the correct conditions are met (H-2).

5.3. Step 2: Modelling the control structure

Modelling the control structure is the second step of STPA. A model views a complex reality as a simplified abstract. How much the reality is simplified depends on the purpose of the model, the STPA handbook (Leveson & Thomas, 2018) provides guidance in how a control structure model is made. Appendix C illustrates different examples of control structure models. A control structure is composed of feedback control loops and enforces constraints on the behaviour of the overall system.

The STPA handbook advises to start modelling an abstract control structure and iteratively add more detail. The control actions and the feedback arrows in the model should be labelled with functional information. A controller is positioned above the controlled process, this results in a hierarchical model where all downward arrows are control actions and all upward arrows are feedback.

To model the control structure for the user process described in section 5.1., a general control structure that functions as a starting model to create specific user process is first created. This general control structure can be used to base a specific user process control structure on. Performing a STPA on all the different user process can be time intensive. By designing a general control structure, a specific user control structure is made faster/easier. Performing a STPA on a generic control structure is less applicable, because the generic control actions will result in generic unsafe control actions in step 3 of STPA, which will make it difficult to identify specific loss scenarios in the last STPA step.

Workshop 'modelling a control structure'

A workshop was organised to model the general control structure and the control structure for user process 48. Two participants were invited for the workshop. One of the participants is thoroughly involved in making user processes for the Dutch railway system (with ERTMS) and the other participant executed a STPA on an user process in 2015. So knowledge about user process specific information and how STPA could be applied was present at the workshop. The theory of modelling a control structure is directly translated into practice in a workshop through exercises. Organizing a workshop was chosen over individual conversations, because it creates synergy and encourages more interactivity. No preparation was required of the participants, only a rough planning was given about the workshop. The workshop was partly inspired by the workshop description of Read et al. (2019). Read et al. organised a workshop to model the whole sociotechnical railway transport system in Australia.

The workshop organised for this thesis started with an introduction about STPA, and the main points of attention to develop a control structure for STPA. A few PowerPoint slides of a presentation from Thomas (2020) were used to illustrate do's and don'ts in modelling a control structure. More control structure information was shared with the participants by discussing six control structures from different authors that focus primarily on the interactions between train driver, ETCS and dispatcher. Namely, six control structures illustrated in appendix C: Figure 30, Figure 31, Figure 34, Figure 37, Figure 38 and Figure 40.

The presented theory was translated into practice by discussing with each other which actors should be included in a generic control structure that can act as a basis for the user process control structures. After an agreement on a generic control structure, the workshop continued by discussing the user process 'combining two trains arriving from opposite directions with movement authority'. The workshop participants discussed which actors are involved, what their responsibilities are, which control actions they execute and which feedback they receive. The workshop concluded by modelling the control structure for user process 48.

The different parts of the workshop are briefly described in appendix E.

General control structure

The four main actors described in the user processes document drawn up for ERTMS level 2 (ProRail, 2022c) are used as main actors in the general control structure. Those main actors are: train driver, train system, trackside system and dispatcher. By retaining the main actors form the user processes document, the general control structure can be more easily converted to an user process specific control structure. The main points that will vary in the specific control structures are the specific applicable control actions and feedback. For some user process control structures, the structure will have to be supplemented with another actor and the associated interactions.

The train system concerns all the (sub)systems that are available to the driver. Systems that are in the train system are illustrated in Figure 7 with the ETCS onboard and the train with its train operating equipment. On the basis of status information in the train system, the system can independently impose braking interventions, if this is necessary from a safety point of view. The train driver operates the train system and receives feedback from the train system (e.g. a dynamic speed profile via the DMI).

The trackside system concerns all the (sub)systems that are available to the dispatcher. Systems that are in the trackside system are illustrated in Figure 7 with the ETCS trackside (RBC and balises), interlocking, the GSM-R module and the traffic control system. The dispatcher gives the trackside system central operating commands and receives feedback from the trackside system, via the traffic control system and the interlocking.

The interactions between the main actors are partly standardized with technical specifications for interoperability (TSI). The TSI relating to the operation and traffic management subsystem (TSI OPE) describes the specifications for interactions between the driver and dispatcher and the driver with the ETCS on-board (ERA, 2019). The TSI relating to the control-command and signalling subsystem (TSI CCS) describes the specifications for interactions between the ETCS trackside and ETCS on-board (ERA, 2016b). The interactions between the Dispatcher and the ETCS trackside is not standardized by a TSI. The user processes are in line with the technical specifications for interoperability. The train and trackside system communicate with each other via GSM-R data and balises. Movement authority, train position and status information can be communicated between the two systems. The train driver and dispatcher can communicate via GSM-R voice.

Figure 15 Illustrates the general control structure. The downward arrows are control actions and the upward arrows are feedback. The horizontal dashed arrow is a (passive or active) communication channel and not a control action, nor feedback. The control structure does not show all the physical implementations of the architecture of the train/trackside system, as shown in Figure 7. A control structure developed in STPA is not intended to become a physical model, but to become a functional model.

The control action and the feedback descriptions are vague and implemented for illustration in Figure 15, those should give specific functional information. Each specific user process control structure will have different control action and feedback descriptions. Figure 15 makes clear that the train system is the controlled system and that the dispatcher is highest in the hierarchy of control, this means that the dispatcher can perform control actions on the trackside system and the driver. Being higher in hierarchy of the control structure is also related to the hierarchy of responsibilities and goals, the goals of the dispatcher are more overarching than the goals of a train driver that operates one train system.

The mechanisms by which a controller executes its control action on the controlled process (an actuator) and the mechanisms by which a controlled process gives feedback for a controller (a sensor) are excluded from the control structure, to make the control structure more abstract.

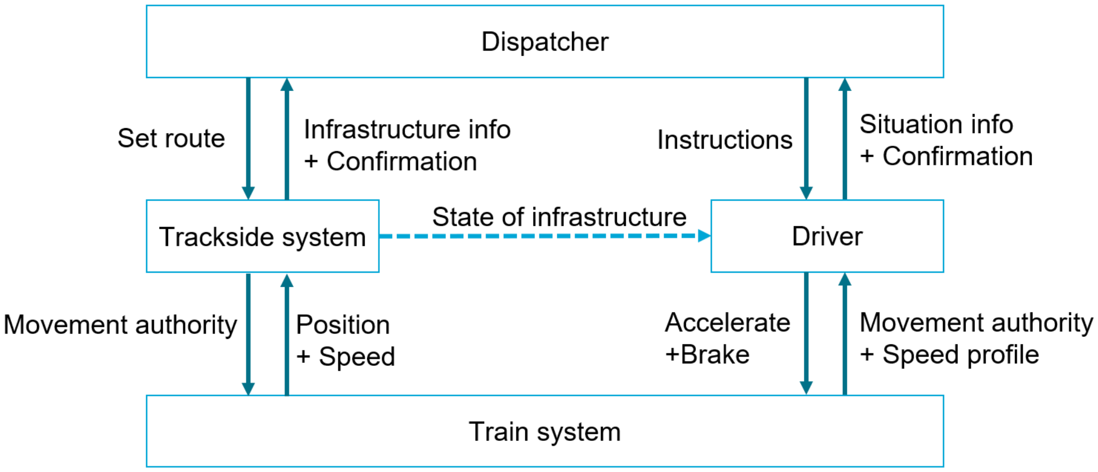


Figure 15: General control structure that can be used to base a specific user process control structure on

User process 48 control structure

Based on the general control structure, a control structure is made for user process 48, this is illustrated in Figure 16. The control structure used the actors described in section 5.1. and appendix D, those are the same actors as in the general control structure with an additional driver and train system. The control actions and feedback are derived from the workshop, by going through the procedure of user process 48 and note all the control actions and feedback.

A remarkable point is the lack of interactions between the dispatcher and driver, none is included in the user process and therefor none in the control structure. Another modification, compared to the general control structure is the addition of a second driver and train system. The interactions with those additional actors are the same as the first driver and train system. The interactions with the first driver and train system have been blurred to make the control structure clearer. For executing the following STPA steps, writing down two times the same control actions and feedback mechanisms is not necessary.

The horizontal dashed arrow is just like the general control structure a (passive/active) communication channel without any control actions or feedback. The SMB informs the driver in the user process what the physical borders are for the combining track. The information exchange between the two different train systems is enabled when the trains are combined.

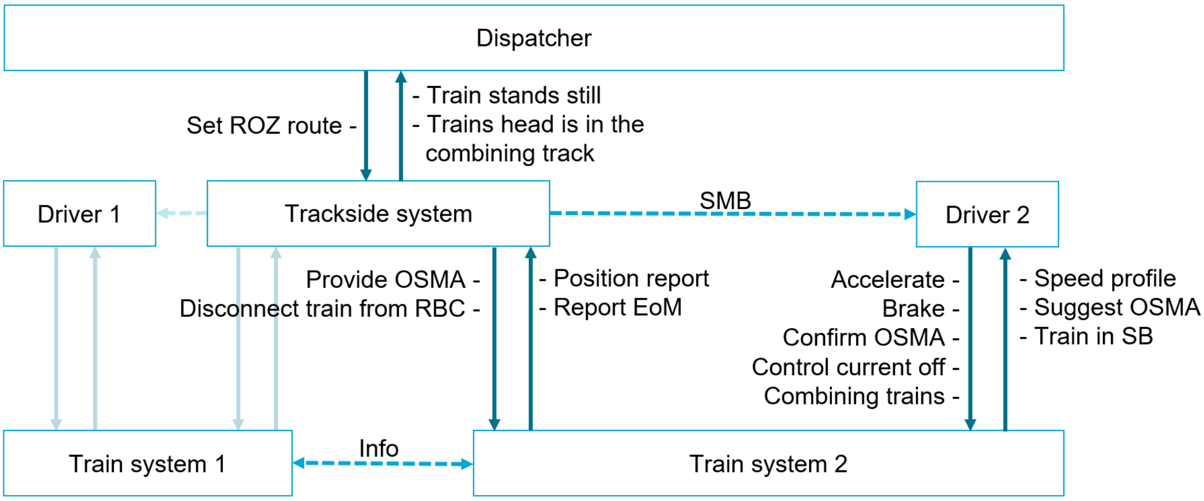


Figure 16: Control structure for user process 48

OSMA stands for on sight movement authority, SB is an abbreviation for stand by. SB and OSMA are operation modes in ETCS.

The responsibilities of actors are expressed in the given control actions and received feedback. Table 9 elaborates about the responsibility of an actor in user process 48, the control actions and feedback that are involved with the corresponding controlled process.

Actor	Responsibility	Controlled process	Control action	Feedback
Dispatcher	Set route on the right time	Trackside system	Set ROZ route	Train (1) stands still, Trains (1) head is in the combining track
Driver (1 and 2)	Operate train in a safe manner for a combining trains procedure	Train system	Accelerate, Brake, Confirm OSMA, Control current off, Combining trains	Speed profile Suggest OSMA, Train in SB
Trackside system	Release a safe route (with movement authority)	Train system	Provide OSMA, Disconnect Train from RBC	Position report, Report EoM
Train system (1 and 2)	Safe movement of the train	-	-	-

Table 10: Responsibilities, control actions and feedback of the actors in user process 48

5.4. Step 3: Identify unsafe control actions

The third step of STPA is identifying unsafe control actions, this is executed with a systematic approach. Unsafe control actions are identified by analysing each control action with guide words (Not providing, providing, too early/too late/wrong order, stopping too soon/applying too long). A control action can be unsafe if:

- Not providing the control action leads to a hazard.
- Providing the control action leads to a hazard.
- Providing a potentially safe control action but too early, too late, or in the wrong order
- The control action lasts too long or is stopped too soon (for continuous control actions, not discrete ones).

Every unsafe control action (UCA) results in at least one hazard and an UCA should refer to its relevant context. Appendix F structured the unsafe control actions in tables for the three different controllers. An example table is illustrated in Table 11.

Control action	Not providing	Providing	Too early, too late or wrong order	Stopping too soon, applying too long

Table 11: Example table to identify the unsafe control actions for each control action in a structured manner

The UCA's are identified by following the STPA handbook (Leveson & Thomas, 2018). The identified UCA's were viewed for a second opinion by someone who knows STPA and the user process.

The identified unsafe control actions are:

- UCA-1: Dispatcher not setting a ROZ route while the train is ready to drive onto the combining track [H-2]
- UCA-2: Dispatcher not setting a ROZ route, because another route (normal or signal passed at danger) is set instead [H-2]
- UCA-3: Dispatcher setting a ROZ route on the wrong track [H-2]
- UCA-4: Dispatcher sets ROZ too early for train 2, while train 1 is not in stand still [H-2]
- UCA-5: Driver does not provide acceleration control action while train drives slower than permitted speed [H-1]
- UCA-6: Driver provides acceleration control action while train drives harder than the permitted speed [H-1]
- UCA-7: Driver provides the acceleration control action with an insufficient level of acceleration while train drives slower than permitted speed [H-1]
- UCA-8: Driver provides the acceleration too late (>TBD seconds) after the train drives slower than permitted speed [H-1]
- UCA-9: Driver stops providing the acceleration control action too early, before the train drives on permitted speed [H-1]
- UCA-10: Driver applies the acceleration control action too long, while the train is already on permitted speed [H-1]
- UCA-11: Driver does not provide the brake while train drives harder than permitted speed [H-1]

- UCA-12: Driver provides the brake while train drives slower than or at the permitted speed [H-1]
- UCA-13: Driver provides the brake with an insufficient level of braking while train drives harder than permitted speed [H-1]
- UCA-14: Driver provides the brake and stops the train before the train is in the right position in the combining track [H-1]
- UCA-15: Driver provides the brake too late (>TBD seconds) after driver receives speeding warning [H-1]
- UCA-16: Driver stopped too soon with braking, while train is not yet standing still in the combining track [H-1]
- UCA-17: Driver does not confirm OSMA, while train system suggests applying OSMA on the DMI and train drives into combining track [H-2]
- UCA-18: Driver does not switch the control current off, while the driver leaves the cab [H-1]
- UCA-19: Driver switches the control current off, while the train still needs to be operated [H-1]
- UCA-20: Driver does not combine trains, while both trains are ready to combine [H-1]
- UCA-21: Driver combines train while not following the combining procedure [H-1]
- UCA-22: Driver combines trains too early, while not all actions for preparations are done [H-1]
- UCA-23: Driver stopping too soon with combining trains, while not all combining actions are done [H-1]
- UCA-24: Trackside system not providing an OSMA while the train is ready to drive in the combining track [H-2]
- UCA-25: Trackside system providing an OSMA for the wrong track [H-2]
- UCA-26: Trackside system does not disconnect the train from the RBC, while the control current is shut off [H-2]
- UCA-27: Trackside system disconnects train from RBC, while the train is still operated by the driver [H-2]

After the unsafe control actions are defined, controller constraints can be written down. A controller constraint is a constraint for the behaviour of the controller that needs to be met to prevent the unsafe control action. Those constraint are put in appendix F.

5.5. Step 4: Identify loss scenarios

The fourth and last step described in STPA is to identify loss scenarios. A loss scenario is described by the STPA handbook (Leveson & Thomas, 2018) as a scenario that describes how causal factors lead to hazard and unsafe control actions. As summarized in appendix B, the loss scenarios are divided into 2 different types:

1. Scenarios that lead to the identified unsafe control actions
2. Scenarios where the control actions could be improperly/not executed.

For the first type of scenarios, the identified UCAs from step 3 are used. The second type of scenarios does not use the UCAs, and only focusses on the control actions.

Both types of scenarios are again subdivided into 2 other loss scenario categories:

1.1. Controller behaviour that is unsafe (the controller; upper part of the control model)
1.2. Feedback and other inputs that are inadequate (the feedback; right part of the control model)
2.1. Causal factors that affect the control path (the control action; left part of the control model)
2.2. Causal factors that affect the controlled process (the controlled process; lower part of the control model)

Those four categories of scenarios are further subdivided with examples to guide the scenario identification process further.

Besides the examples for the different kind of scenarios in the STPA handbook, no suggestion is provided for an approach to identify the scenarios. Different approaches can be useful, if at least all the relevant scenario categories are considered for the UCAs (scenario categories 1.1. and 1.2.) and control actions (scenario categories 2.1. and 2.2). Enough expert knowledge about user process 48 is also needed to perform step 4 of STPA.

Workshop identifying loss scenarios

A workshop was organised to identify the loss scenarios. A workshop was chosen for the same reason as described in section 5.3. Two participants were invited for the workshop, one participant was also present in the workshop for modelling the control structure (the one who has experience of performing STPA on a user process). The other participant had no experience with STPA, but has expert knowledge about the analysed user process.

The workshop started by discussing user process 48, so the procedure of combining two trains arriving from opposite directions was understood well. Then STPA was explained and the system-level hazards, the modelled control structure and the identified unsafe control actions were shown. Step 4 of STPA, the identification of loss scenarios, was elaborately explained with examples from the STPA handbook.

After informing about STPA, the collaboration started. The different actuators and sensors between the four actors in het control structure were identified to better identify loss scenarios. The loss scenarios were then identified, this was done via a systematic approach. First, the first UCA was discussed and the first two categories of loss scenarios (1.1. and 1.2.) were identified for this UCA. When all the UCAs for one control action were discussed (for example: UCA 1, 2, 3 and 4 are all about the control action of setting a ROZ route) and loss scenarios were identified accordingly, then the other two categories of loss scenarios (2.1. and 2.2.) were discussed for the same control action.

After the workshop was done, the identified scenarios were written down according to the STPA handbook guidelines. Loss scenarios were identified for the 27 UCAs and for the 8 control actions involved in the user process.

Four hours were scheduled for the workshop, the first two hours were used to explain STPA, elaborate about how loss scenarios are identified and identifying the actuators and sensors. The remaining 2 hours were not enough to work through all the UCAs and control actions. To finish the workshop, 2 extra hours were needed the next day.

Identified loss scenarios

Actuators and sensors are identified in the workshop, because these can be helpful to identify scenarios for specific causes of unsafe feedback or control. Actuators execute the control actions and feedback is measured or detected by sensors. Defining what the sensors and actuators are between the different actors in the control structure for user process 48 took half an hour. Discussions were about what can be seen as an actuator or sensor and if the suggested actuators/sensors are not just communication devices. A few sensors and actuators are mentioned in the loss scenarios, for example the odometer as sensor or the DMI as indirect actuator.

The loss scenarios identified in the workshop are written down at a level of detail as was discussed in the workshop. Some scenarios could be worked out in more detail, but if it has not been discussed in more detail in the workshop, it has not been written down in more detail. All the loss scenarios are structured in appendix G. The loss scenarios are also provided in this paragraph, but (almost) duplicate scenarios are combined and recurring phrases are abbreviated using quotation marks.

ROZ route loss scenarios (LS)

- LS-1: 'Dispatcher not setting a ROZ route while the train is ready to drive onto the combining track (UCA-1)', because the dispatchers training is inadequate, new systems are used under ERTMS (for example 'ERTMS Treininformatiesysteem'/ETIS) and the procedure changes. The dispatcher may be wrong with the old procedure and think that a call is needed to confirm that the train is standing still.
- LS-2: '…', because the dispatcher thinks that the train is not yet standing still, because the dispatcher once had experience with a train driver who drove very slowly.
- LS-3: '…', because the dispatcher expects the train to move slightly, even if it is currently standing still. The dispatcher relies on the system, but thinks the train will move slightly again. The dispatcher does not receive confirmation from the driver that the train will not move again.
- LS-4: '...', because the feedback from the trackside system does not send a position report. This might be caused by no connection between the 'procesleiding' and ETIS, but also between ETIS and the RBC.
- LS-5: '…', because the train movement is not included in the route plan (Dutch: rijwegplan), so the dispatcher does not know that the combining of the train is planned.
- LS-6: '…', because the configurations are not consistent between procesleiding and ETIS. Example: ETIS says that the train is on spot A, but the procesleiding thinks that this spot is somewhere else or does not know the spot. (LS-9, LS-12, LS-17 and LS-67 have a similar scenario with the same configurations inconsistencies causing an UCA)
- LS-7: 'Dispatcher not setting a ROZ route, but another route (normal or signal passed at danger) is set instead (UCA-2)', because the dispatcher does not know which track are combining tracks (the procesleiding does not differentiate tracks between normal and combining tracks) and might think that the train wants a normal route if the route plan is not followed.
- LS-8: '…', because a ROZ route is not possible (for example, due to a switch malfunction) and the dispatcher choses for the possibility of a signal passed at danger route.
- LS-10: 'Dispatcher setting a ROZ route on the wrong track (UCA-3)', because the dispatcher is used to combine on another track and thinks that the route plan is wrong.

- LS-11: '…', because the dispatcher makes a mistake by applying the ROZ route for a different route of another train that needs to combine.
- LS-13: 'Dispatcher sets ROZ too early for train 2, while train 1 is not in stand still (UCA-4)', because the dispatcher is in a hurry and thinks that the train is almost stopped.
- LS-14: '…', because the dispatcher forgot to check if the train is standing still.
- LS-15: '…', because train incorrectly reports that it is standing still, due to an odometry error. (LS-18, LS-22, LS-24, LS-27, LS-29, LS-35, LS-39, LS-41 and LS-45 have a similar scenario with the same odometry error causing an UCA)
- LS-16: ROZ route is not set due to malfunctioning of hardware or software, the mouse of the dispatcher might break or no selection of ROZ can be chosen in procesleiding. [H-2]

Accelerating loss scenarios

- LS-19: 'Driver does not provide acceleration control action while train drives slower than permitted speed (UCA-5)', because past experience makes the driver think the train is coming from the same direction and the driver stops at the wrong place of the combining track
- LS-20: '…', because the driver thinks that the train has a different length than the actual length and does not accelerate, due to habituation of driving with another length of the train on the same track. (LS-23, LS-26 LS-28, LS-37, LS-40 and LS-44 have a similar scenario with the same habituation with other train lengths/weights causing an UCA)
- LS-21: '…', because the signage along the track is misinterpreted by the driver.
- LS-25: Driver provides the acceleration too late (>TBD seconds) after the train drives slower than permitted speed (UCA-8), because the driver is distracted, no sound notification is provided if the train drives too slow.
- LS-30: Driver applies the acceleration control action too long, while the train is already on permitted speed (UCA-10), because the driver is distracted and the warning sound is broken/not heard.
- LS-31: The acceleration control action is improper executed due to engine failure [H-1]
- LS-32: The acceleration control action is improper executed because the lever sticks, so acceleration is less or too much provided. [H-1]
- LS-33: Environmental factors, like a slope in the track, can cause the vehicle to drive too fast without acceleration. [H-1]
- LS-34: Environmental factors, like a slippery track, can cause a lack of acceleration. [H-1]

Braking loss scenarios

- LS-36: 'Driver does not provide the brake while train drives harder than permitted speed (UCA-11)', because past experience makes the driver think the train is coming from the same direction and the driver stops at the wrong place of the combining track.
- LS-38: '…', because the signage along the track is misinterpreted by the driver.
- LS-42: Driver provides the brake and stops the train before the train is in the right position in the combining track (UCA-14), because it is not clear for the driver where to stop exactly on the combining track. The driver can be used to combining with trains coming from the same direction, instead of combining with trains coming from opposite directions. The first driver often does not know in which direction the second train is arriving from.
- LS-43: Driver provides the brake too late (>TBD seconds) after driver receives speeding warning (UCA-15), because the driver is distracted and the warning sound is broken/not heard.
- LS-46: The brake control action is improper executed due to engine failure [H-1]
- LS-47: The brake control action is improper executed because the lever sticks, so acceleration is less or too much provided. [H-1]
- LS-48: Environmental factors, like a slippery track, can cause a lack of deceleration. [H-1]

Confirming OSMA loss scenarios

- LS-49: 'Driver does not confirm OSMA, while train system suggests applying OSMA on the DMI and train drives into combining track (UCA-17)', because the driver thinks that the combine track is positioned further away, due to experiences of other combine tracks on other platforms.

- LS-50: '…', because the driver does not pay attention to the DMI and the sound for new notifications on the DMI is missed or interpreted as a sound for another notification.
- LS-51: '…', because the driver is distracted by other messages on the control table or from outside, causing the driver to forget to confirm.
- LS-52: Confirming OSMA is not executed, because the DMI touchscreen broke or is not sensitive enough for dirty/greasy/wet fingers. [H-2]

Switching the control current off loss scenarios

- LS-53: 'Driver does not switch the control current off, while the driver leaves the cab (UCA-18)', because the driver is used to other trains and does not know how to switch of the control current of its train.
- LS-54: '…', because the driver is in a hurry and forgets it. No warning is given when driver leaves the cab
- LS-55: 'Driver switches the control current off, while the train still needs to be operated (UCA-19)', because the accidently touched it or mistake it with another function.
- LS-56: '…', because the driver 1 thinks that the other train comes from the same direction to combine the trains. In the procedure for this other user process (user process 50), driver 1 switches its control current off if the train is standing still. So, both driver are switching its control current off and the trains cannot be combined. The first driver does not know in which direction the second train is arriving from.
- LS-57: Switching of the control current is not executed, because the switch broke. [H-1]

Combining trains loss scenarios

- LS-58: 'Driver does not combine trains, while both trains are ready to combine (UCA-20)', because driver 1 mixes up procedures (user process 48 and 50) and expects the other driver to combine the trains.
- LS-59: '…', because driver 1 does not know if train 2 is ready to combine (for example, if the control current is switched off)
- LS-60: Driver combines train while not following the combining procedure (UCA-21), because the type of train is different than usual and the driver is used to a different procedure.
- LS-61: Driver combines trains too early, while not all actions for preparations are done (UCA-22), because driver 1 does not know if train 2 is ready to combine (for example, if the control current is switched off)
- LS-62: 'Driver stopping too soon with combining trains, while not all combining actions are done (UCA-23)', because the type of train is different than usual and the driver is used to a different procedure.
- LS-63: '…', because the driver receives only visual feedback of the physical state of the coupling and thinks that the trains are combined. Insufficient feedback is received by the driver.
- LS-64: Combining trains is executed incorrect, causing incorrectly connected trains (for example, the electromechanical parts are not connected properly). [H-1]

Providing an OSMA loss scenarios

- LS-65: 'Trackside system not providing an OSMA while the train is ready to drive in the combining track (UCA-24)', because RBC, IXL or GSM-R is malfunctioning.
- LS-66: '…', because the train system sends a position report that indicates that the train is moving, but in reality, the train is standing still. This can be caused by an odometry error.
- LS-68: Providing an OSMA is not executed due to GSM-R errors and information is partially/not transmitted. Those errors can be caused by power failure, hacking or interventions by jammers (for example 5G transmitters)[H-2]

Disconnecting the train from the RBC loss scenarios

- LS-69: Trackside system does not disconnect the train from the RBC, while the control current is shut off (UCA-26), because the End of mission is not received by the trackside system, due to GSM-R errors or train system not sending it.
- LS-70: Trackside system disconnects train from RBC, while the train is still operated by the driver (UCA-27), because connection between train and trackside system is disconnected (>TBD seconds) due to a GSM-R error.

Analysis of the loss scenarios

In total, 70 loss scenarios are identified. Most of the identified loss scenarios are related to the first 2 scenario categories (1.1. and 1.2.). The examples given in the STPA handbook are about as many examples for the first 2 scenario categories as for the last 2 scenario categories. But the first 2 categories are applied to every UCA under a control action (there are for example 4 UCAs for the control action 'setting a ROZ route') and the last 2 scenario categories are applied to only the control action itself. This difference resulted in 15 loss scenarios identified that are related to setting a ROZ route scenario for categories 1.1. and 1.2. and 2 loss scenarios identified that are related to setting a ROZ route scenario for categories 2.1. and 2.2.

A few remarkable comments about the identified loss scenarios are discussed below, references are made with the loss scenario identifications (for example: LS-1).

- The train driver does not provide feedback to the dispatcher about if the driver intends to not move the train anymore, this can lead to LS-3. So a feedback mechanism is missing for the dispatcher. In LS-3, the dispatcher expects that the driver will start moving again and no ROZ route is set (UCA-1).
- The dispatcher cannot see which tracks are combining tracks and which are normal tracks on its screen. This can lead to LS-7.
- A number of loss scenarios are related to each other, because they reoccur under other UCAs or are similar to them. For example: the same configurations inconsistencies (LS-6, LS-9, LS-12, LS-17 and LS-67), the same habituation with other train lengths/weights (LS-20, LS-23, LS-26 LS-28, LS-37, LS-40 and LS-44) or the same odometry error (LS-15, LS-18, LS-22, LS-24, LS-27, LS-29, LS-35, LS-39, LS-41 and LS-45)
- A sound message is given if new information is provided on the DMI or if the train drives faster than permitted, but no sound is given if the train drives a lot slower (>TBD km/h slower) than permitted, which can lead to delays (LS-25).
- The loss scenarios for accelerating and braking are the opposites, just like with the UCAs of those control actions.
- Where the first train needs to stop exactly in the combining track can be unclear, the train driver often does not know from which direction the other train is arriving from and a stop sign (a transportable blue lamp) is not always present, which can lead to LS-42.
- The touchscreen of the DMI might malfunction or be inoperable when fingers are dirty/greasy/wet, no computer mouse or backup screen is available to still execute tasks on the DMI (LS-52).
- No reminder is present or warning is given to switch off the control current when the driver leaves the cab (LS-54).
- In user process 48 (combining trains arriving from opposite directions), the train that arrives second in the combining track switches off its control current first, in user process 50 (combining trains arriving from the same direction) the train that arrives first in the combining track switches off its control current first. The first train driver does not know from which

direction the other train arrives, so the driver might switch off its control current and the second driver could do the same, according to the user processes (LS-56).

- The user processes 48 and 50 are almost similar, so those could be mixed up. In user process 48, driver 1 combines the train, in user process 50, the second driver combines the train. This can lead into confusion and both drivers not combining the train. Especially, because the first arriving driver does not know from which direction the other train arrives (LS-58).
- Train driver 1 does not know exactly when the combining trains procedure can start, because the second driver does not give feedback to the first driver that the train is ready for combining (LS-59 and LS-61).
- The driver that combines the trains does not receive feedback on its DMI that combining the trains went well, the driver can only see the physical state of the coupling (LS-63).
- The loss scenarios between the trackside and train systems are technical related, because no human is involved in the interactions. The loss scenarios are less specific and often about failing actuators. More scenarios and more specific scenarios can be identified if there were workshop participants with more technical knowledge about the different specific system components (LS-65, LS-66, LS-67, LS-68, LS-69 and LS-70).

5.6. Implementation of STPA in the railway transport system

The previous sections applied STPA on an user process, this section elaborates further about how STPA can be implemented in the railway transport system. As seen in section 4.2., STPA is useful outside the narrow scope of user processes and can be implemented in the whole/different parts of the sociotechnical transport system.

How STPA can be implemented in the railway transport system is researched by conducting semi-structured interviews to gather in-depth information from experts by experience. Interviews were chosen over questionnaires or surveys because the researched subject is very specific and the number of experts by experience is relatively small.

Semi-structured interviews were held individually with 3 participants that have experience with applying STPA in the Dutch railway transport system. One participant has little experience by only partly executing STPA, the others executed STPA fully on one or two different projects. The interviews were conducted via Teams on the 10th of august 2022. The author of this thesis did also answer the questions and this was done in writing on the 17th of august 2022, after STPA was fully applied on user process 48. The interviews lasted between 60 and 90 minutes. The interviews were recorded, transcribed checked by participants and approved by participants, those are found in appendix I. The structure and the questions of the interview are described in appendix H, this appendix was sent to the participants two days prior the interview took place. The interviews started with a few practical questions to sketch the context of the interviewee. The main part of the interview consists of two parts. The first part is about the experiences of the interviewee with STPA and the second part are questions about how STPA can be applied within the railway transport system with ERTMS. A total of 16 questions were asked in the main part. The questions are based on questions that arose from the previous chapters and conversations with a few of the research supervisors of this thesis.

Analysis of the interviews

The answers of the 3 interviewed persons and the responses from the author himself are found in appendix I, this section will summarize the answers.

Why the interviewees started using STPA is divers, one interviewee searched an accident analysis and found STPA by chance, another searched for an analyses model to analyse the whole railway transport system. STPA is still used by one interviewee if it can analyse risks by different controllers and a control structure is helpful for this analysis. Two interviewees stopped using STPA, one stopped because of the type of trivial risks one identifies, the other one because no one (other than the interviewee self) in the organisation knows how to perform a STPA.

The mentioned advantages of STPA are: it is a very structured method and not superficial, it analyses more than just a single object, it helps to model a control structure and it gives specific tools to identify loss scenarios. The mentioned disadvantages of STPA are: it is a lot of work, many (reoccurring) loss scenarios, the unfamiliarity of the analysis in organisations, wrongs in the beginning of the analysis will result in wrongs in the loss scenarios and the analysis stops abrupt after loss scenarios are identified.

A few of the lessons learned by the participants are: scope the system that you analyse with STPA down to things you control, try to exclude similar unsafe control actions, decide which information must be shared during a meeting with expert to identify loss scenarios, diffuse systems like the railway transport system can be analysed with STPA, STPA helps with system thinking and STPA can be used for identifying risks in systems that are not yet developed.

Opinions differed between the participants about the complexity to learn STPA, some found it more complex than other methods. A reason for the extra complexity is the lack of STPA experts to ask for help and the overview in the amount of loss scenarios can be lost easily. ‘Don’t try this at home’ was a quote of an interviewee, referring to the difficulty of executing the analysis fully. FRAM (functional resonance analysis method) is suggested as a more approachable alternative for modelling complex socio-technical systems.

The first step of STPA (define purpose) is seen as the least time consuming and most easy step by all participants. Modelling the control structure (step 2) is seen as a time consuming and difficult task by three of the four participants. One interviewee found the identification of unsafe control actions (step 3) time consuming. The last step, identifying loss scenarios is according to all participants a difficult and time consuming step of STPA.

The results of STPA are not compared to other hazard analysis techniques by any interviewee.

When STPA is executed, a list of loss scenarios are identified, but no follow-up steps are provided to do something with these findings. A few tips are given by the participants to practically do something with the loss scenarios: you can go through each loss scenario and every scenario can be put in a risk matrix and risk mitigations can be applied, a hazardlog can be applied where the scenarios are defined and mitigated accordingly, the analysis technique PRISMA can be used (as already described in section 3.3.) or identify leading indicators for risk management (as described in chapter 6 of the STPA handbook). An interviewee mentioned that the modelled control structure can also function as an illustration to explain a complex system and can be seen as a practical implication of STPA.

To implement STPA successfully into an organisation a few tips are provided: the organisation must accept STPA as a method to use, a few people must be well trained in STPA and a STPA expert or guru is needed that has experience with STPA applying on different real projects, so questions can be asked to the expert and the expert can check if STPA is applied well.

Different answers were given on the question about which parts of the railway transport system are worth the effort of STPA. It depends on the purpose of the analysis. STPA can be used for overarching systems (like systems of systems) or not yet developed systems, but you must have some kind of influence on the analysed system, otherwise the loss scenarios cannot be changed. Opposing opinions were shared about applying STPA on user processes, one interviewee said that other techniques (like HAZOP) are as suitable for this analysis, one interviewee said that STPA is a relevant method to apply on user processes, because different controllers are present in those procedures. The participants agreed on the opinion that STPA is not worth the effort for simple or standalone systems, because those often do not have different controllers.

To execute STPA, experts are needed on STPA and on the analysed system/process. Try to perform STPA yourself and check with the system experts if assumption are right. In step 4 of STPA, system experts are necessary to perform the step. It can also be helpful to invite someone who is not an expert of the system, that person can asks the right questions and is critical about the system. Involve system experts by starting with a rough explanation about STPA, give easy examples for clarification and elaborate about the definitions that are used in STPA to prevent miscommunication.

STPA can be used besides other hazard/risk analyses if the surroundings of the system need to be included in the analysis or if a system is not yet well defined. Be critical in deciding for which project STPA is suitable. None of the participants said that STPA can replace the current (traditional) hazard analyses fully. The main reason for this is that STPA is not seen as complete, a risk matrix or a hazardlog with mitigation measures is still needed.

6.

Discussion

The key results from the desk research, the case study and the interviews are discussed in this chapter. This discussion focusses on the interpretations, implications and limitations of the results. The results from the desk research (chapter 2 till 4) are compared with the results from the case study and interviews (chapter 5). How do they relate to each other and what are the similarities and contradictions? The limitations of the results are acknowledged throughout the discussion. The conclusions and recommendations follow after the discussion, in the next chapter.

The desk research demonstrated what changes for the train driver and dispatcher when they switch from ATB-EG/NS'54 toward ERTMS. The results of this research demonstrated different kinds of changes, the results ranged from a shift of visual focus for the train driver to new intervention possibilities for train dispatchers. The identified changes are universally formulated. Per railway undertaking the changes can be formulated more specific, based on the specific equipment and procedure they use. The identified changes for the drivers and dispatchers are not processed in any way in the executed STPA, because STPA analyses the designed system and not the change in the system. The changes did demonstrate the urgency to apply a hazard analysis on procedures for drivers and dispatchers, because those changes can result in new, changed or removed risks that influence the reliability of the railway transport system.

This study indicates that reliability can be formulated in different ways. The reliability of the railway transport system is expressed in this study as 1 minus the probability of failure. In the formulated reliability requirement for ERTMS, a failure event is defined whether train delay takes place or not. The system reliability is partly influenced by the more interwoven human-machine interactions, due to the introduction of ERTMS. User process 48 (combining of trains arriving from opposite directions) is a procedure that illustrates a few of those human-machine interactions. In this study, STPA is applied to identify loss scenarios for this user process. STPA does not quantify the probability or impact of those loss scenarios, but the results may contribute to substantiating the reliability of the railway transport system. This can be done by quantifying the loss scenarios with expert judgment on the probability of occurring and the number of train delay minutes that the scenario will cause. So the results of STPA need to be translated into risks (with severity and rate of occurrence) to say something about how they influence the reliability.

As was described by Patriarca et al. (2022), the rate of occurrence and the severity of the loss scenario's should also be determined to make STPA more quantitative. The interviewees and literature acknowledged that STPA does not provide follow-up steps after the loss scenarios are identified. They also suggested to quantify the results, by applying a harardlog, PRISMA or leading indicators. Quantification can lead to an analysis and evaluation of the loss scenarios.

Seventy loss scenarios were identified by applying STPA on one user process. This will be a lot more if all the 65 user processes are analysed with STPA. STPA can identify many (reoccurring) loss scenarios, as mentioned as a disadvantage in the interviews. For readability and clarity reasons, the (almost) duplicate loss scenarios should be removed in the opinion of the author of this thesis, as was done in section 5.5. and not in appendix G. And a prioritization of the results are favourable to target the scenarios that have a high probability of occurring or a high negative impact, this prioritization is subjective and should be done by system experts to achieve the best results. The impact can be categorized in the already made failure categories in Table 7. The identified loss scenarios should be workable by applying prioritization, so acceptable and unacceptable scenarios are differentiated and the results are made manageable.

An advantage of STPA over traditional hazard analyses (like FMECA) that is mentioned multiple times in the interviews and was not found in the literature review (in the comparison of FMECA and STPA), is that STPA is very structured and not superficial. The steps of STPA are clear and the loss scenarios are identified via a well-guided method. The downside of this is that the interviewees found STPA a lot of work, even though Leveson & Thomas (2018) claim that STPA requires about 2 or 3 times less time to find the same and more causal scenarios. The opinion of the interviewees might be influenced by the lack of applying STPA fully for a few times, because all the interviewees did not apply STPA fully on more than 2 different projects.

Constructing the control structure made the interactions between the operating parts of the railway transport system became clearer. The control structure illustrated the hierarchy of which actor influences other actors and it illustrated how the control actions and feedback mechanisms work in the system. When the two control structures for this research are compared with the different control structures in appendix C, differences are noticeable. Differences could be caused by the time period those structures were made in. If control structures were made before March 2018, then those structures were modelled before the STPA handbook was published with a step-by-step plan for modelling a control structure. Many control structure in appendix C did not have the hierarchy right, not all downward arrows were control actions and not all upward arrows were feedback.

When FMECA was applied on user process 48, only 4 issues were identified. When STPA was applied on user process 48, 70 loss scenarios were identified. In simple terms, issues are somewhat simpler loss scenarios. Even though many of the loss scenarios are closely related or even duplicates, without those closely related scenarios does STPA identify far more than 4 loss scenarios. The 4 issues identified by FMECA are also identified with more context by STPA. The circumstances under which the two analyses were conducted do differ, with the main difference that STPA was applied on only 1 user process and FMECA was applied on all the 65 user processes. The time spend for identifying the issues in FMECA is unknown for the author of this thesis, but it is likely that less time was spend with FMECA on 1 user process, than the time that was spend with STPA on this user process. Subjectivity is also a factor that influences the amount/kind of results. Both analysis involve subjectivity and it is likely that the results obtained by different risk analysts will differ, even if the same information is shared and the same process is analysed (Redmill, 2002). When the results of FMECA and STPA are compared, STPA identified more detailed loss scenarios and most scenarios were not identified by FMECA. The newly identified loss scenarios varied widely and are mainly related to interactions and how unsafe control actions could take place. This makes sense, because STPA treats losses as a control problem, instead of a component failure. Even though a lot more loss scenarios are identified by STPA, it cannot be proven that all scenarios are now identified for this user process. It is also unknown for the author of this thesis if the newly identified loss scenarios are truly new and not yet discovered in other hazard analyses besides the FMECA.

STPA is applied on only 1 user process, but the fourth sub-question for this thesis is about the hazards caused by interactions between train drivers, dispatchers and ETCS. So, this sub-question is about more than 1 user process. In the scope of this research, it was already stated that only one user process is analysed, due to the available time. The author of this thesis predicts that the number of identified loss scenarios by this 1 user process is representative for the number of identified loss scenarios in other user processes, because the user processes differ in details, but the actors are mostly the same. So, if STPA is applied to other user processes, the analysis will also produce multiple unidentified loss scenarios. Other user processes are different, but not significantly different, all the processes have interactions between different actors and those are often the train driver, the dispatcher, the trackside system and the train system. The results of Step 1 of STPA can mostly remain the same if another user process is analysed for the same purpose. A control structure with the applicable actors and associated control actions and feedback can be made with the general control structure (Figure 15) as a base. For the last step of STPA, identifying loss scenarios, are experts necessary for relevant results. Especially this last step will be time consuming, even if the experts understand how the analysis is done and what the principles behind STPA are. Applying STPA on user processes for freight transport might even so be relevant for identifying new loss scenarios, because those processes only differ a little bit with the passenger transport. The user processes (with ERTMS) used outside the Netherlands will also be similar, due to the mandatory technical specifications for interoperability, so STPA can also be applied for those user processes.

The two organised workshops to apply the second (model the control structure) and fourth step (identify loss scenarios) of STPA were drafted without the support of the STPA handbook. The setup of the workshop for modelling the control structure worked well, the results were as expected and the workshop went according to the plan. The workshop for identifying loss scenarios required more time than anticipated and the setup of the workshop could improve in different ways. First of all by identifying loss scenarios by myself, prior to the meeting. Some of the more obvious loss scenarios can already be identified, without expert knowledge about the system. This makes the workshop less time consuming and it also provides a few examples of loss scenarios that the workshop participants help with understanding the systematic steps of STPA. The longer the workshop lasts, the less focussed the participants are in identifying loss scenarios. Nevertheless, 70 loss scenarios are identified in the workshop. It can also be helpful to identify the loss scenarios in an iterative manner, by analysing only one UCA of a control action and proceed by analysing an UCA from another control action. By temporary skipping the UCAs from the same control action, the participants keep their focus, because the analysed UCAs are not as similar as the previous one.

STPA identified new loss scenarios that were not found with the previously used method FMECA. The claims that STPA identifies loss scenarios that are not found by traditional hazard identification methods (like FMECA) can be a reason to implement STPA into relevant organisations. Chapter 8 of the STPA handbook (Leveson & Thomas, 2018) and the interviewees provide tips to implement STPA successfully into an organisation. An interviewee commented that only a few organisation are familiar with STPA and that STPA is not yet acknowledged as a suitable hazard analysis technique. As the literature review from Zhang et al. (2022) showed, only a few cases are known in the literature that apply STPA in the rail sector. To implement STPA into an organisation, the organisation itself must accept the method and make STPA available to use in standard processes. Demonstration project can help by presenting the advantages and the use of STPA, this thesis is an example of that. The interviewees mentioned that experts/gurus in STPA are necessary for a good implementation of STPA in an organisation. Those experts should have experience with applying STPA on real projects and not just be trained with the STPA handbook. STPA is learned by doing and learning STPA is most difficult for people who are used to doing traditional hazard analyses (Leveson & Thomas, 2018). The experts can review STPA results, facilitate initial STPA training, help with defining the purpose, help with modelling the control structure and questions can be asked to the experts, so the experts provide guidance and expertise. When STPA is applied in an organisation, the appropriate technical knowledge about the analysed system must be in place to implement the method.

The number of interviewees is a limitation of the conducted interviews. Only 3 interviewees were found that had experience with applying STPA in the Dutch railway transport system. Those interviewees provided an in-depth understanding of their experiences with STPA and their recommendations for implementing STPA in an organisation. The answers of the interviewees are subjective and cannot be generalized to a large extend.

7.

Conclusions and recommendations

This last chapter contains the conclusions and recommendations from this research. First the research sub-questions are answered after which the main research question is answered. Academic and practical recommendations are provided after the conclusions.

Sub-question 1: How will the introduction of ERTMS influence train drivers and dispatchers?

The Dutch railway transport system is introduced with the radio-based signalling standard ERTMS. the automatic train protection system ATB-EG and the block signalling system NS’54 will be replaced on different lines by ERTMS level 2. With ERTMS level 2, communication between train and track becomes digital and light signalling along the track are replaced by in-cab signalling. The train drivers and dispatchers interact with ERTMS and notice the most from the transition toward ERTMS.

Train drivers experience the introduction of ERTMS in different manners. The main changes are: A shift of movement authority from outside to in-cab. Communication via ERTMS standardized GSM-R equipment. More information is required to be filled in the DMI before driving. Driver becomes more reactive on what the DMI shows with the braking curve and proactive with the increase of available information. Extra and different user processes.

The main changes for dispatchers are: More operable infrastructure. Increase in available information about the trains. New intervention possibilities and new indirect functionalities.

Sub-question 2: What is reliability in the railway transport system and how is this currently demonstrated?

On technical component level, reliability is often expressed in the amount of time the component is available. Reliability of the railway transport system can be formulated in many different ways. This thesis expresses reliability of the railway transport system as 1 minus the cumulative probability of failure over time. The system fails if it cannot achieve its system goal of providing safe and on-time transportation of people and/or goods by rail. The reliability requirement for ERTMS focusses on the on-time part and defines failure whether train delay takes place or not. Those failures can be classified in failure categories that express the train delay in an extent of delays (in minutes).

The reliability is influenced by human-machine interactions and the failures can be identified through risk analyses. The reliability of the interactions between ETCS, train drivers and dispatchers are currently demonstrated by the means of a FMECA. The FMECA identified failures and determined the cause, the effects, the handling, the classification in failure categories, the difference of the failure between ERTMS and ATB-EG/NS’54, prevention measures and mitigation measures. FMECA is a traditional/sequential method that is not sufficient to analyse socio-technical systems or system of systems.

Sub-question 3: How can STPA be used for identifying risks and reliability in railway transport systems?

The hazard analysis technique STPA identifies all kinds of hazardous scenarios in the whole system, hazards that are caused by human error/design error/software/interactions/management or organizational factors. So it focuses on more than the electro-mechanical sub-systems. STPA provides a structured approach to identify scenarios that can lead to unsafe control actions or improperly executed control actions. STPA is gradually accepted and applied as a (supplementary) hazard analysis in some railway transport systems around the world. The desk research shows that STPA can be used for identifying hazards in the railway transport system in a systematic way, examples varied from analysed user process to analysing the overarching socio-technical system. A literature study indicates that STPA identifies hazards which are missing in FMECA. With the by STPA identified hazards, the risks can be formulated and the reliability of the railway transport system can be more substantiated.

Sub-question 4: What are the hazards caused by interactions between train drivers, dispatchers and ETCS?

STPA identified 27 unsafe control actions and 70 loss scenarios for the user process about combining trains that arrive from opposite directions. Those loss scenarios are hazards that are a part of the system-level hazards: 1. Train stands still or does not run at the best operational speed (that is permitted) 2. Relevant movement authority is not given or adhered to.

Some of the hazards included missing, failing or inadequate feedback mechanisms/sensors for one of the three controllers (train dispatcher, trackside system and train driver), which leads to unsafe control actions. Other hazards included design flaws/inconsistent process models, like habituation with previous driven trains or confusion with almost similar other procedures, which leads to unsafe control actions. Some controllers could experience actuator errors, like configurations inconsistencies.

Main research question: To what extent can STPA be applied to identify risks and determine the system reliability of interactions between ETCS, train drivers and dispatchers?

The implementation of ERTMS will remove, alter and add hazards in the railway transport system, but traditional hazard analyses are insufficient to identify these hazards. The STPA method is made to model complex systems (including software and humans) and identify hazards in those complex systems. STPA identifies more (challenging) hazards/loss scenarios than traditional hazard analyses do, so STPA can be applied to identify those. After the hazards are identified, the STPA method described in the STPA handbook stops with the hazard analyses. To identify the risks and determine the system reliability, the qualitative hazard should be quantified. The probability of occurring and the impact in train delay minutes should be determined for each hazard to quantify the reliability of the railway transport system.

The application of STPA to an user process illustrated many more loss scenarios/hazards than the currently applied tradition technique FMECA identified. 70 loss scenarios with STPA and only 4 issues were identified with FMECA. This quantitively illustrates that STPA is advantageous to analyse the interactions between ETCS, train drivers and dispatchers. The loss scenarios illustrated besides the technical failure scenarios also design flaws in the procedure and unsafe interactions with unsafe control actions or inadequate feedback.

Applying STPA in an organisation is made easy due to the elaborately described systematic approach depicted in the STPA handbook, but it also has some boundary conditions. The method needs to be accepted and be made available by the organisation. And experts in STPA are necessary for a good implementation of STPA. Those challenges can be taken away by trainings and experiences of employees of the organization that applied STPA on a complex system.

Academic recommendations

Applying STPA on user process 48 provided new identified loss scenarios, but as is concluded, the STPA method stops once the loss scenarios are identified. Future studies could address this by researching the possibilities of relevant follow up steps with STPA. The follow up steps can include a method to analyse and evaluate the identified loss scenarios, so appropriate elimination or mitigation measurements can be described. Exploiting the identified loss scenarios can be done by applying a risk matrix, hazard registers, hazardlog, PRISMA or leading indicators are examples that can help with implementing the STPA results and were suggested in the conducted interviews.

Traditional hazard analyses techniques are insufficient to identify the hazards of socio-technical system and system-of-systems, like the railway transport system. This thesis used the modern hazard analysis technique STPA which is based on systems theory concepts. But there are more modern hazard analysis techniques that claim to sufficiently identify the hazards in complex systems. Further research is needed to determine if and how those other techniques could be applied to identify hazards due to interactions between ETCS, train drivers and dispatchers. The results of those other techniques can also be compared with the results of this thesis. As mentioned in the interviews, one of those techniques is the Functional Resonance Analysis Model (FRAM), developed by Hollnagel (2004). Another technique that is mentioned repeatedly in the literature alongside STPA and FRAM is AcciMap (Hulme et al., 2019). AcciMap is developed by Rasmussen (1997).

The control actions or feedback mechanisms in STPA may change over time. System dynamics (SD) models can be used to model and understand dynamic changes in systems. SD makes also use of feedback loops, but models them differently than in STPA. The linkages are easily understood thanks to the model. The model includes variables and arrows that indicate whether an influence is positive or negative. The identified hazards in STPA can be further analysed with a SD model, especially hazards that are influenced by organizational/contextual aspects or hazards that result from dynamic and multiple changes in the system (Leveson, 2012). SD helps with visualizing causal relations and informing about positive and negative feedback loops. With SD, the connection between different control structures can be modelled (e.g. control structures from different user processes). Examples of SD applied to a railway transport system is done in Kawakami (2014) and Bugalia et al. (2020). With the results from this thesis, user process 48 can be further analysed with SD, to analyse the interconnectedness with other user processes or to analyse more contextual factors that influence the user process. New hazards might be identified and the model of SD can be used to illustrate how unsafe control actions or loss scenarios could occur.

The last academic recommendation is to apply STPA on the whole Dutch railway transport system, including the system development part and the whole system operations part with legislatures and other stakeholders. Modelling the control structure can already identify if feedback or control actions are missing. The model can also be used to illustrate how the control is organised in the railway transport system. STPA can be used to identify loss scenarios in other parts of the railway transport system than the operating process part, for example in the way laws and regulations are made or how permits are issued. Modelling the control structure for the whole railway transport system is already done in Australia by Read et al. (2019), but not yet in the Netherlands. The systems between Australia and the Netherlands will differ in stakeholders and the connections between those stakeholders.

Practical recommendations

This thesis has not made use of STPA software tools to execute STPA, but it can be recommended to use those tools for a more efficient workflow when multiple STPAs are executed. STPA tools are not required to apply STPA, but nevertheless there are multiple tools available to assist in applying STPA. Those tools can assist with following the STPA steps in a well-arranged way. Assistance is provided in different manners, examples are: software to easily model the control structure, a format to document the STPA steps or visualizing the connections and traceability between the losses, hazards, unsafe control actions, constraints and loss scenarios. Available STPA (and CAST) tools are structured on this website: http://psas.scripts.mit.edu/home/stamp-tools/.

The reliability requirement described by the ERTMS Programme Management states that the operational impact of disruptions in the railway transport system should remain the same or decrease as a result of the addition of ERTMS to the system. One way to (partly) demonstrate this, is by identifying the risks before and after the addition of ERTMS. Some risks will be added, some risks change and some risks are removed due to the addition of ERTMS. A practical example is to apply STPA on the user process about combing trains arriving from opposite direction in the railway transport system without the addition of ERTMS. The identified hazards can be compared with the hazards identified in this thesis. When the hazards are translated in risk, the reliability of both system (with and without ERTMS) affected by this one user process can be indicated. When alle user processes are compared in this way, fulfilment of the reliability requirement can be substantiated a little more. This process would take a lot of time and might not be worth the effort.

STPA is used in this thesis for a reliability analysis, but the method can also be used for safety. The losses that are identified in step 1 of STPA can then be changed from a transportation goal loss to a loss like injury or damage (as described in section 4.2.). This modern hazard analysis technique is appropriate for the complexities in the railway transport system. With STPA, safety is viewed form a different perspective, losses are treated as a control problem, instead of a component failure problem. The safety engineer can especially use STPA as an additional hazard identification method if systems with different controlling actors are analysed. Applying multiple hazard analysis techniques are appropriate in complex systems, because every technique has different strengths and weaknesses and no single technique will capture all the possible hazards.

Recommendations for ERTMS programme management

STPA identified more loss scenarios than FMECA and identifies design flaws in the procedure and unsafe control/feedback interactions, it is therefore recommended to apply STPA also on other user processes for the identification of unknown loss scenarios. The generic control structure (Figure 15) can be used as a base for modelling a control structure for a specific user process. Simple examples of how STPA can be executed are helpful in workshops where loss scenarios are identified with people who are unfamiliar with STPA. Explaining STPA principles and definitions is also advised for involving system experts, to avoid miscommunication. If analysing all the user processes takes too much time, than the user processes which are frequently occurring and have many interactions can be prioritized to analyse.

To implement STPA successfully into the ERTMS programme management and execute the analysis sufficient, a STPA expert who has experience in applying STPA on real projects is highly recommended. This STPA expert can also be someone within ProRail. This expert can answer al the STPA related questions and check if STPA is applied appropriately.

Systems experts of the analysed system can be involved in a STPA by starting with a rough explanation of STPA, with examples and STPA definitions to prevent miscommunication. A training for every employee that is (in)directly involved with risk analysis or risk management is recommended, so those people know the STPA basics and know when and how STPA is suitable to carry out on a project they work on.

It depends on the purpose of the analysis and the analysed system if STPA is suitable to perform. STPA is suitable for identifying hazards in complex systems. A complex system is for example the whole railway transport system (a system of systems) or a not yet developed system. Systems that have multiple controllers and controlled processes are especially suitable to execute STPA on. The analysed system should be a system which can be influenced by the ERTMS programme management. As was said in the practical recommendations, STPA can be used to substantiate the reliability requirement, but also for safety analysis.

Performing STPA can be done with the help of the STPA handbook. This handbook walks you through the steps with examples and lists common errors. STPA handbook:
http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

Bibliography

Abraha, H. H.; Liyanage, J.P. (2015)s. Review of Theories and Accident Causation Models: Understanding of Human-Context Dyad Toward the Use in Modern Complex Systems. Springer International Publishing.

Aven, T. (2017). Improving the foundation and practice of reliability engineering. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability. 231 (3): 295–305. https://doi.org/10.1177%2F1748006X17699478

Bainbridge, L. (1983). Ironies of automation. Analysis, Design and Evaluation of Man–Machine Systems, Pages 129-135. Pergamon. https://doi.org/10.1016/B978-0-08-029348-6.50026-9.

Barnatt, N.; Jack, A. (2018). Safety analysis in a modern railway setting. Safety Science, 110, 177–182. https://doi.org/https://doi.org/10.1016/j.ssci.2018.08.005

Bensaci, C.; Zennir, Y.; Pomorski, D. (2018) A Comparative Study of STPA Hierarchical Structures in Risk Analysis: The case of a Complex Multi-Robot Mobile System. European Conference on Electrical Engineering & Computer Science, EECS 2018. Bern, Switzerland.

Brandenburger, N.; Hörmann, H.J.; Stelling, D.; Naumann, A. (2017). Tasks, skills, and competencies of future high-speed train drivers. Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit 231 (10), 1115–1122.

Britannica (n.d.). Signaling. Retrieved 2 Mei 2022, from https://www.britannica.com/technology/railroad/Signaling.

Bugalia, N.; Maemura, Y.; Ozawa, K. (2020). Organizational and institutional factors affecting high-speed rail safety in Japan. Safety Science, Volume 128, Article 104762. https://doi.org/10.1016/j.ssci.2020.104762.

Buksh, A.; Sharples, S.; Wilson, J.R.; Morrisroe, G.; Ryan, B. (2013). Train automation and control technology - ERTMS from users' perspectives. Anderson, M. (Ed.) Contemporary Ergonomics and Human Factors. Boca Raton: CRC Press.

CBS. (2009). Hoe druk is het nu werkelijk op het Nederlandse spoor. The Hague: Centraal Bureau voor de Statistiek.

CENELEC (1999). EN 50126: Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS). Brussels

Dabekaussen, M. (2017). Assuring safety during the partial implementation of ERTMS in the Netherlands. Weesp: iSquare.

De Bruijn, D. W.; Jhari, R., Van Es, A.; Zeilstra, M. P. (2018). ERTMS veiligheidsanalyses - Nadere beschouwing op 5 incidenttypes. Utrecht: ProRail.

de Carvalho, P.V. (2011). The use of Functional Resonance Analysis Method (FRAM) in a mid-air collision to understand some characteristics of the air traffic management system resilience. Reliability Engineering & System Safety, Volume 96, Issue 11, Pages 1482-1498. https://doi.org/10.1016/j.ress.2011.05.009.

De Vries, M. (2016). ERTMS Driver Machine Interface (DMI) in accordance with SRS 3.6.0.

Dong, A. (2012). Application of CAST and STPA to Railroad Safety in China. Master's thesis. Dalian Maritime University.

EEIG ERTMS Users Group. (1998). ERTMS/ETCS RAMS Requirements Specification: Chapter 2 – RAM. Reference EEIG : 96S126

ERA, European Railway Agency (2008). Glossary of railway terminology.

ERA, European Railway Agency (2016a). System Requirements Specification. UNISIG SUBSET 026-2. Issue: 3.6.0.

ERA, European Railway Agency (2016b). 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. Official Journal of the European Union

ERA, European Railway Agency (2017). ERTMS deployment action plan.

ERA, European Railway Agency (2019). COMMISSION IMPLEMENTING REGULATION (EU) 2019/773 of 16 May 2019 on the technical specification for interoperability relating to the operation and traffic management subsystem of the rail system within the European Union and repealing Decision 2012/757/EU. Official Journal of the European Union

Ericson, C. A. (2005). Hazard analysis techniques for system safety. Fredericksburg, Virginia: John Wiley & Sons.

ERTMS pilot Amsterdam-Utrecht (2015). Eindrapport Lessen uit het rijden onder ERTMS Level 2 in Dual Signalling omstandigheden.

ERTMS (2021). Waar komt ERTMS? Retrieved 1 April 2022, from https://www.ertms.nl/over-ertms/waar/default.aspx.

ERTMS Programme Management (2019a). Dossier Programmabeslissing, S1 Railmap 4.0.

ERTMS Programme Management (2019b Dossier Programmabeslissing, S2 Programmaplan Realisatiefase.

ERTMS Programme Management (2019c). Dossier Programmabeslissing, U2 Programma van Eisen Vervoersysteem ERTMS.

ERTMS Programme Management (2019d). Dossier Programmabeslissing, U3 ERTMS Vervoerssysteemarchitectuur (VSA).

ERTMS Programme Management (2019e). Dossier Programmabeslissing, U1 Scopedocument.

ERTMS Programme Management (2019f). Dossier Programmabeslissing, U2.2 Operationeel kader.

ERTMS Programme Management (2019g). Dossier Programmabeslissing, U2.5 RAM kader.

ERTMS Programme Management (2021a). Kennisdocument Architectuur.

ERTMS Programme Management (2021b). 'SMART' PvE Vervoersysteem met ERTMS V2.2.

ERTMS Programme Management (2022). Operational Concept Description (OCD) van migratiestap 9 t/m 15.

EU (2006). Commission Decision of 7 November 2006 Concerning a Technical Specification for Interoperability Relating to the Control-Command and Signalling Subsystem of the Trans-European High Speed Rail System and Modifying Annex A to Decision 2006/679/EC Concerning the Technical Specification for Interoperability Relating to the Control-Command and Signalling Subsystem of the Trans-European Conventional Rail System (Notified under Document Number C(2006) 5211).

EU (2015). COMMISSION REGULATION (EU) 2015/995 of 8 June 2015 amending Decision 2012/757/EU concerning the technical specification for interoperability relating to the 'operation and traffic management' subsystem of the rail system in the European Union. Official Journal of the European Union.

EU (2019). COMMISSION IMPLEMENTING REGULATION (EU) 2019/773 of 16 May 2019 on the technical specification for interoperability relating to the operation and traffic management subsystem of the rail system within the European Union and repealing Decision 012/757/EU. Official Journal of the European Union.

Europese commissie (2021). Verslag van de commissie aan het Europese parlement en de raad: Zevende monitoringsverslag over de ontwikkeling van de spoorwegmarkt, krachtens artikel 15, lid 4, van Richtlijn 2012/34/EU van het Europees Parlement en de Raad. Brussel: Raad van de Europese Unie

Flammini, F.; Marrone, S.; Iacono, M.; Mazzocca, N.; Vittorini V. (2014). A multiformalism modular approach to ERTMS/ETCS failure modelling. International Journal of Reliability, Quality and Safety Engineering, Vol. 21, No. 1, Article 1450001. https://doi.org/10.1142/S0218539314500016

Flammini, F.; Vittorini V. (2006). Modelling structural reliability aspects of ERTMS/ETCS by Fault Trees and Bayesian Networks. Guedes Soares & Zio (Eds.) Safety and Reliability for Managing Risks, Taylor & Francis Group.

Fleming, C.H.; Spencer, M.; Thomas, J.; Leveson, N.; Wilkinson, C. (2013). Safety assurance in NextGen and complex transportation systems. Safety Science, 55, 173–187.

Goverde, R. M. P. (2012). Robuust spoor met ERTMS. Colloquium Vervoersplanologisch Speurwerk: Amsterdam.

Goverde, R. M. P. (2022, February 8). Lecture slides MSc Course CIE5826 Railway operations and control, Brief history of railway signalling. Delft.

Hall-May, M.; Kelly, T. (2005). Defining and Decomposing Safety Policy for Systems of Systems. Computer Safety, Reliability, and Security 3688 (pp. 37–51). Berlin: Springer.

Hale, A. R.; M. Hale (1970). Accidents in perspective, in: Occupational psychology (44): pp. 115–122.

Hamilton, W.; Colford, N., (2003). Developing a baseline operational specification of driver requirements for UK ERTMS. In: Proceedings of the XVth Triennial Congress of the International Eronomics Association. Seoul, Korea, August 24-29, 2003.

Heinrich, W. H. (1931). Industrial Accident Prevention: A Scientific Approach. Mc GrawHill Book Company: New York and London.

Hinzen, A. (1993). The Impact of Human Error on Railway Safety, RWTH Aachen, Aachen.

Hollnagel, E. (1992). The reliability of man-machine interaction. Reliability Engineering & System Safety, Volume 38, Issues 1–2, Pages 81-89. https://doi.org/10.1016/0951-8320(92)90108-W

Hollnagel, E. (2004). Barriers and Accident Prevention. Aldershot: Ashgate Publishing Limited.

Hulme, A.; Stanton, N. A.; Walker, G. H.; Waterson, P.; Salmon, P. M. (2019). What do applications of systems thinking accident analysis methods tell us about accident causation? A systematic review of applications between 1990 and 2018. Safety Science, Volume 117, Pages 164-183. https://doi.org/10.1016/j.ssci.2019.04.016

IRSE (1996). The influence of human factors on the performance of railway systems. The Technical Committee Report No. 3.

Kawakami, S. (2014). Application of a Systems-Theoretic Approach to Risk Analysis of High-speed Rail Project Management in the US. Massachusetts Institute of Technology.

Kiran, D. R. (2017). Chapter 26 - Failure Modes and Effects Analysis. Total Quality Management, Butterworth-Heinemann, Pages 373-389. https://doi.org/10.1016/B978-0-12-811035-5.00026-X.

Kirwan, B. (1994). A guide to practical human reliability assessment, Taylor&Francis, London.

Klein, S. (2006). Time: The stuff of life. An instruction manual, Fischer S. Verlag, Frankfurt am Main.

Kleiner, B. M. (2006). Macroergonomics: Analysis and design of work systems. Applied Ergonomics, 37(1), 81–89.

Kuiken, A. (2012). Eindrapport Parlementair onderzoek Onderhoud en innovatie spoor. The Hague: Ministerie Infrastructuur en Milieu.

Leveson, N.G. (2004) A New Accident Model for Engineering Safer Systems. Safety Science, Vol. 42, 237-270.

Leveson, N.G. (2012) Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press. https://doi.org/10.7551/mitpress/8179.001.0001

Leveson, N.G. (2015). A systems approach to risk management through leading safety indicators. Reliability Engineering and System Safety, 136. https://doi.org/10.1016/j.ress.2014.10.008

Leveson, N.G. (2021). Introduction to STAMP [PowerPoint slides]. Retrieved 26 May 2022, from https://www.youtube.com/watch?v=_ptmjAbacMk

Leveson, N.G.; Thomas, J.P. (2018) STPA Handbook. MIT Press.

Li, C.; Tang, T.; Chatzimichailidou, M.; Jun, G.; Waterson, P. (2019). A hybrid human and organisational analysis method for railway accidents based on STAMP-HFACS and human information processing. Applied Ergonomics, Volume 79, Pages 122-142. https://doi.org/10.1016/j.apergo.2018.12.011.

Li, M.; Yan, F.; Niu, R.; Xiang, N. (2021). Identification of causal scenarios and application of leading indicators in the interconnection mode of urban rail transit based on STPA. Journal of Rail Transport Planning & Management, Volume 17, Article 100238. https://doi.org/10.1016/j.jrtpm.2021.100238.

Mansveld, W. (2014). Voorkeursbeslissing ERTMS en Railmap 3.0/Nota Alternatieven. The Hague: Ministerie Infrastructuur en Milieu.

Martinez, R.S. (2015). System Theoretic Process Analysis of Electric Power Steering for Automotive Applications. MIT Master's Thesis

Meyer, T.; Reniers, G. (2016). Engineering Risk Management (2nd ed.). Berlin: Walter de Gruyter.

Ministry of infrastructure and water management (2021). 16e voortgangsrapportage van het Programma ERTMS, Verslagperiode: 1 juli 2021 – 31 december 2021

Møller, J. H.; Gammon, R.; van Schijndel, B. (2019). Delivering change in Denmark: operational readiness of successful ERTMS programmes. IRSE News, Institution of Railway Signal Engineers, Issue 261, Pages 2-12.

Montuori, A. (2011). Systems Approach. Encyclopedia of Creativity (Second Edition), Academic Press, Pages 414-421. https://doi.org/10.1016/B978-0-12-375038-9.00212-0.

Muttram, R. (2018). How do we reduce the number of accidents involving human factors? IRSE News, Institution of Railway Signal Engineers, Issue 242, Pages 1-6.

Naghiyev, A.; Sharples, S.; Carey, M.; Coplestone, A.; Ryan, B. (2014). ERTMS train driving incab vs. outside: an explorative eye-tracking field study. In S. Sharples & S.T. Shorrock (Eds.), Contemporary Ergonomics and Human Factors 2014. Proceedings of the international conference on Ergonomics & Human Factors 2014 (pp 343-350). London: Taylor & Francis.

NS (2019). NS annual report. Retrieved 1 April 2022, from https://www.nsannualreport.nl/FbContent.ashx/pub_1001/downloads/v200416100644/NS_annualreport_2019.pdf

Onderzoeksraad voor de Veiligheid (2005). Door rood op Amsterdam CS. Den Haag: Onderzoeksraad voor de Veiligheid.

Ouyang, M.; Hong, L.; Yu, M.; Fei, Q. (2010). STAMP-based analysis on the railway accident and accident spreading: taking the China-Jiaoji railway accident for example. Saf. Sci. 48 (5), 544–555.

Patriarca, R.; Chatzimichailidou, M.; Karanikas, N.; Di Gravio, D. (2022). The past and present of System-Theoretic Accident Model And Processes (STAMP) and its associated techniques: A scoping review. Safety Science, Volume 146, Article 105566. https://doi.org/10.1016/j.ssci.2021.105566.

Pawlicki, T.; Samost, A.; Brown, D.W.; Manger, R.P; Kim, G.; Leveson, N.G. (2016). Application of systems and control theory-based hazard analysis to radiation oncology. Medical Physics, Volume 43, Issue 3, p. 1514-1530. https://doi.org/10.1118/1.4942384.

Porter, D. (2011). Implementing ERTMS in the UK: Human Factors Implications for Train Drivers [PowerPoint slides]. Retrieved 27 July 2022, from https://slideplayer.com/slide/4755067/.

Posner, M.I. (1980). Orienting of attention. Quarterly Journal of Experimental Psychology, 32, 3-25.

ProRail (2019). Ontwerpvoorschrift ATB Nieuwe Generatie (ATB-NG) Baanapparatuur. OVS60520-1

ProRail (2020). Meer en snellere treinen. Retrieved 2 March 2022, from https://www.prorail.nl/nieuws/meer-en-snellere-treinen

ProRail (2021). Richtlijn gebruikersprocessen ERTMS level 2. v2.0_20220120. Report number: RLN60560-5

ProRail (2022a). Prestaties gericht op het laten rijden van reizigerstreinen. Retrieved 10 May 2022 from https://prestaties.prorail.nl/reizigersvervoer/cDU174_Reizigersvervoer.aspx

ProRail (2022b). D0270 Veiligheidsanalyse instellen van een TSB (PvE v004) v13.0.

ProRail (2022c). Gebruikersprocessen ERTMS level 2. Version: 2.0

Qureshi, Z. H. (2007). A Review of Accident Modelling Approaches for Complex Sociotechnical Systems. In Proceedings of the Twelfth Australian Workshop on Safety Critical Systems and Software and Safety-related Programmable Systems - Volume 86 (pp. 47–59). Darlinghurst, Australia: Australian Computer Society, Inc.

Rasmussen, J. (1983). Skills, Rules and Knowledge; Signals, Signs and Symbols, and other distinctions in human performance models, in: IEEE transactions on systems, man, and cybernetics SMC-13(3): pp. 257-266.

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. Safety Science, Volume 27, Issues 2–3, Pages 183-213. https://doi.org/10.1016/S0925-7535(97)00052-0.

Rausand, M.; Barros, A.; Hoyland, A. (2004). System Reliability Theory. New Jersey: John Wiley & Sons.

Read, G.J.M.; Naweed, A.; Salmon, P.M. (2019). Complexity on the rails: a systems-based approach to understanding safety management in rail transport. Reliab. Eng. Syst. Saf. 188, 352–365.

Reason, J. (1990). Human Error. Cambridge University Press: Cambridge

Redmill, F. (2002). Risk analysis-a subjective process. Engineering Management Journal, 12(2), 91–96.

Rosberg, T.; Cavalcanti, T.; Thorslund, B.; Prytz, E.; Moertl, P. (2021). Driveability analysis of the european rail transport management system (ERTMS) - A systematic literature review. Journal of Rail Transport Planning & Management, Volume 18, Article 100240.

Sallak, M.; Schön, W.; Destercke, S.; Berdjag, D.; van der haegen, F.; Simon, C. (2015). Uncertainty, elicitation of experts' opinion, and human failures: Challenges for RAM analysis of ERTMS. International Conference on System of Systems Engineering, SoSE, pp. 88–93. https://doi.org/10.1109/SYSOSE.2015.7151917.

Sharma, R. K.; Kumar, D.; Kumar, P. (2005). Systematic failure mode effect analysis (FMEA) using fuzzy linguistic modelling. International Journal of Quality & Reliability Management, 22(9), 986- 1004. https://doi.org/10.1108/02656710510625248

Smith, P.; Majumdar, A.; Ochieng W. A. (2012). An overview of lessons learnt from ERTMS implementation in European railways. Journal of Rail Transport Planning & Management. Volume 2, Issue 4, 79-87. https://doi.org/10.1016/j.jrtpm.2013.10.004.

Spoor pro. (2022). Data-uitwisseling wal en trein verbeterd voor routesysteem machinisten. Retrieved 2 August 2022, from https://www.spoorpro.nl/spoorbouw/2022/03/30/data-uitwisseling-wal-en-trein-verbeterd-voor-routesysteem-machinisten/

Sulaman, S.; Beer, A.; Felderer, M.; Host, A. (2019). Comparison of the FMEA and STPA safety analysis methods–a case study. Software Qual J 27, 349–387. https://doi.org/10.1007/s11219-017-9396-0

Tessédre, D.; UIC, International Union of Railways (2004). Safe Culture, A Method for Assessing Organisational Safety at Interfaces. UIC/Communications Department, Edition: JC Dan Partners.

Theeg, G.; Vlasenko, S. (2009). Railway Signalling & Interlocking. Hamburg: Eurailpress.

Thomas, J. (2020). Use of STPA in Practice: Lessons Learned. [PowerPoint slides]. Retrieved 25 July 2022, from http://psas.scripts.mit.edu/home/wp-content/uploads/2020/07/JThomas-Lessons-Learned-in-STPA.pdf

Thomas, J. (2021). Introduction to STPA. [PowerPoint slides]. Retrieved 25 May 2022, from https://www.youtube.com/watch?app=desktop&v=2W-iqnPbhyc

Tweede kamer (2019). Spoorbeveiligingssysteem European Rail Traffic Management System (ERTMS). Tweede Kamer der Staten Generaal, 33652, nr. 65, The Hague.

UIC, International Union of Railways (2004). UIC Code 406: Capacity. UIC, Parijs, 1 september 2004.

UIC, International Union of Railways (2015). What is ERTMS? Retrieved 2 February 2022, from https://uic.org/rail-system/ertms/

Underwood, P.; Waterson,P. (2013). Systemic accident analysis: Examining the gap between research and practice. Accident Analysis & Prevention, Volume 55, Pages 154-164. https://doi.org/10.1016/j.aap.2013.02.041.

Underwood, P., & Waterson, P. (2014). Systems thinking, the Swiss Cheese Model and accident analysis: A comparative systemic analysis of the Grayrigg train derailment using the ATSB, AcciMap and STAMP models. Accident Analysis & Prevention, 68, 75–94. https://doi.org/10.1016/j.aap.2013.07.027

Unife (2021a). factsheet #28, ERTMS advantages.

Unife (2021b). factsheet #3, ERTMS levels.

Unife (2022). Deployment world map. Retrieved 1 February 2022, from https://www.ertms.net/deployment-world-map/#

van den Top, J. (2007). Veilig regelen van railverkeer, huidige invulling van d functies. Op de rails 4 – 2007.

van den Top, J. (2009). Railverkeer veilig én economisch regelen. Op de rails 1 – 2009.

van den Top, J. (2010). Modelling Risk Control Measures in Railways. Analysing how designers and operators organise safe rail traffic. PhD thesis. Delft: TU Delft.

Van der Schaaf, T. W.; Wright, L. B. (2005). The development of PRISMA-Rail: a generic root cause analysis approach for the railway industry. Wilson, J. R.; Norris, B. Clarke, T.; Mills, A. (Eds.) Rail Human Factor: Supporting the Integrated Railway. London: Taylor & Francis. https://doi.org/10.4324/9781315089201-37

Van der Weide, R.; De Bruijn, D.W.; Zeilstra, M.P. (2017). ERTMS pilot in The Netherlands – impact on the train driver. Paper submitted for Sixth International Human Factors Rail Conference, London, 6-9 November 2017.

van der Weide, R.; van der Vlies, V.; van der Meer F. (2022). Train driver experience: A big data analysis of learning and retaining the new ERTMS system. Applied Ergonomics, Volume 99, Article 103627. https://doi.org/10.1016/j.apergo.2021.103627

van der Weide, R. (2017). ERTMS roll out from a train driver's perspective. Golightly, D., et al. (Eds.), Sixth International Human Factors Rail Conference 6-9, pp. 612–621. London.

van Es, A. (2017). Feasibility study reference system ERTMS. Arcadis, Amersfoort.

Van Vliet, J. (2018). Human Factors RAM ERTMS Machinisten en Treindienstleiders. Report number: 203.006. Utrecht: Programma Management ERTMS.

Vromans, M. (2005). Reliability of Railway Systems. PhD thesis. Rotterdam: Erasmus University Rotterdam

Wang, j. (2018). Chapter 11 - Safety Analysis Methods for Train Control Systems. Safety Theory and Control Technology of High-Speed Train Operation, Academic Press, Pages 309-354. https://doi.org/10.1016/B978-0-12-813304-0.00011-6.

Weinberg, G. M. (1975). An introduction to general systems thinking. New York: Wiley

Wickens, C. D. (1984). Processing resources in attention. In R. Parasuraman and D.R. Davies (eds). Varieties of attention, London: Academic Press, pp. 63-102.

Wickens, C. D.; Hollands, J. G.; Banbury, S.; Parasuraman, R. (2016). Engineering psychology and human performance. 4th ed. London, New York: Routledge.

Wilde, G.J.S. (2014). Target Risk 3 – Risk Homeostatis in Everyday Life. Toronto: PDE Publications – Digital Edition.

Wohlin, C., 2014. Guidelines for snowballing in systematic literature studies and a replication in software engineering. ACM International Conference Proceeding Series. https://doi.org/10.1145/2601248.2601268

Young, M.S.; Stanton, N.A.; Walker, G.H. (2006). In loco intellegentia: human factors for the future European train driver. Int. J. Indust. Syst. Eng., 1 (4).

Zeilstra, M.P.; van der Weide, R. (2016). ERTMS in Holland: overview of human factors issues in a pilot with dual signalling. In: Milius, Birgit, Naumann, Anja (Eds.), Rail Human Factors Proceedings of the 2nd German Workshop on Rail Human Factors March, 8th and 9th, 2016 Stadthalle Braunschweig, pp. 88–95.

Zhang, Y.; Dong, C.; Guo, W.; Dai, J.; Zhao, Z. (2022). Systems theoretic accident model and process (STAMP): A literature review. Safety Science, Volume 152, Article 105596. https://doi.org/10.1016/j.ssci.2021.105596.

Zhang, Y.; Shao, W.; Zhang, M.; Li, H.; Yin, S.; Xu, Y. (2016). Analysis 320 coal mine accidents using structural equation modeling with unsafe conditions of the rules and regulations as exogenous variables. Accid. Anal. Prev. 92, 189–201.

Appendix A.

Systems Theoretic Accident Model and Processes (STAMP)

STAMP is a new type of accident (causality) modelling. Accident models simplify the reality by abstraction and is used to analyse and prevent accidents (Leveson, 2004). Models help to understand how a complex system works and filter out irrelevant information. The STAMP model is a hierarchical safety control structure. The control structure models the interactions between system components and the interactions between the system components interact through feedback control loops. The control structure consists of controllers that control the process, sensors that sense feedback and actuators that implement control actions (Leveson, 2012). A basic control structure is illustrated in Figure 17.

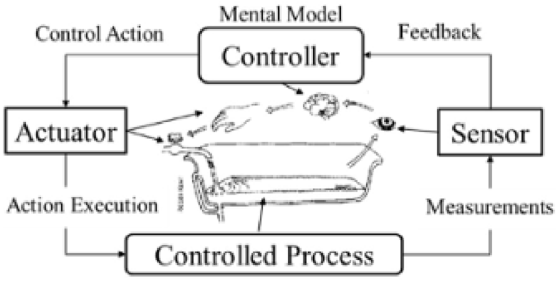


Figure 17: Basic control structure (Bugalia et al., 2020).

This appendix explains how STAMP is an alternative accident model, compared to the traditional accident models and how STAMP makes use of system theory for its accident modelling.

Traditional accident models

The nature of accidents have changed and so the accident models have changed (Zhang et al., 2016). Traditional accident models are based on a linear chain of failure events (COE) model. It assumes that an accident can be understood with a linear causality model. In COE, one event is the root cause of a loss event and contributory causes are in an event chain. Those models work for simple systems and failures of physical components. But times have changed, as seen in the examples of change that influenced into more complex systems: Faster past of technological change, accidents caused by software, higher impacting hazards (for future generations and environment), more complex human-machine interactions and a shift of safety responsibility from individuals to governments (Leveson, 2004).

COE is typically represented with the domino model (Heinrich, 1931) and the Swiss cheese model (Reason, 1990). Those illustrate the chain of event that lead to an accident and contribute to the understanding of what leads to an accident and how to prevent it.

The domino model is illustrated in Figure 18. Heinrich demonstrates with the model that accidents can be prevented by removing one of the contributing events. Without the unsafe act, no accident will occur, without human error, no unsafe act occurs. The domino model often implicitly gives someone the blame for an accident, because a fault of a person is often the root cause, even if the person is influenced by the environment.

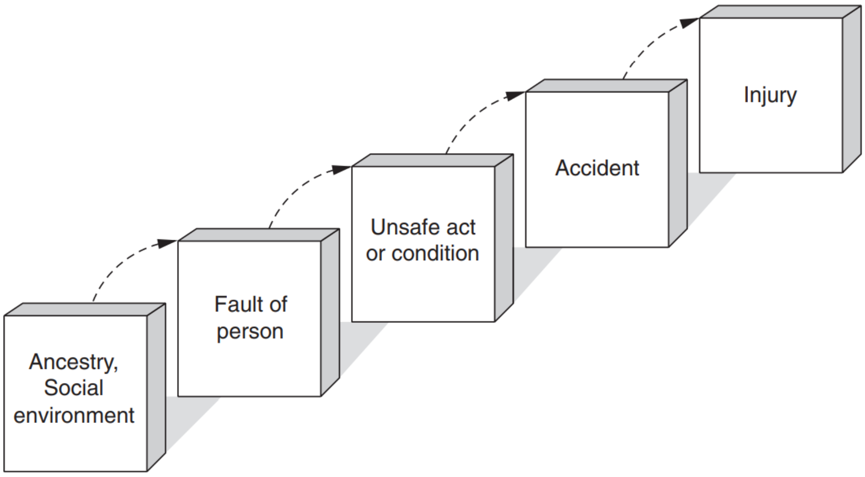


Figure 18: Domino accident model (Heinrich, 1931).

The Swiss cheese model from Reason is illustrated in Figure 19. The model includes barriers/defences for an accident to happen that look like slices of cheese. Each barrier have flaws/limitations where a system is vulnerable under certain conditions. More barriers/defences added or patching the holes in the slices could prevent accidents. However this model excludes the dependence between the defences, all the defences could be affected simultaneously by the same change.

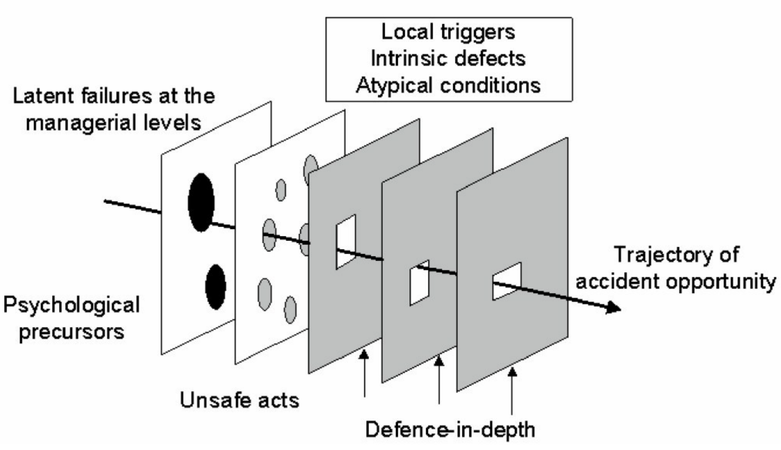


Figure 19: Swiss cheese model (Reason, 1990).

The domino model and swiss cheese model treat humans as a single component in a system. The reliability of the human behaviour is then estimated. Leveson (2012) treats the human error not as an source of accidents, but as an symptom of it. Leveson argues that human error is not random and can therefore not be measured as a mechanical component of a system.

The linear chain of failure models have more drawbacks, like choosing a factor as the root cause of an accident and therefor ignoring other potential factors. Those linear models are great for simple systems, but not for the increasingly complex systems (Leveson 2012).

STAMP challenges the 'old' assumptions made for the chain of events model, so Leveson made new/adapted assumptions for today's more complex sociotechnical systems (Leveson 2012). Table 10 displays the old and the new assumptions. The new assumptions are not applicable for the chain of events model, but is applicable for STAMP.

Old Assumption	New Assumption
Safety is increased by increasing system or component reliability; if components do not fail, then accidents will not occur.	High reliability is neither necessary nor sufficient for safety.
Accidents are caused by chains of directly related events. We can understand accidents and assess risk by looking at the chains of events leading to the loss.	Accidents are complex processes involving the entire sociotechnical system. Traditional event-chain models cannot describe this process adequately.
Probabilistic risk analysis based on event chains is the best way to assess and communicate safety and risk information.	Risk and safety may be best understood and communicated in ways other than probabilistic risk analysis.
Most accidents are caused by operator error. Rewarding safe behaviour and punishing unsafe behaviour will eliminate or reduce accidents significantly.	Operator error is a product of the environment in which it occurs. To reduce operator " error " we must change the environment in which the operator works.
Highly reliable software is safe.	Highly reliable software is not necessarily safe. Increasing software reliability will have only minimal impact on safety.
Major accidents occur from the chance simultaneous occurrence of random events.	Systems will tend to migrate toward states of higher risk. Such migration is predictable and can be prevented by appropriate system design or detected during operations using leading indicators of increasing risk.
Assigning blame is necessary to learn from and prevent accidents or incidents.	Blame is the enemy of safety. Focus should be on understanding how the system behaviour as a whole contributed to the loss and not on who or what to blame for it.

Table 12: New assumptions that are the foundation for STAMP (Leveson, 2012).

System theory

Many traditional risk analysis techniques, like Fault Tree Analysis, Event Tree Analysis, HAZOP and FMECA are based on chain of events models. STAMP is not based on chain of events model, but on system theory, where risks arise from system components interactions, besides the components itself. Systems can be described as a group of elements that are interacting and are interdependent, but form a complex whole. Examples of those elements are assets, humans or information. In system theory a system can be affected by its environment, this is called an open system. Open systems receive inputs from the environment and sends outputs to the environment. Feedback loops are also considered in the system, those loops provide information from the outputs and transfers it to the inputs (Montuori, 2011). An example of system theory can be seen in a thermostat on the heating, where the thermostat controls, measures and adjusts the heat, related to the desired value.

System theories treat a system as a whole and not as a cumulation of the different system components, because the whole system is more than the sum of components. Key concerns in system theory are the emergent properties of a system, examples of those properties are reliability or safety. Those properties emerge from the complex interactions between individual system components and from individual component behaviour (Weinberg, 1975). The emergent properties are required to be controlled and is illustrated in the model of Figure 20.

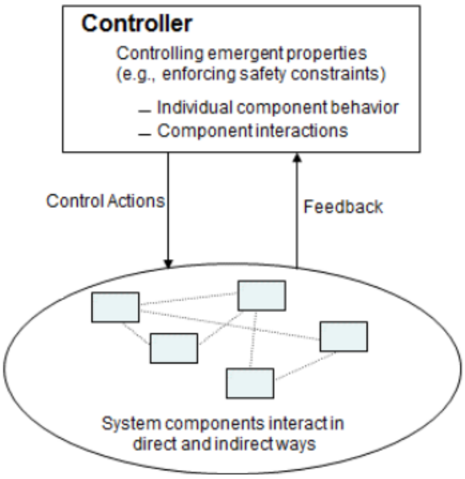

Controller
Controlling emergent properties
(e.g., enforcing safety constraints)
– Individual component behavior
– Component interactions
Control Actions
Feedback
System components interact in
direct and indirect ways

Figure 20: Feedback control loop model (Leveson & Thomas, 2018).

A few more characteristics of STAMP

System accident models, like STAMP can describe non-linear risk behaviours in complex systems (Abraha and Liyanage, 2015).

STAMP Defines accidents/losses as a dynamic control problems and not as a component failure. It can be applied to very complex systems and it includes: scenarios from traditional accident models, software and design errors, human errors, component interaction accidents and the social side of socio-technical systems (Leveson, 2012). STAMP does not imply that previous accident models are wrong, but STAMP offers a new and broader model which is more powerful than the chain of events.

STAMP has a new view on human error and failing software. Human error is seen as a symptom of a system that needs to be redesigned. Software cannot fail, because it is pure design, so it must be seen as a design error (Leveson, 2012). Accidents are caused by insufficient control, STAMP identifies the control and feedback loops that can cause accidents (Leveson, 2012).

More information about the need for STAMP and its characteristics can be found in de book written by Leveson (2012): 'Engineering a Safer World: Systems Thinking Applied to Safety'.

Appendix B.

Overview of the 4 STPA steps

STPA is done in 4 steps, section 4.1 briefly explained the steps, this appendix elaborates more into detail. The information in this appendix is a summary of STPA handbook chapter 2, made by Leveson and Thomas (2018) and a STPA introduction prestation presented by Thomas (2021). For more examples and more detailed explanation, those sources are highly recommended.

1) Define purpose of the analysis

The first step is to define the purpose of the analysis, as shown in Figure 21. This step includes four steps: 1. Identify losses 2. Identify system-level hazards 3. Identify system-level constraints 4. refine hazards (optional).

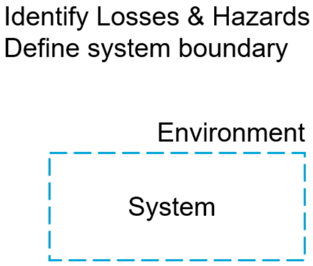


Figure 21: Step 1: Defining the purpose of the analysis (Leveson & Thomas, 2018).

1. Identify losses

Losses involve something of value to stakeholders and can vary from human injury to loss of reputation, so it is something that is unacceptable to the stakeholders. STPA targets those losses and the goal of STPA is to prevent losses.

Identifying losses can be done with a general approach:
1. Identify the stakeholders (e.g. train users, train drivers and railway undertakings)
2. Identify the stakeholders goals and what they value (e.g. useable train, provide transportation on time)
3. Translate the values or goals into losses (e.g. loss of transportation goal, loss of life/health/train/customer satisfaction)

2. Identify system-level hazards

A hazard is a system state or set of condition that has the potential to lead to a loss. A system-level hazard can be identified by first identifying what is included in the system and what the boundaries are. It is useful to include the parts of the system that can be controlled by a responsible stakeholder (like the ERTMS Programme Management). Some level of control over the system is necessary to eliminate/mitigate effects of hazards.

Example of system-level hazards are: train does not maintain safe distance from other trains, train enters dangerous area/region, train exceeds safe operating in environment (longitudinal/lateral forces, speed).

Each hazard can lead to one or more losses. A system-level hazard is defined with three criteria: a hazard is a system state or condition (not an environmental state or component-level cause), a hazard will lead to a loss in some worst case environment, a hazard must describe a state or condition to be prevented.

Hazards should not be confused with the cause of hazards. This can be countered by referring to the overall system and not to system components. A hazard should contain:
<Hazard specification (e.g. H-1, H-2 or H-3)> = <System (e.g. railway transport system)> & <Unsafe condition> & <Link to Losses (e.g. L-1, L-2 and/or L-3>

When hazards are defined, not to many should be defined, a maximum of 7 is preferable, otherwise hazards should be combined into more abstract hazards. Avoid ambiguous or recursive wording and do not confuse hazards with failures (e.g. train are too close to each other, instead of an unsafe train).

3. Identify system-level constraints

System-level constraints are constraints that specify system behaviours or conditions that prevent hazards (and losses). Generally written:
<System-level hazard specification> = <System> & <Unsafe condition> & <Link to Losses>
e.g. H-1 = ‘Train’ ‘violate minimum separation standards’ ‘[L-1, L-3]’
<System-level constraint> = <System> & <Condition to enforce> & <Link to Hazards>
e.g. SC-1 = ‘Train’ ‘must satisfy minimum separation standards from other trains’ ‘[H-1]’
A constrain can also define how losses in a system must be minimized. Generally written:
<System-level constraint specification> = if <Hazard>, then <what needs to be done to prevent or minimize a loss> & <Link to Hazards>

4. Refine hazards (optional)

The hazards and consequently the constraints can be refined by identifying sub-hazards. Those sub-hazards can be found by first identifying what need to be controlled to prevent a hazard. And then determine what hazards could occur by inadequately control. This step is optional and could be helpful in big complex systems.

2) Model the control structure

Step 2 is to model the control structure, as seen in Figure 22.

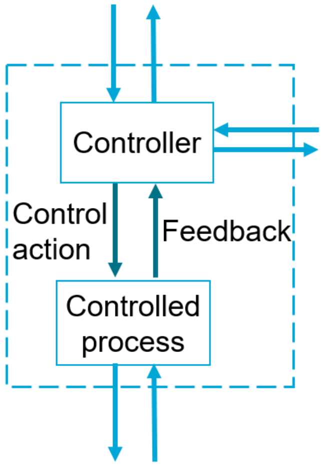


Figure 22: Step 2: Model the control structure (Leveson & Thomas, 2018).

A control structure is composed of feedback control loops and enforces constraints on the behaviour of the overall system. The control model consisted at least of a controlled process that is controlled by a controller. This controller gets feedback from the controlled process, on which the controller can perform a control action on the process. Lastly, other inputs to and outputs from components can be added (those are neither control nor feedback and those arrows are positioned horizontal).

The downward arrows on the vertical axis indicates control and authority in the system. High-level controllers are at the top of the control structure, the lowest-level controllers at the bottom. A controller has control and authority over the entity below it. So, all arrows pointed downwards are control actions and all upward arrows are feedback.

The control structure is a functional model, not an physical model (like a block/schematic diagram) nor executable/simulation model (the control structure may include humans, that are not present in executable models). In the control structure, obedience should not be assumed to the control actions, neither should be assumed that feedback is actually provided (correct) in practice.

The modelling of control structures should begin with an abstract model and iteratively add more detail, but the control actions and feedback arrows should be labelled with detailed functional information at all times. Understanding how a system-level constraint can be enforced might be helpful to identify which control structure entities are in the control structure. To identify the different types of control actions and feedback, it can be helpful to describe the different responsibilities of control structure entities.

A control structure does not require a full linear hierarchy, multiple controllers can be located at the same vertical level, information exchange between those controllers are then represented with horizontal arrows.

Appendix C illustrates different examples of control structures.

3) Identify unsafe control actions

After a control structure is modelled, the unsafe control actions are identified in step 3, this is illustrated in Figure 23.

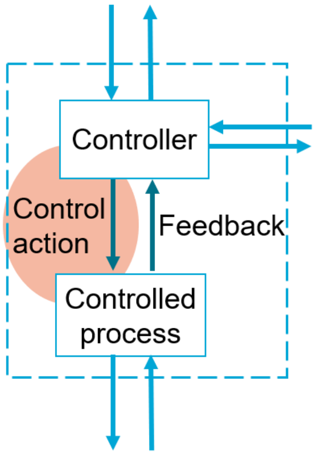


Figure 23: Step 3: Identify unsafe control actions (Leveson & Thomas, 2018).

An unsafe control action (UCA) refers to a control action that will lead to a hazard in a worst-case environment and particular context. There are four ways/types in which a control action can be unsafe:
1. Not providing the control action leads to a hazard.
2. Providing the control action leads to a hazard.
3. Providing a potentially safe control action but too early, too late, or in the wrong order
4. The control action lasts too long or is stopped too soon (for continuous control actions, not discrete ones).

Every UCAs results in one or more hazards. And every UCA should refer to relevant context which made the control action unsafe, word like 'while', 'when' or 'during' are helpful to develop the context. The context must be defined clearly and be the actual state or condition (not a belief or process model).

An UCA can generally be written as:
<UCA specification> = <Source> & <Type> & <Control Action> & <Context> & <Link to Hazards>
e.g. UCA-1 = 'Automatic train protection system' 'not providing' 'a brake command' 'while coming track section is occupied.' '[H-1]'

STPA is an worst case analysis method, so UCAs should still be identified if there are safeguards in place for a particular UCA.

An UCA can be inverted, so a controller constraint is defined. A controller constraint is the behaviour of a controller specified, so it prevents a UCA.

4) Identify loss scenarios

With the identification of unsafe control actions, the last step of STPA starts. Step four is to identify loss scenarios, as illustrated in Figure 24.

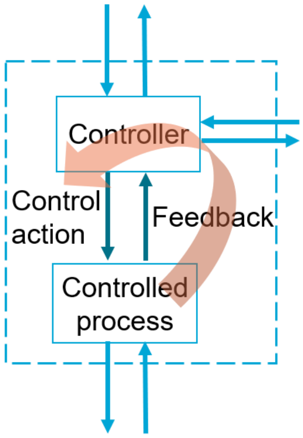


Figure 24: Step 4: Identify loss scenarios (Leveson & Thomas, 2018).

A loss scenario describes how causal factors lead to hazard and unsafe control actions. There are two types of loss scenarios that are answered by two questions:
1. Why would the Unsafe Control Actions occur? (Figure 25)
2. Why would the control actions be improperly executed or not executed, leading to hazards? (Figure 26)

In the example Figure 25, sensors and actuators are included, this refinement of the control structure is done to identify specific scenarios that cause unsafe control and feedback.

1. Identifying scenarios that lead to unsafe control actions. (Why would Unsafe Control Actions occur?)

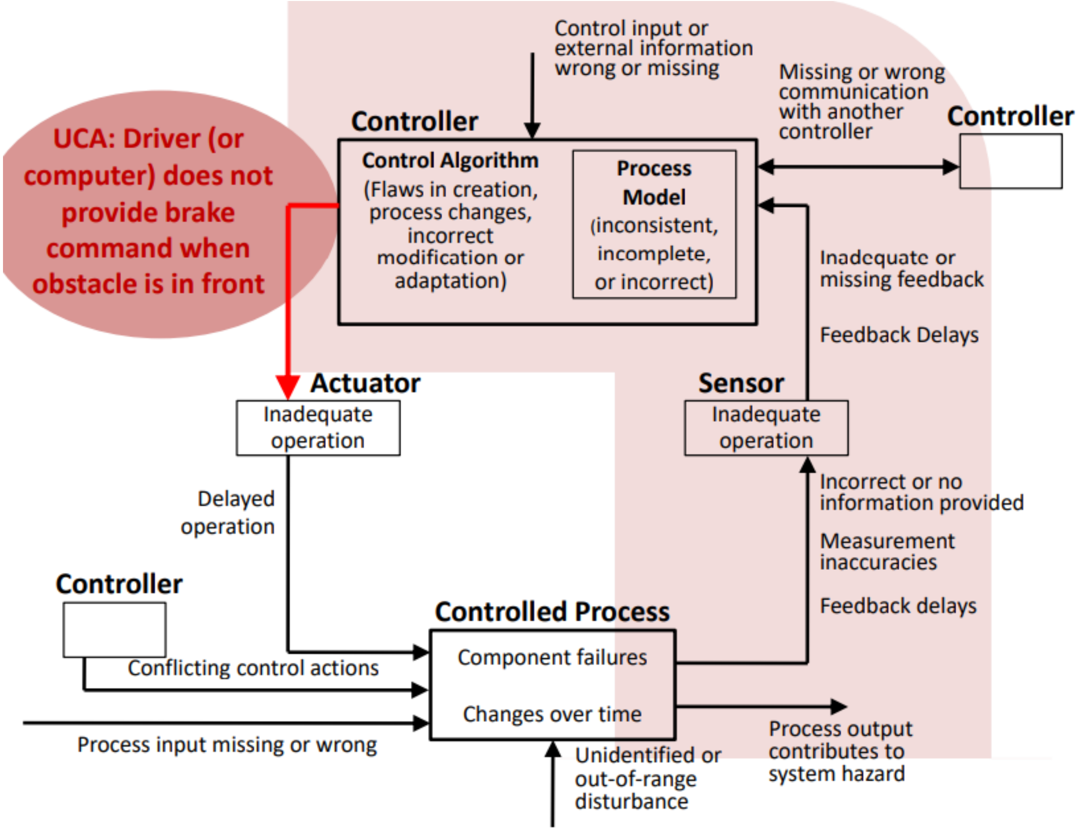

UCA: Driver (or computer) does not provide brake command when obstacle is in front
Control input or external information wrong or missing
Missing or wrong communication with another controller
Controller
Controller
Control Algorithm (Flaws in creation, process changes, incorrect modification or adaptation)
Process Model (inconsistent, incomplete, or incorrect)
Inadequate or missing feedback
Feedback Delays
Actuator
Inadequate operation
Sensor
Inadequate operation
Delayed operation
Incorrect or no information provided
Measurement inaccuracies
Feedback delays
Controller
Controlled Process
Component failures
Changes over time
Conflicting control actions
Process input missing or wrong
Unidentified or out-of-range disturbance
Process output contributes to system hazard

Figure 25: example of what could cause unsafe control actions (Thomas, 2021).

This first scenario type identifies scenarios by starting at the UCA and work backward in the control loop to explain how the controller could cause the UCA. The UCAs can be caused by:
1.1. Controller behaviour that is unsafe (the upper part of Figure 25)
1.2. Feedback and other inputs that are inadequate. (the right part of Figure 25).

General examples of controller behaviour that is unsafe:

- Controller failures
  - If the controller is physical.
- Control algorithms that are inadequate
  - A control algorithm selects the control action, based on previous input/output and the controllers process model. For human controllers is the selections of control actions based on different factors, like past experience, training and procedures.
- Wrong or missing control input
  - For instance from other controllers.
- Process models that are inadequate
  - Process models are representing the beliefs of the controller that are used by the control algorithm. A process model is inadequate if the reality does not match with the believes, this may occur due to: incorrect feedback/info received, interpretation of feedback/info is incorrect/ignored, feedback/info is not/delayed received or the necessary feedback/info does not exist.

Those scenarios can be generally written down as:
<Scenario identification> = <UCA> & <the controlled process models (beliefs) that could cause the UCA> & <Identification of how the process model might occur due to (not) received feedback/info>

General examples of feedback and other inputs that are inadequate:

- Feedback/info not received
    - Info sent by sensor, but controller did not receive it.
    - Info is received/applied to a sensor, but not sent by the sensor.
    - Info is not received/applied to a sensor.
    - Info does not exist or sensor does not exist.
- Inadequate feedback received
    - The sensor responds adequately, but the info is inadequate received by controller.
    - The sensor responds inadequately to info.
    - The sensor is not designed/capable to provide necessary info.

Those scenarios can be generally written down as:
<Scenario identification> = <UCA> & <True state from UCA context> & <information received> & <how the information received could happen, given the true state>

2. Identifying scenarios in which control actions are improperly executed or not executed. (Why would control actions be improperly executed or not executed, leading to hazards?)

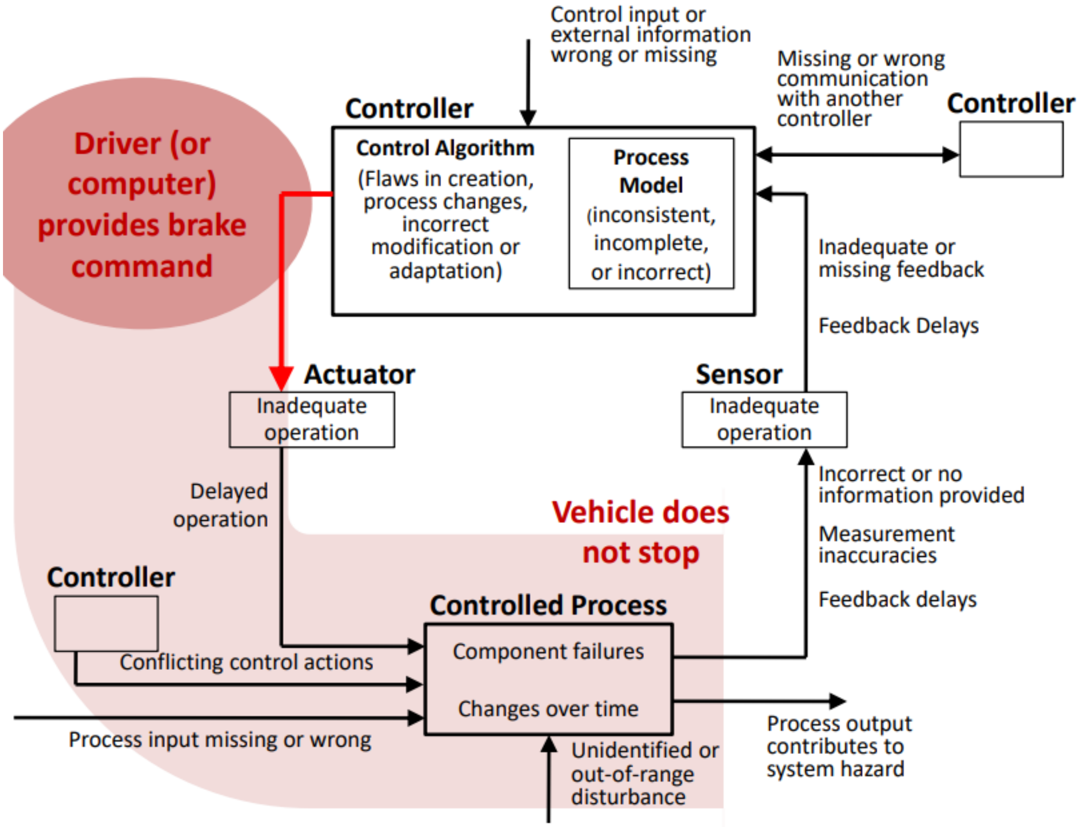

Control input or external information wrong or missing
Missing or wrong communication with another controller
Controller
Controller
Driver (or computer) provides brake command
Control Algorithm
(Flaws in creation, process changes, incorrect modification or adaptation)
Process Model
(inconsistent, incomplete, or incorrect)
Inadequate or missing feedback
Feedback Delays
Actuator
Inadequate operation
Sensor
Inadequate operation
Delayed operation
Vehicle does not stop
Incorrect or no information provided
Measurement inaccuracies
Feedback delays
Controller
Controlled Process
Component failures
Changes over time
Conflicting control actions
Process input missing or wrong
Unidentified or out-of-range disturbance
Process output contributes to system hazard

Figure 26: example of Why would control actions be improperly executed or not executed, leading to hazards (Thomas, 2021).

This second scenario type identifies hazard scenarios caused without a UCA. A hazard is then caused by a control action that is safe, but not executed or executed improperly. Two considerations must be made:
2.1. Factors that affect the control path (the control path transfers the control action to the controlled process).
2.2. Factors that affect the controlled process (the lower part of Figure 26).

General examples of scenarios that involve the control path:

- The control action is not executed
    - The control action is not received by actuator, but was sent by controller.
    - The control action is received by actuator, but the actuator does not respond.
    - The control action is received by actuator and it responds, but the controlled process does not receive the response.
- The control action is improperly executed
    - The control action is sent, but improperly received by actuator.
    - The control action is sent and received by actuator, but the actuator responds inadequately.
    - The control action is received and sent by actuator adequately, but the controlled process receives/applies the control action improperly.
    - No control action is set by controller, but actuator responds as if it was sent.

Those scenarios can be generally written down as:
<Scenario identification> = <control action> & <the result of improper/no execution> & <how could the control path contribute to this behaviour> & <resulting in hazard>

General examples of scenarios that involve the controlled process:

- The control action is not executed
    - The control action is properly received by the controlled process, but the controlled process does not respond.
- The control action is improperly executed
    - The control action is properly received by the controlled process, but the controlled process responds improperly.
    - No control action is received by the controlled process, but the controlled process responds as if it was received.

Those scenarios can be generally written down as:
<Scenario identification> = <control action> & <identification of what factors make the control action in the controlled process ineffective> & <resulting in hazard>

Traceability and solutions in STPA

With STPA, traceability is maintained throughout the steps. The loss scenarios are linked to the unsafe control actions, which in turn are linked to the hazards and the hazards are linked to the losses. With those links, a loss scenario can be traced back to the system-level Loss.

STPA does not only identify hazards or loss scenarios, but it also gives grip in how to prevent the identified hazards or loss scenarios. In step 1, system constraints are drafted to prevent the system hazards. Step 3 prevents unsafe control structure actions by suggesting controller constraints. After step 4, the most detailed and precise prevention measurements can be prescribed for the identified loss scenarios.

The traceability and solutions in STPA are illustrated in Figure 27.

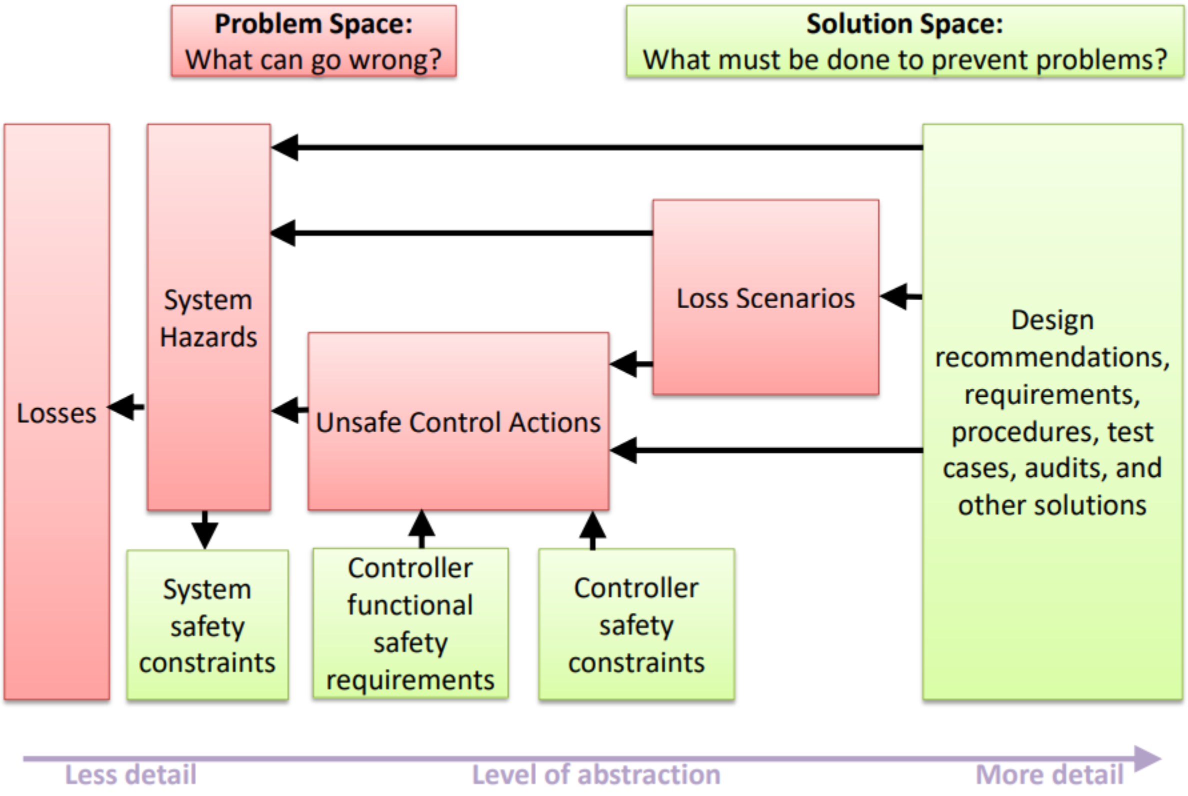

Problem Space:
What can go wrong?
Solution Space:
What must be done to prevent problems?
Losses
System Hazards
Loss Scenarios
Unsafe Control Actions
Design recommendations, requirements, procedures, test cases, audits, and other solutions
System safety constraints
Controller functional safety requirements
Controller safety constraints
Less detail
Level of abstraction
More detail

Figure 27: Traceability and solutions in STPA (Thomas, 2021).

Appendix C.

General and railway control structure examples

Step 2 in appendix B explains what the basics are for a control structure. This appendix illustrates different examples of control structures. It starts with generic control structures and the following models are applied to the railway industry and derived from different literature sources.

Control structures can differ in form and scope. In step 1 of STPA a system boundary is chosen, this boundary varies depending on the chosen scope. The system boundary for Figure 28 is only a part of the whole sociotechnical system chosen in Figure 29. More details can be added by broadening the scope and include more overarching factors in the control structure, like a socio-technical control structure. Or more details can be added by making the entities more specific, as illustrated in Figure 28. It is advised to model a control structure first as an abstract model (3, 4 or 5 entities, like Figure 30) and iteratively add more detail, the control actions and feedback arrows should always have detailed functional information.

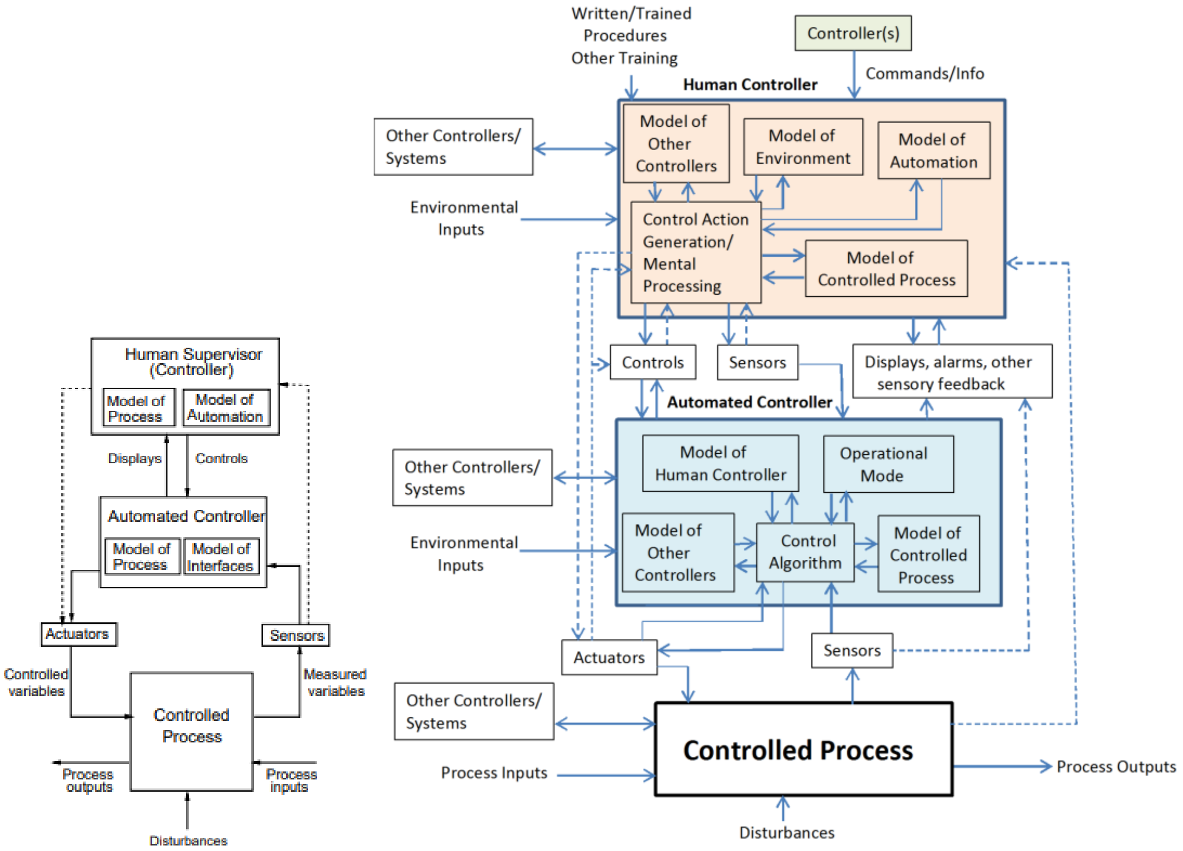


Figure 28: Two general control structures with human controller and automated controller. Left (Leveson 2004), Right (Leveson, 2018).

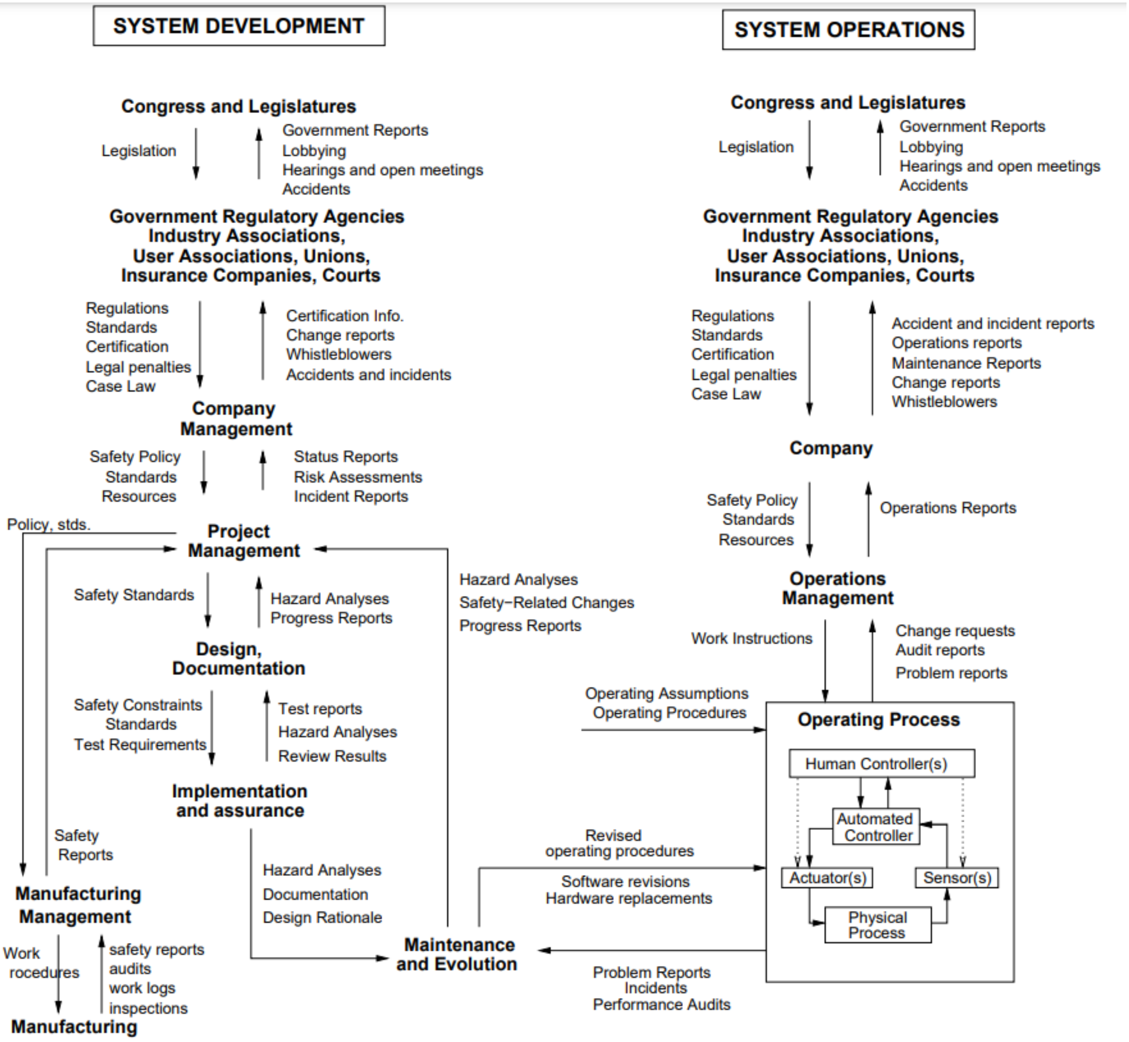


Figure 29: General Socio-technical control structure (Leveson, 2004).

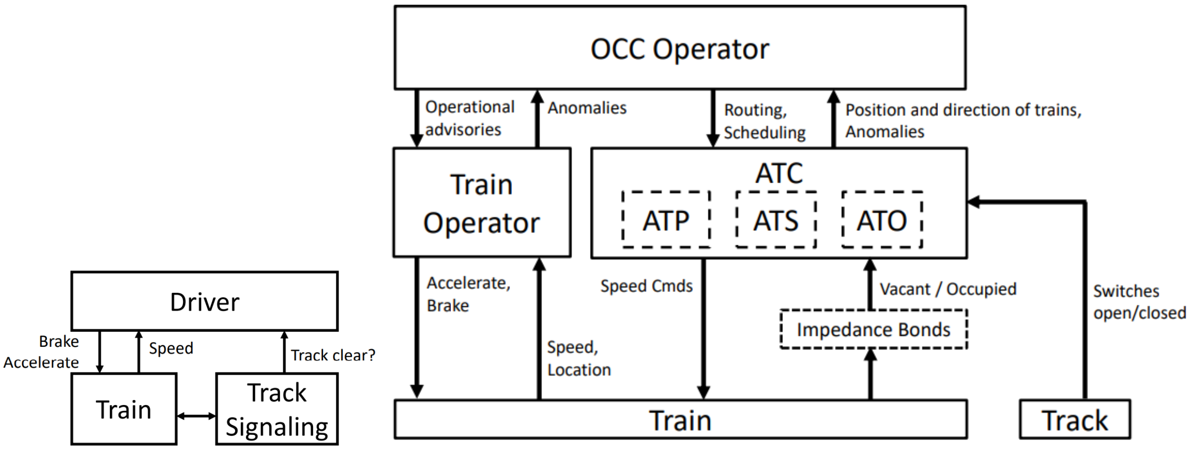


Figure 30: Two simplified train control structures (Thomas, 2021).

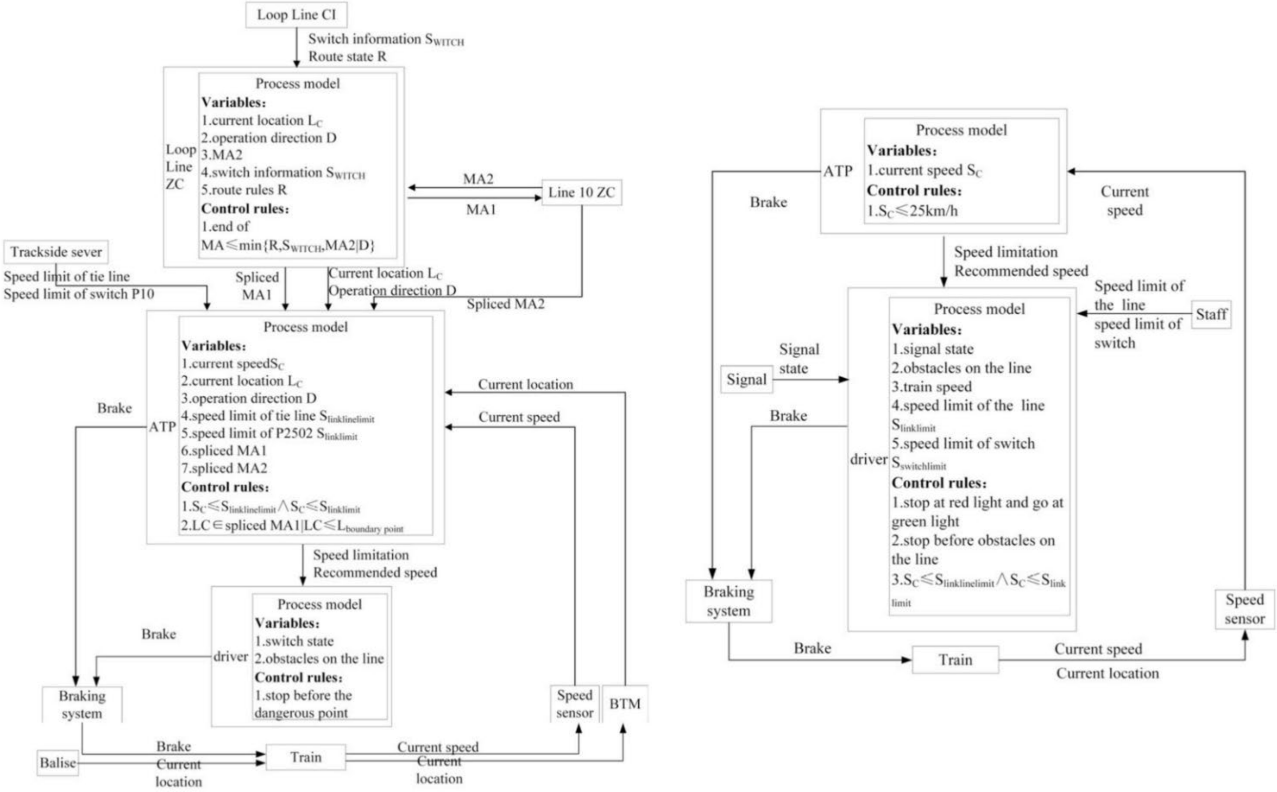


Figure 31: left: train control structure in communications-based train control mode. Right: train control structure in restriction mode. (Li et al., 2021)

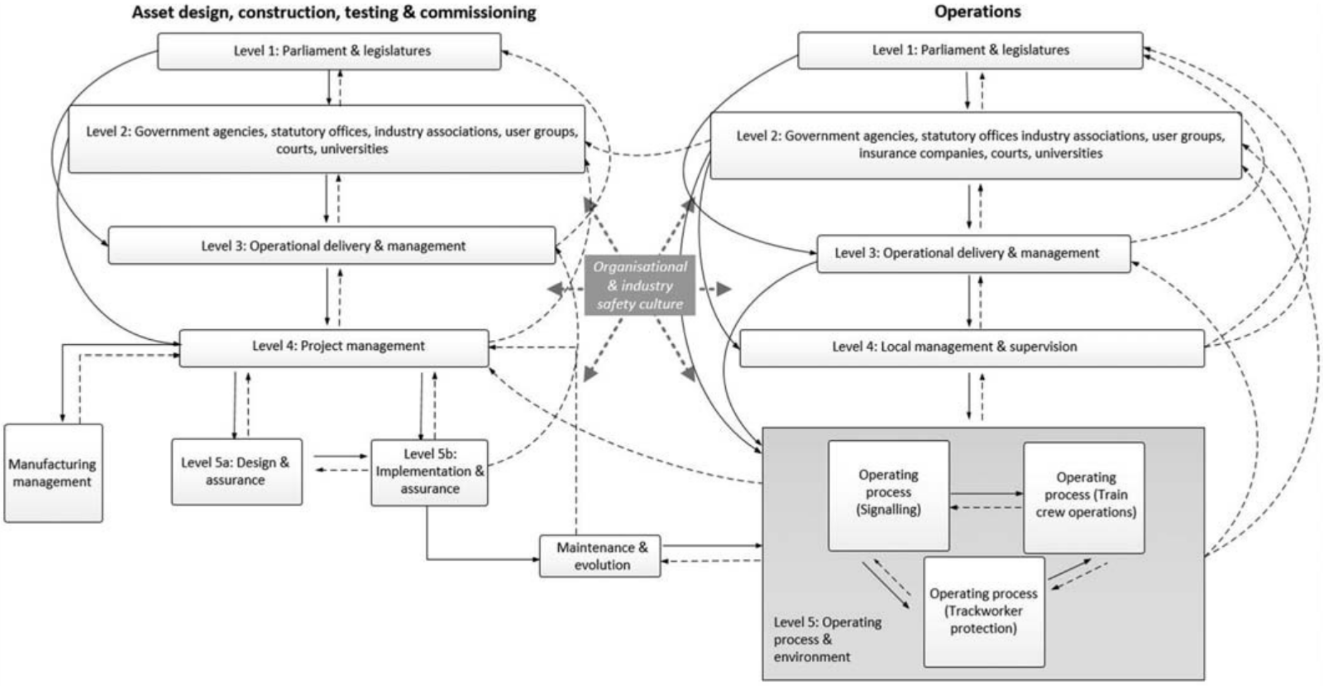

Asset design, construction, testing & commissioning
Level 1: Parliament & legislatures
Level 2: Government agencies, statutory offices, industry associations, user groups, courts, universities
Level 3: Operational delivery & management
Level 4: Project management
Manufacturing management
Level 5a: Design & assurance
Level 5b: Implementation & assurance
Maintenance & evolution
Organisational & industry safety culture
Operations
Level 1: Parliament & legislatures
Level 2: Government agencies, statutory offices industry associations, user groups, insurance companies, courts, universities
Level 3: Operational delivery & management
Level 4: Local management & supervision
Operating process (Signalling)
Operating process (Train crew operations)
Operating process (Trackworker protection)
Level 5: Operating process & environment

Figure 32: Summary overview of the control structure model for the sociotechnical railway industry in Australia (Read et al., 2019).

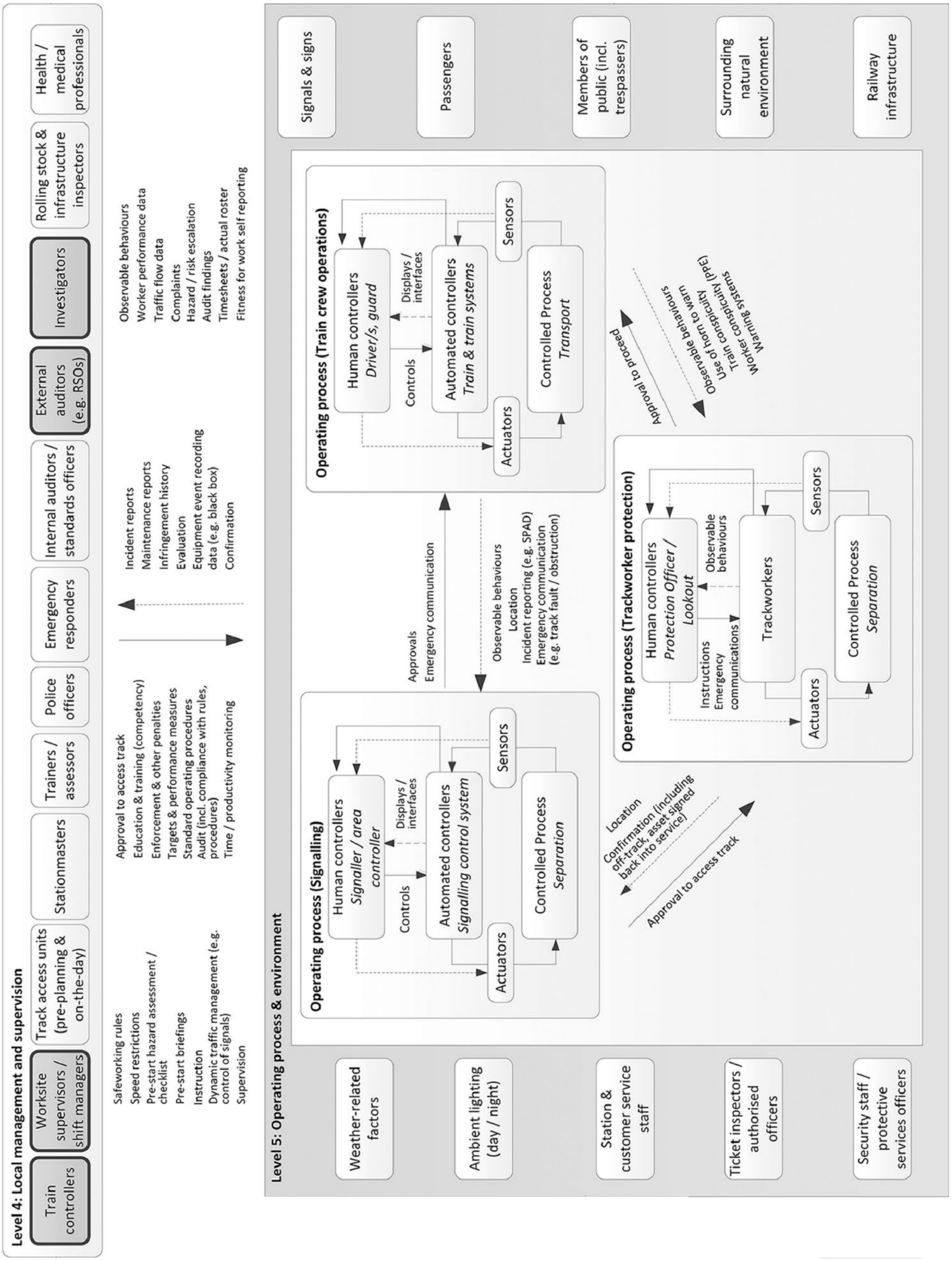
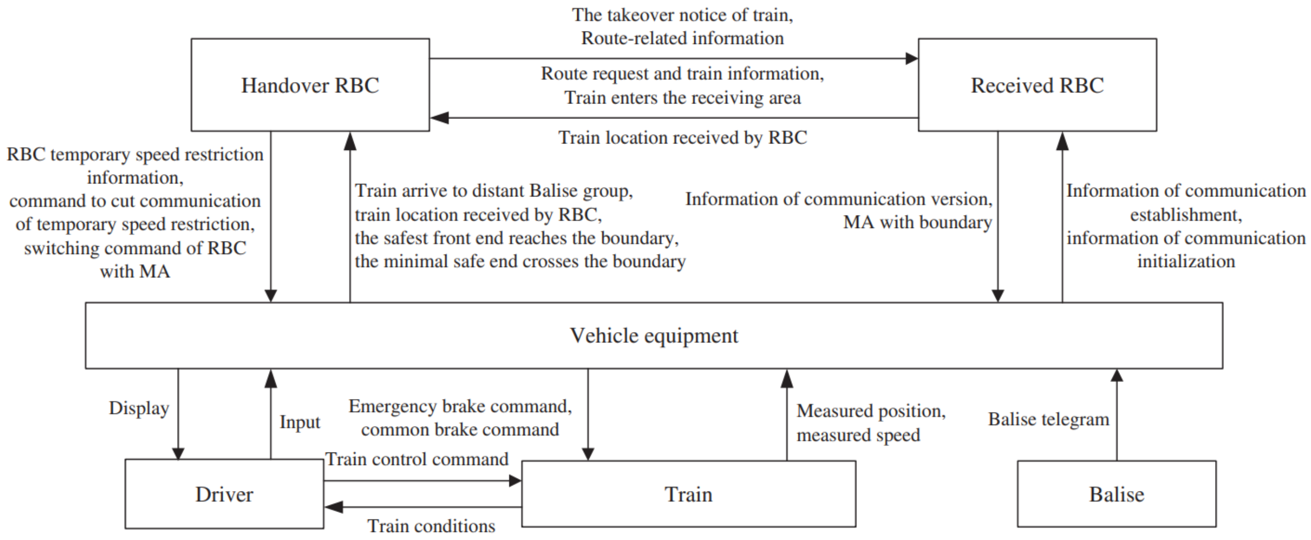

Level 4: Local management and supervision
Train controllers
Worksite supervisors / shift managers
Track access units (pre-planning & on-the-day)
Stationmasters
Trainers / assessors
Police officers
Emergency responders
Internal auditors / standards officers
External auditors (e.g. RSOs)
Investigators
Rolling stock & infrastructure inspectors
Health / medical professionals
Safeworking rules
Speed restrictions
Pre-start hazard assessment / checklist
Pre-start briefings
Instruction
Dynamic traffic management (e.g. control of signals)
Supervision
Approval to access track
Education & training (competency)
Enforcement & other penalties
Targets & performance measures
Standard operating procedures
Audit (incl. compliance with rules, procedures)
Time / productivity monitoring
Incident reports
Maintenance reports
Infringement history
Evaluation
Equipment event recording data (e.g. black box)
Confirmation
Observable behaviours
Worker performance data
Traffic flow data
Complaints
Hazard / risk escalation
Audit findings
Timesheets / actual roster
Fitness for work self reporting
Level 5: Operating process & environment
Weather-related factors
Ambient lighting (day / night)
Station & customer service staff
Ticket inspectors / authorised officers
Security staff / protective services officers
Signals & signs
Passengers
Members of public (incl. trespassers)
Surrounding natural environment
Railway infrastructure
Operating process (Signalling)
Human controllers Signaller / area controller
Controls
Displays / interfaces
Automated controllers Signalling control system
Actuators
Sensors
Controlled Process Separation
Approvals
Emergency communication
Observable behaviours
Location
Incident reporting (e.g. SPAD)
Emergency communication (e.g. track fault / obstruction)
Operating process (Train crew operations)
Human controllers Driver/s, guard
Controls
Displays / interfaces
Automated controllers Train & train systems
Actuators
Sensors
Controlled Process Transport
Location
Confirmation (including off-track, asset signed back into service)
Approval to access track
Operating process (Trackworker protection)
Human controllers Protection Officer / Lookout
Instructions
Emergency communications
Observable behaviours
Trackworkers
Actuators
Sensors
Controlled Process Separation
Approval to proceed
Observable behaviours
Use of horn to warn
Train conspicuity (PPE)
Worker conspicuity
Warning systems

Figure 33: A closer look at levels 4 and 5: the operations side of the control structure presented on the previous page. Solid arrows represent control actions; broken arrows represents feedback (Read et al., 2019).



The takeover notice of train,
Route-related information
Handover RBC
Received RBC
Route request and train information,
Train enters the receiving area
Train location received by RBC
RBC temporary speed restriction information,
command to cut communication of temporary speed restriction,
switching command of RBC with MA
Train arrive to distant Balise group,
train location received by RBC,
the safest front end reaches the boundary,
the minimal safe end crosses the boundary
Information of communication version,
MA with boundary
Information of communication establishment,
information of communication initialization
Vehicle equipment
Display
Input
Emergency brake command,
common brake command
Measured position,
measured speed
Balise telegram
Train control command
Driver
Train
Balise
Train conditions

Figure 34: Control structure of RBC handover in the Chinese train control system (Wang, 2018).

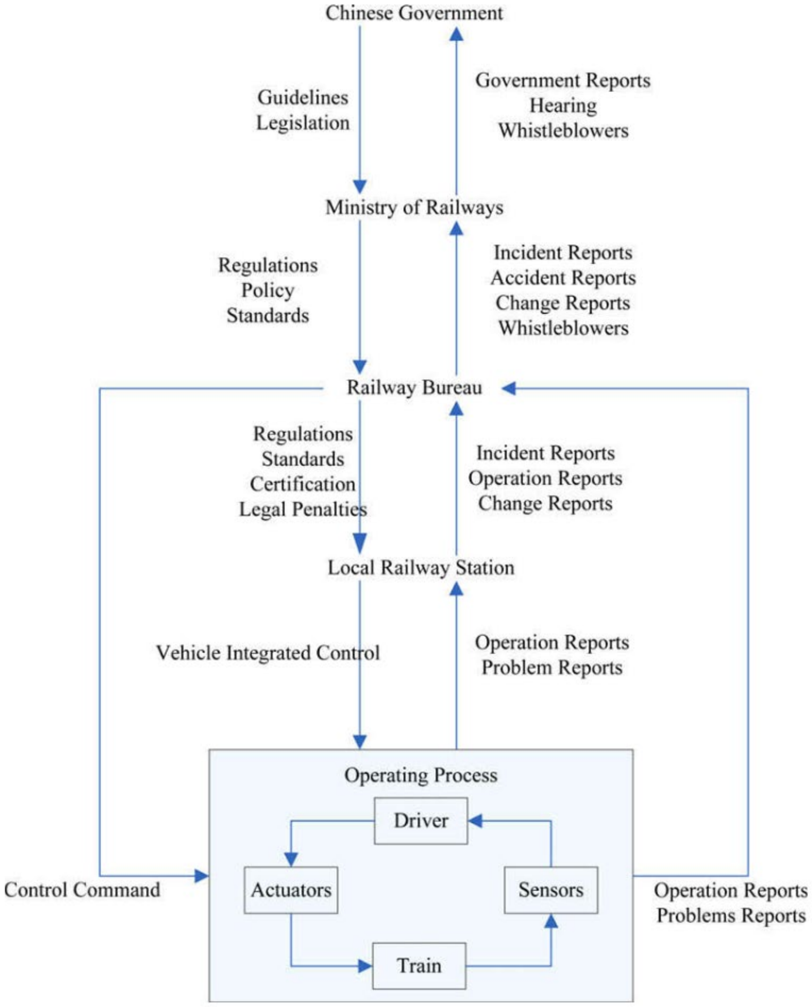


Figure 35: Control structure of Chinese sociotechnical railway transport system (Ouyang et al., 2010).

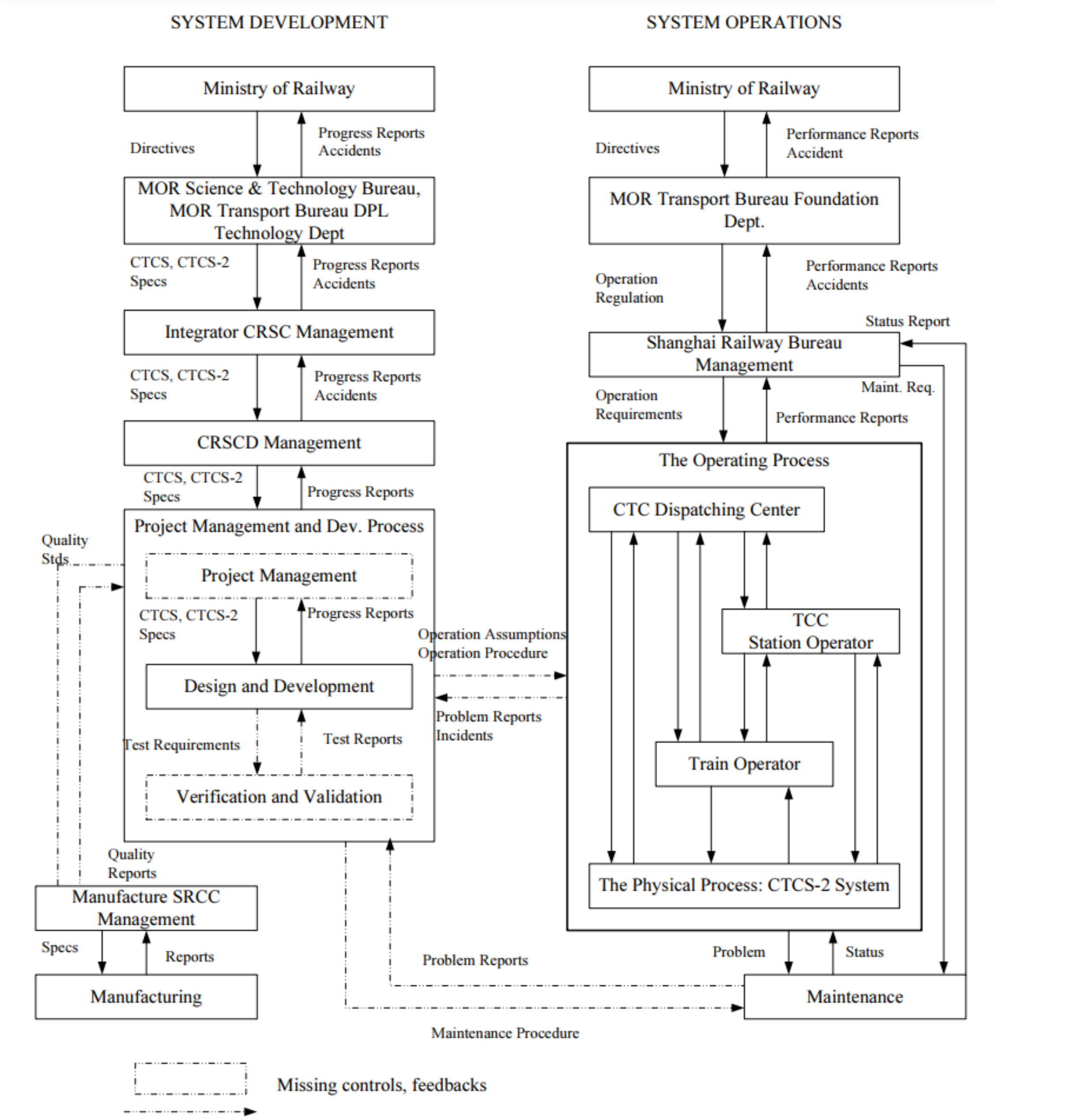


Figure 36: Chinese Train Control System project development and operations control structure (Dong, 2012).

Abbreviations used in the figure:
CTC = Centralized Traffic Control
TCC = Train Control Center
CTCS = Chinese Train Control System
MOR = Ministry of Railway
SRCC = Shanghai Railway Communication Company

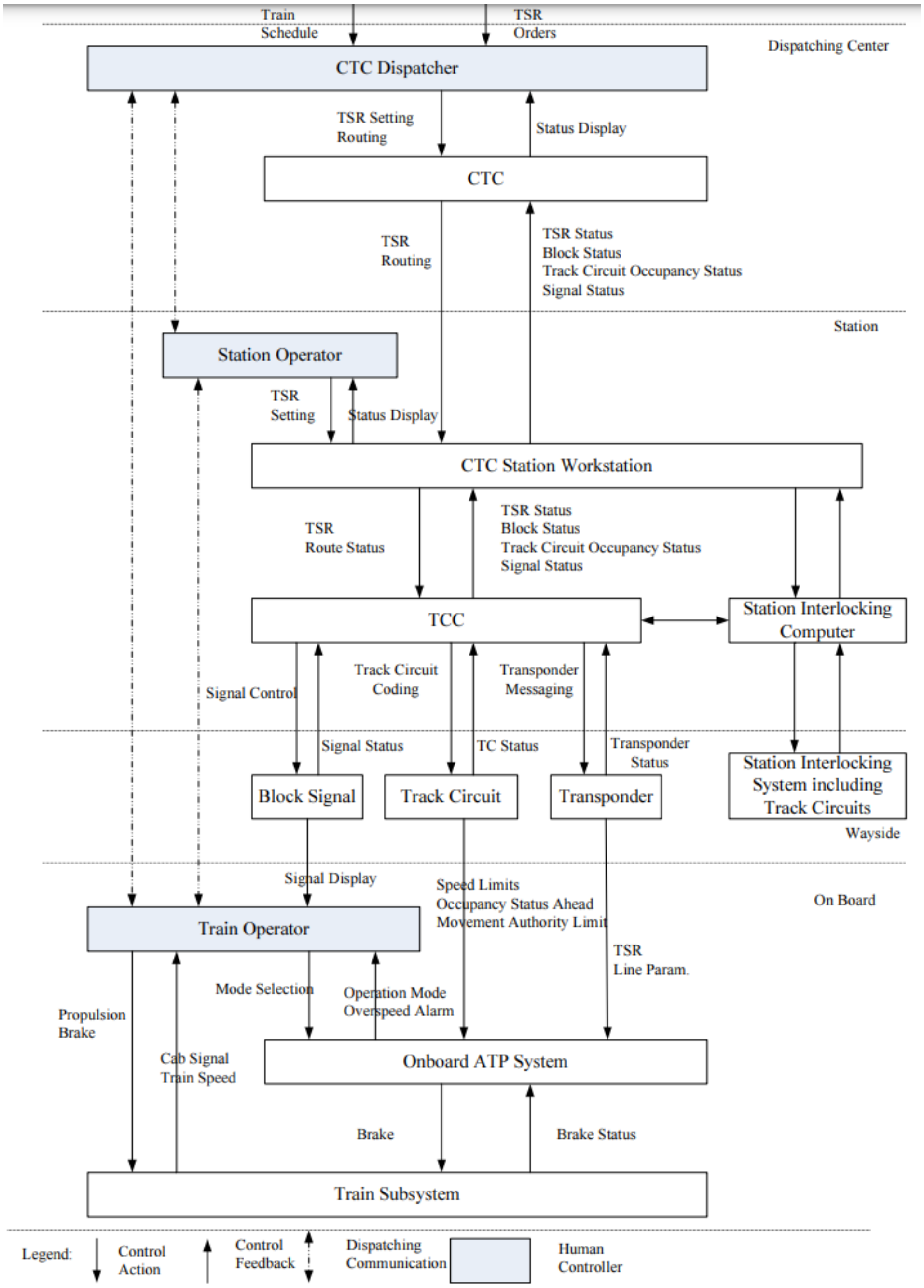


Figure 37: Control structure, to prevent collision between trains (Dong, 2012).

Abbreviations used in the figure:
CTC = Centralized Traffic Control
TCC = Train Control Centre
TC = Train-borne Controller
TSR = Temporary Speed Restriction

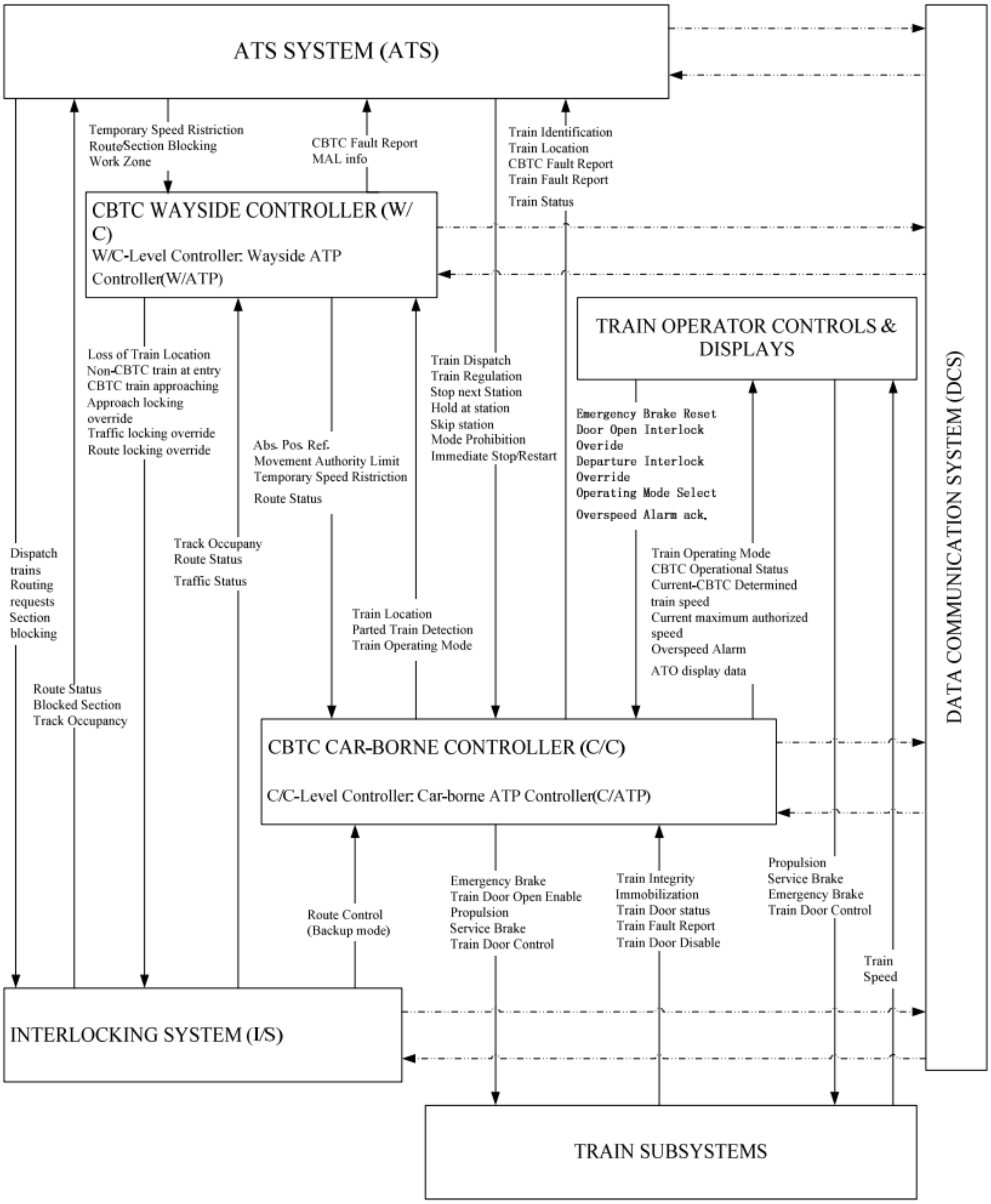


Figure 38: Control structure of a communication based train control system (Dong, 2012).

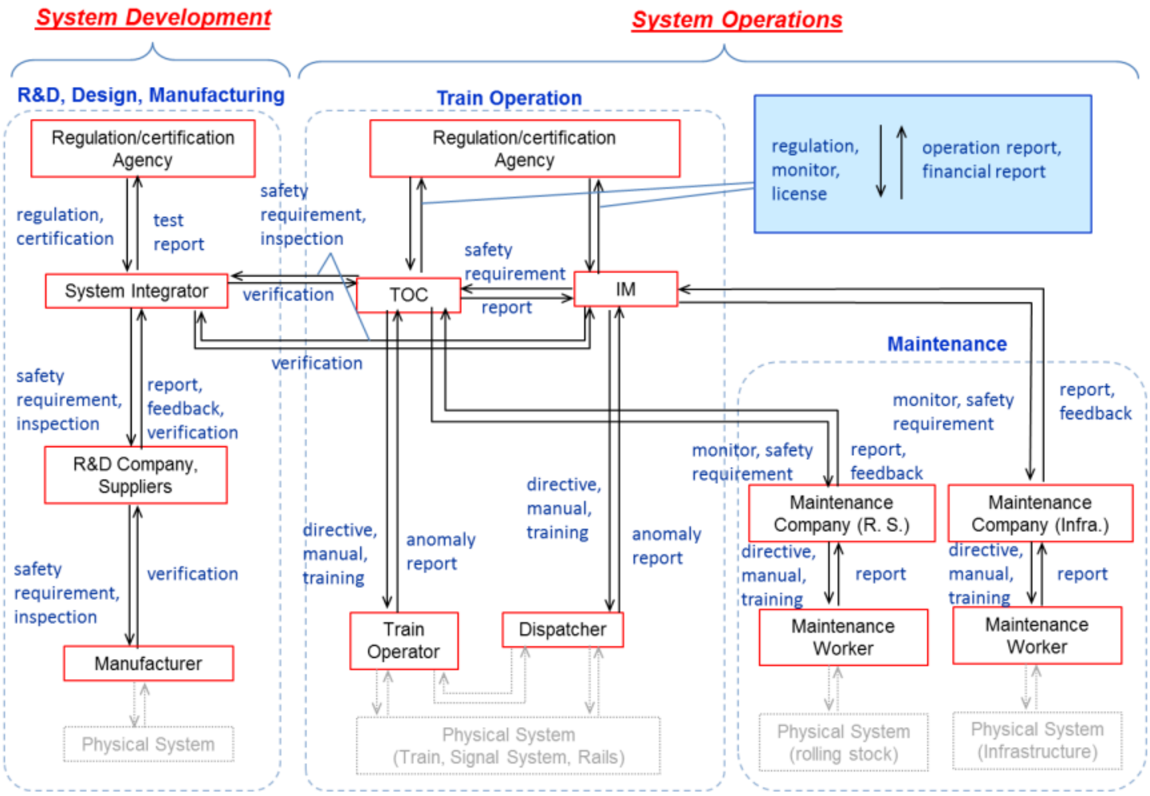

System Development
System Operations
R&D, Design, Manufacturing
Train Operation
Maintenance
Regulation/certification Agency
regulation, certification
test report
safety requirement, inspection
System Integrator
verification
safety requirement, inspection
report, feedback, verification
R&D Company, Suppliers
safety requirement, inspection
verification
Manufacturer
Physical System
Regulation/certification Agency
regulation, monitor, license
operation report, financial report
TOC
safety requirement
report
IM
verification
directive, manual, training
anomaly report
directive, manual, training
anomaly report
Train Operator
Dispatcher
Physical System (Train, Signal System, Rails)
monitor, safety requirement
report, feedback
monitor, safety requirement
report, feedback
Maintenance Company (R. S.)
Maintenance Company (Infra.)
directive, manual, training
report
directive, manual, training
report
Maintenance Worker
Maintenance Worker
Physical System (rolling stock)
Physical System (Infrastructure)

Figure 39: Safety control structure of a generic highspeed railsystem (Kawakami, 2014).

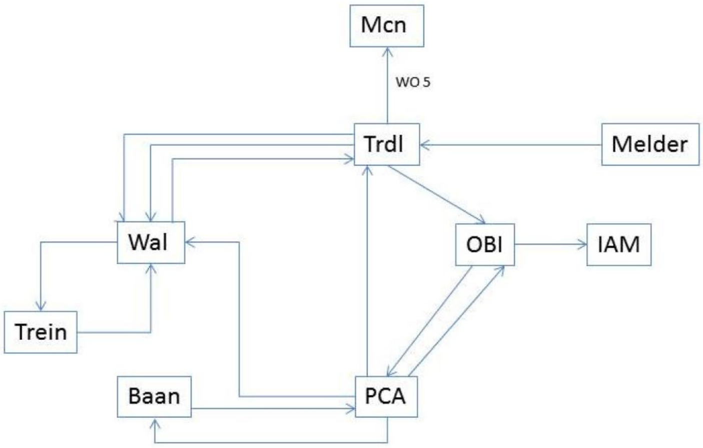


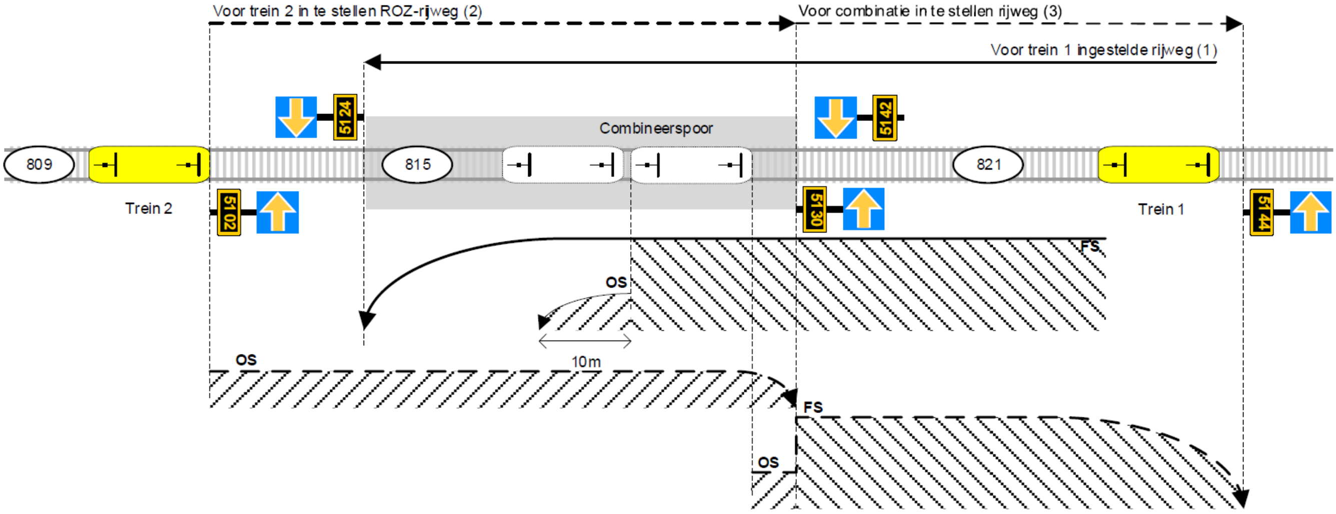
Figure 40: Control structure of user process 47: 'setting a temporary speed limit' (ProRail, 2022b).

Figure 40 illustrates a different control structure, compared to the previously illustrated ones. The hierarchical structure is not illustrated (in hierarchical structures, all downward facing arrows are control actions and all upward facing arrow are feedback) and no information is provided for the control actions and feedback mechanisms. This was the only control structure found by the author that models a structure from a process executed in the Netherlands. The control structure is made for investigating hazards in the user process of setting a temporary speed limit. Abbreviations used in the figure: MCN = train driver; TRDL = train dispatcher; Melder = reporting person; Wal = train control system and central safety system; OBI = control room rail; IAM = information to train driver; Trein = train; Baan = train track; PCA = process contractor.

Appendix D.

Behavioural chain of user process 48

This appendix illustrates a behavioural chain of user process 48 with an example scenario. The example scenario is shown in Figure 41, where two train (depicted in yellow trains) arrive from opposite directions.
User process 48 is: ‘Combining two trains coming from opposite directions with movement authority.’



Voor trein 2 in te stellen ROZ-rijweg (2)
Voor combinatie in te stellen rijweg (3)
Voor trein 1 ingestelde rijweg (1)
5124
5142
Combineerspoor
809
815
821
Trein 2
Trein 1
5102
5130
5144
FS
OS
10m
OS
FS
OS

Figure 41: User process 48 example illustration: Combining two trains coming from opposite directions with movement authority (ProRail, 2022c).

The behavioural chain is illustrated in Dutch in Figure 42.

Abbreviations used in the behavioural chain:
SMB = Stop marker bord
ROZ = Driving on sight (Dutch: rijden op zicht)
OS = On sight
FSMA = Full supervision movement authority
OSMA = On sight movement authority
EoA = End of authority
SB = Standby
SL = Sleeping
RBC = Radio block centre

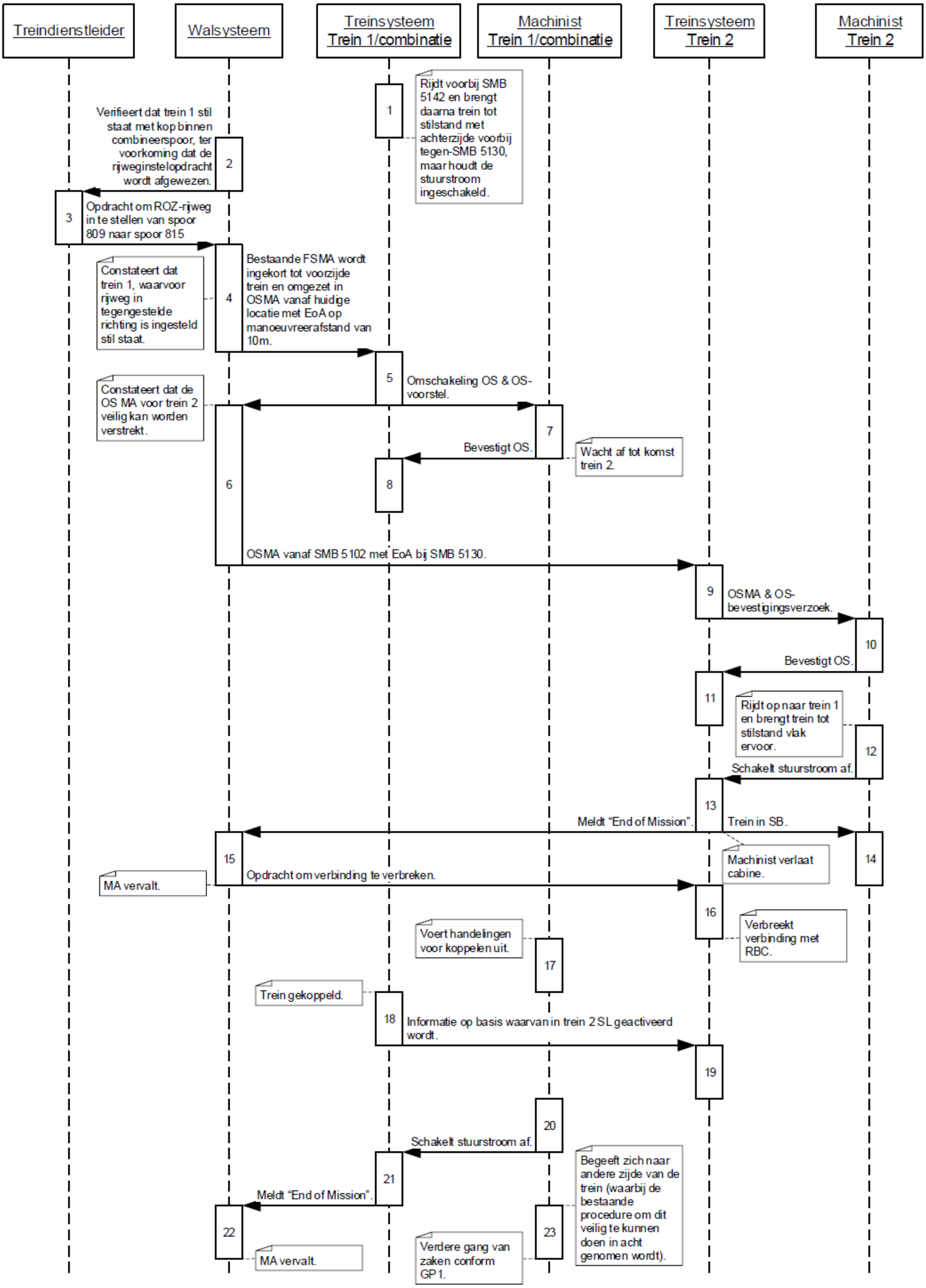

Treindienstleider
Walsysteem
Treinsysteem Trein 1/combinatie
Machinist Trein 1/combinatie
Treinsysteem Trein 2
Machinist Trein 2
1
Rijdt voorbij SMB 5142 en brengt daarna trein tot stilstand met achterzijde voorbij tegen-SMB 5130, maar houdt de stuurstroom ingeschakeld.
Verifieert dat trein 1 stil staat met kop binnen combineerspoor, ter voorkoming dat de rijweginstelopdracht wordt afgewezen.
2
3
Opdracht om ROZ-rijweg in te stellen van spoor 809 naar spoor 815
Constateert dat trein 1, waarvoor rijweg in tegengestelde richting is ingesteld stil staat.
4
Bestaande FSMA wordt ingekort tot voorzijde trein en omgezet in OSMA vanaf huidige locatie met EoA op manoeuvreerafstand van 10m.
5
Omschakeling OS & OS-voorstel.
Constateert dat de OS MA voor trein 2 veilig kan worden verstrekt.
6
7
Bevestigt OS.
Wacht af tot komst trein 2.
8
OSMA vanaf SMB 5102 met EoA bij SMB 5130.
9
OSMA & OS-bevestigingsverzoek.
10
Bevestigt OS.
11
Rijdt op naar trein 1 en brengt trein tot stilstand vlak ervoor.
12
Schakelt stuurstroom af.
13
Meldt “End of Mission”.
Trein in SB.
14
15
Machinist verlaat cabine.
MA vervalt.
Opdracht om verbinding te verbreken.
16
Verbreekt verbinding met RBC.
Voert handelingen voor koppelen uit.
17
Trein gekoppeld.
18
Informatie op basis waarvan in trein 2 SL geactiveerd wordt.
19
20
Schakelt stuurstroom af.
21
Begeeft zich naar andere zijde van de trein (waarbij de bestaande procedure om dit veilig te kunnen doen in acht genomen wordt).
Meldt “End of Mission”.
22
23
MA vervalt.
Verdere gang van zaken conform GP1.

Figure 42: Behavioural chain of user process 48 (ProRail, 2022c).

Appendix E.

Framework of the workshop ‘modelling a control structure’ (In Dutch)

Datum: 27 juli

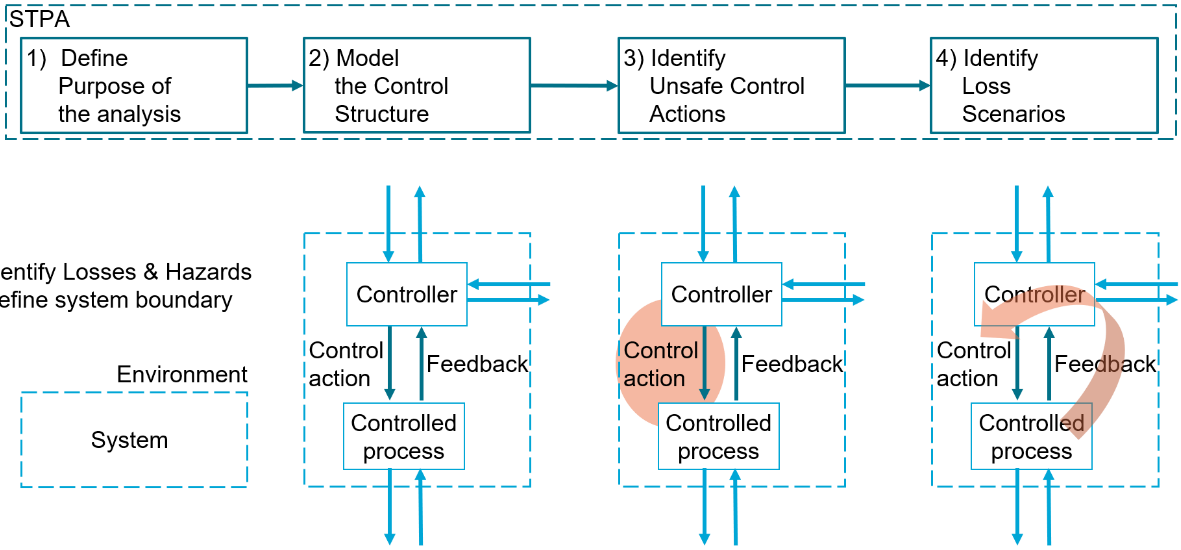
[13.00-13.05] Informatief

1. uitleg workshop

- Workshop opnemen via teams
- Middag planning, eerst uitleg, dan generiek, dan specifiek
- Voorstellen. Deelnemer 1 kent de gebruikersprocessen goed, deelnemer 2 kent STPA goed

[13.05-13.15] Informatief

2. Uitleg stap 2 STPA (controle structuur maken volgens het STPA handboek en de do’s and don’t)



- STPA is een systematisch aanpak om gevaren te identificeren en analyseren.
- Definitie controle structuur: een hiërarchische controle structuur is een model van een systeem dat bestaat uit iets wat controleert en het gecontroleerde proces met daartussen feedback controle mechanismes.
- Naar beneden gaande lijnen zijn controle acties, naar boven gaande lijnen is feedback, horizontale lijnen zijn in en output en dus geen controle acties of feedback.
- Een controle structuur is een ‘functional model’ en geen ‘physical model’ (zoals blok diagrammen) of ‘executable/simulation model’ (want het kan mensen bevatten in het model).
- Gehoorzaamheid aan controle acties of correcte feedback moet niet worden aangenomen.
- Een model mag abstract/generiek (high-level) zijn, als de controle acties en feedback maar wel specifiek is. Voorbeeld slides van lessons learned (Thomas, 2020).
- De Pijlen moeten specifieke functionele informatie bevatten (Wel: stuurstroom uit/aan-zetten. Niet: stuurstroom knop).

- De verantwoordelijkheden van een actor moet naar voren komen in de controle acties en de feedback.
- Hoger in de hiërarchie betekend ook dat ze hogere doelen nastreven (treindienstleider staat boven de machinist met verantwoordelijkheid voor maar 1 trein).

[13.15-13.30] Informatief en licht interactief

3. Trein controle structuur voorbeelden bekijken en positieve en negatieve doorspreken met elkaar

- Figure 30: Actoren boven en onder elkaar geven goed de hiërarchie aan, duidelijke beschrijving bij de pijlen.
- Figure 31: Niet duidelijk hiërarchisch afgebeeld, maar laat wel de process model, actuatoren en sensoren zien (welke niet verplicht zijn, maar wel verduidelijkend kunnen werken voor de laatste stap van STPA).
- Figure 34: Controle structuur voor het gebruikersproces voor het veranderen van RBC, maar klopt hiërarchisch niet.
- Figure 37: Niet hiërarchisch en geen info bij de pijlen.
- Figure 38: Algemeen controle structuur, waardoor deze goed uitgebreid is.
- Figure 40: 7 actoren en duidelijke info bij de pijlen, daarnaast zie je dat de DCS niet in de hiërarchie staat, maar een communicatie kanaal aangeeft.

[13.30-13.50] Interactief

4. Gezamenlijk een generiek controle structuur maken van een ERTMS trein controle structuur (generieke actoren, controle acties en feedback)

- Een model dat als beginpunt (goede inspiratie kan dienen) om verschillende controle structuren op te baseren.
- A3 papier gebruiken voor het schetsen van de controle structuur

[13.50-14.05] Informatief

5. Uitleg GP48: combineren van twee treinen komende uit tegengestelde richting met MA

- Bespreken van het gebruikersproces procedure in bijlage D beschreven.
- Verduidelijkende vraag: wat gebeurt er als het combineren niet op het combineerspoor plaats vindt? Trein 1 voor de eerste SMB al stopt of juist na de tweede SMB?
- Verduidelijkende vraag: wat is een combineerspoor? Fysiek iets anders dan een ander spoor?
- Verduidelijkende vraag: hoe wordt ROZ rijweg ingesteld? Wat houdt ROZ in?
- Verduidelijkende vraag: hoe controleert ETCS trackside of een trein stil staat?

[14.05-14.15] Interactieve brainstorm

6. Betrokken actoren benoemen (controllers and controlled process)

- Welke actoren zijn betrokken bij dit GP?
- Wat houden deze actoren in (korte beschrijving)
- Wat zijn hun verantwoordelijkheden?

[14.15-14.25] Interactieve brainstorm

7. Betrokken controle acties en feedback bespreken

- Controle acties en feedback bespreken per actor
- Invloeden van buitenaf? (planning, staat van het spoor, wet- en regelgeving, trainingen)
- Verduidelijkende vraag: resulteert elke controle actie ook tot feedback uit het gecontroleerde proces?

[14.25-14.35] Individueel

8. Controle structuur maken voor GP48

- A3 papier gebruiken voor het schetsen van de controle structuur

[14.35-15.00] Interactief

9. Elkaars GP48 controle structuur bespreken en 1 controle structuur maken

- Elkaars controle structuur bespreken
- Gezamenlijk een controle structuur maken
- Hoe kan het meer generiek gemaakt worden?
- Hoe kan het meer specifiek gemaakt worden?

Bedanken voor uw deelname aan de workshop

Appendix F.

Unsafe control actions

This appendix elaborates about the unsafe control actions (UCA) in user process 48. The UCA's are identified by following the STPA handbook. The UCA's are written following the advised format: <UCA specification> = <Source> & <Type> & <Control Action> & <Context> & <Link to Hazards>

If no UCA is found, then 'not applicable' is noted in the table. An UCA is not applicable if non UCA is found or applicable. Control actions that do not have a duration, cannot be stopped to soon or applied too long, so those are never applicable.

Control action	Not providing	Providing	Too early, too late or wrong order	Stopping too soon, applying too long
Set ROZ route	UCA-1: Dispatcher not setting a ROZ route while the train is ready to drive onto the combining track [H-2] UCA-2: Dispatcher not setting a ROZ route, because another route (normal or signal passed at danger) is set instead [H-2]	UCA-3: Dispatcher setting a ROZ route on the wrong track [H-2]	UCA-4: Dispatcher sets ROZ too early for train 2, while train 1 is not in stand still Setting a ROZ route too early, resulting in UCA-1	Not applicable

Table 13: Unsafe control actions from dispatcher

Control action	Not providing	Providing	Too early, too late or wrong order	Stopping too soon, applying too long
Accelerate	UCA-5: Driver does not provide acceleration control action while train drives slower than permitted speed [H-1]	UCA-6: Driver provides acceleration control action while train drives harder than the permitted speed [H-1] UCA-7: Driver provides the acceleration control action with an insufficient level of acceleration while train drives slower than permitted speed [H-1]	UCA-8: Driver provides the acceleration too late (>TBD seconds) after the train drives slower than permitted speed [H-1]	UCA-9: Driver stops providing the acceleration control action too early, before the train drives on permitted speed. [H-1] UCA-10: Driver applies the acceleration control action too long, while the train is already on permitted speed [H-1]
Brake	UCA-11: Driver does not provide the brake while train drives harder than the permitted speed [H-1]	UCA-12: Driver provides the brake while train drives slower than or at the permitted speed [H-1] UCA-13: Driver provides the brake with an insufficient level of braking while train drives harder than permitted speed [H-1] UCA-14: Driver provides the brake and stops the train before the train is in the right position in the combining track. [H-1]	UCA-15: Driver provides the brake too late (>TBD seconds) after driver receives speeding warning [H-1] Braking too early, resulting in UCA-12	UCA-16: Driver stopped too soon with braking, while train is not yet standing still in the combining track [H-1]

Confirm OSMA	UCA-17: Driver does not confirm OSMA, while train system suggests applying OSMA on the DMI and train drives into combining track [H-2]	Not applicable	Confirming OSMA too late, resulting in UCA-17	Not applicable
Control current off	UCA-18: Driver does not switch the control current off, while the driver leaves the cab. [H-1 (indirectly)]	UCA-19: Driver switches the control current off, while the train still needs to be operated. [H-1]	Switching of the control current in the wrong order, resulting in UCA-19 Switching of the control current too late, resulting in UCA-18	Not applicable
Combining trains	UCA-20: Driver does not combine trains, while both trains are ready to combine [H-1]	UCA-21: Driver combines train while not following the combining procedure [H-1]	UCA-22: Driver combines trains too early, while not all actions for preparations are done. [H-1 (indirectly)]	UCA-23: Driver stopping too soon with combining trains, while not all combining actions are done [H-1]

Table 14: Unsafe control actions from driver

Control action	**Not providing**	**Providing**	**Too early, too late or wrong order**	**Stopping too soon, applying too long**
Provide OSMA	UCA-24: Trackside system not providing an OSMA while the train is ready to drive in the combining track [H-2]	UCA-25: Trackside system providing an OSMA for the wrong track [H-2]	Trackside system too late providing OSMA, resulting in UCA-24	Not applicable
Disconnect train from RBC	UCA-26: Trackside system does not disconnect the train from the RBC, while the control current is shut off [H-2]	UCA-27: Trackside system disconnects train from RBC, while the train is still operated by the driver [H-2]	Trackside system too early disconnecting train from RBC, resulting in UCA-27	Not applicable

Table 15: Unsafe control actions from trackside system

Controller constraints

Controller constraints can be defined if unsafe control actions are identified. The STPA handbook defines controller constraints as constraints that specify the behaviour of the controller that needs to be met to prevent an UCA. Simply set is a controller constraint the inverted version of the UCA. The controller constraints are mentioned below.

C-1: Dispatcher must set a ROZ route if the train is ready to drive onto the combining track [UCA-1]
C-2: Dispatcher must set the appropriate route [UCA-2]
C-3: Dispatcher must set a ROZ route on the right track [UCA-3]
C-4: Dispatcher must not set ROZ too early for train 2, if train 1 is in stand still [UCA-4]
C-5: Driver must provide acceleration control action if train drives slower than permitted speed [UCA-5]
C-6: Driver must not provide acceleration control action if train drives harder than the permitted speed [UCA-6]
C-7: Driver must provide the acceleration control action with a sufficient level of acceleration if train drives slower than permitted speed [UCA-7]
C-8: Driver must not provide the acceleration too late (>TBD seconds) after the train drives slower than permitted speed [UCA-8]
C-9: Driver must not stop providing the acceleration control action too early, before the train drives on permitted speed [UCA-9]
C-10: Driver must not apply the acceleration control action too long, if the train is already on permitted speed [UCA-10]
C-11: Driver must provide the brake if train drives harder than permitted speed [UCA-11]
C-12: Driver must not provide the brake if train drives slower than or at the permitted speed [UCA-12]
C-13: Driver must provide the brake with a sufficient level of braking if train drives harder than permitted speed [UCA-13]
C-14: Driver must not provide the brake and stop the train, before the train is in the right position in the combining track [UCA-14]
C-15: Driver must not provide the brake too late (>TBD seconds) after driver receives speeding warning [UCA-15]
C-16: Driver must not stop too soon with braking, if train is not yet standing still in the combining track [UCA-16]
C-17: Driver must confirm OSMA, if train system suggests applying OSMA on the DMI and train drives into combining track [UCA-17]
C-18: Driver must switch the control current off, if the driver leaves the cab [UCA-18]
C-19: Driver must not switch the control current off, if the train still needs to be operated [H-1]
C-20: Driver must combine trains, if both trains are ready to combine [H-1]
C-21: Driver must combine train, following the combining procedure [H-1]
C-22: Driver must not combine trains too early, if not all actions for preparations are done [H-1]
C-23: Driver must not stop too soon with combining trains, if not all combining actions are done [H-1]
C-24: Trackside system must provide an OSMA if the train is ready to drive in the combining track [H-2]
C-25: Trackside system must not provide an OSMA for the wrong track [H-2]
C-26: Trackside system must disconnect the train from the RBC, if the control current is shut off [H-2]
C-27: Trackside system must not disconnect a train from RBC, if the train is still operated by the driver [H-2]

Appendix G.

Loss scenarios for user process 48

The different scenario categories are generally written in the following way:

1.1. <Scenario identification> = <UCA> & <Because Beliefs/control algorithm/defect/input> & <context>
1.2. <Scenario identification> = <UCA> & <True state from UCA context> & <information received> & <how the information received could happen, given the true state>
2.1. <Scenario identification> = <control action> & <the result of improper/no execution> & <how could the control path contribute to this behaviour> & <resulting in hazard>
2.2. <Scenario identification> = <control action> & <identification of what factors make the control action in the controlled process ineffective> & <resulting in hazard>

Loss scenarios for setting a ROZ route
Related to UCA-1 (scenario categories 1.1. and 1.2.)

- LS-1: Dispatcher not setting a ROZ route while the train is ready to drive onto the combining track, because the dispatchers training is inadequate, new systems are used under ERTMS (for example ETIS) and the procedure changes. The dispatcher may be wrong with the old procedure and think that a call is needed to confirm that the train is standing still.
- LS-2: Dispatcher not setting a ROZ route while the train is ready to drive onto the combining track, because the dispatcher thinks that the train is not yet standing still, because the dispatcher once had experience with a train driver who drove very slowly.
- LS-3: Dispatcher not setting a ROZ route while the train is ready to drive onto the combining track, because the dispatcher expects the train to move slightly, even if it is currently standing still. The dispatcher relies on the system, but thinks the train will move slightly again. The dispatcher does not receive confirmation from the driver that the train will not move again.
- LS-4: Dispatcher not setting a ROZ route while the train is ready to drive onto the combining track, because the feedback from the trackside system does not send a position report. This might be caused by no connection between the ‘procesleiding’ and ETIS, but also between ETIS and the RBC.
- LS-5: Dispatcher not setting a ROZ route while the train is ready to drive onto the combining track, because the train movement is not included in the route plan (Dutch: rijwegplan), so the dispatcher does not know that the combining of the train is planned.
- LS-6: Dispatcher not setting a ROZ route while the train is ready to drive onto the combining track, because the configurations are not consistent between procesleiding and ETIS. Example: ETIS says that the train is on spot A, but the procesleiding thinks that this spot is somewhere else or does not know the spot.

Related to UCA-2 (scenario categories 1.1. and 1.2.)

- LS-7: Dispatcher not setting a ROZ route, but another route (normal or signal passed at danger) is set instead, because the dispatcher does not know which track are combining tracks (the procesleiding does not differentiate tracks between normal and combining tracks) and might think that the train wants a normal route if the route plan is not followed.
- LS-8: Dispatcher not setting a ROZ route, but another route (normal or signal passed at danger) is set instead, because a ROZ route is not possible (for example, due to a switch malfunction) and the dispatcher choses for the possibility of a signal passed at danger route.

- LS-9: Dispatcher not setting a ROZ route, but another route (normal or signal passed at danger) is set instead, because the configurations are not consistent between procesleiding and ETIS.

Related to UCA-3 (scenario categories 1.1. and 1.2.)

- LS-10: Dispatcher setting a ROZ route on the wrong track, because the dispatcher is used to combine on another track and thinks that the route plan is wrong.
- LS-11: Dispatcher setting a ROZ route on the wrong track, because the dispatcher makes a mistake by applying the ROZ route for a different route of another train that needs to combine.
- LS-12: Dispatcher setting a ROZ route on the wrong track, because the configurations are not consistent between procesleiding and ETIS.

Related to UCA-4 (scenario categories 1.1. and 1.2.)

- LS-13: Dispatcher sets ROZ too early for train 2, while train 1 is not in stand still, because the dispatcher is in a hurry and thinks that the train is almost stopped.
- LS-14: Dispatcher sets ROZ too early for train 2, while train 1 is not in stand still, because the dispatcher forgot to check if the train is standing still.
- LS-15: Dispatcher sets ROZ too early for train 2, while train 1 is not in stand still, because train incorrectly reports that it is standing still, due to an odometry error.

Related to the control action (scenario categories 2.1. and 2.2.)

- LS-16: ROZ route is not set due to malfunctioning of hardware or software, the mouse of the dispatcher might break or no selection of ROZ can be chosen in procesleiding. [H-2]
- LS-17: ROZ route is not set due to configuration inconsistencies, corruption of the control action can be caused by a hack. [H-2]

Loss Scenarios for accelerating

Related to UCA-5 (scenario categories 1.1. and 1.2.)

- LS-18: Driver does not provide acceleration control action while train drives slower than permitted speed, because the speed profile indicates a faster speed than the actual speed, this can be caused by a malfunctioning odometry
- LS-19: Driver does not provide acceleration control action while train drives slower than permitted speed, because past experience makes the driver think the train is coming from the same direction and the driver stops at the wrong place of the combining track
- LS-20: Driver does not provide acceleration control action while train drives slower than permitted speed, because the driver thinks that the train has a different length than the actual length and does not accelerate, due to habituation of driving with another length of the train on the same track.
- LS-21: Driver does not provide acceleration control action while train drives slower than permitted speed, because the signage along the track is misinterpreted by the driver.

Related to UCA-6 (scenario categories 1.1. and 1.2.)

- LS-22: Driver provides acceleration control action while train drives harder than the permitted speed, because the speed profile indicates a slower speed than the actual speed, this can be caused by a malfunctioning odometry

Related to UCA-7 (scenario categories 1.1. and 1.2.)

- LS-23: Driver provides the acceleration control action with an insufficient level of acceleration while train drives slower than permitted speed, because the driver is used to drive with other trains (a lighter/shorter train for example), which makes the driver think that the train can accelerate faster.
- LS-24: Driver provides the acceleration control action with an insufficient level of acceleration while train drives slower than permitted speed, because the speed profile indicates a faster speed than the actual speed, this can be caused by a malfunctioning odometry.

Related to UCA-8 (scenario categories 1.1. and 1.2.)

- LS-25: Driver provides the acceleration too late (>TBD seconds) after the train drives slower than permitted speed, because the driver is distracted, no sound notification is provided if the train drives too slow.

Related to UCA-9 (scenario categories 1.1. and 1.2.)

- LS-26: Driver stops providing the acceleration control action too early, before the train drives on permitted speed, because the driver is used to drive with other trains (a lighter/shorter train for example), which makes the driver think that the train is already getting to the desired speed.
- LS-27: Driver stops providing the acceleration control action too early, before the train drives on permitted speed, because the speed profile indicates a faster speed than the actual speed, this can be caused by a malfunctioning odometry.

Related to UCA-10 (scenario categories 1.1. and 1.2.)

- LS-28: Driver applies the acceleration control action too long, while the train is already on permitted speed, because the driver is used to drive with other trains (a heavier/longer train for example), which makes the driver think that the train is not yet reaching the desired speed.
- LS-29: Driver applies the acceleration control action too long, while the train is already on permitted speed, because the speed profile indicates a slower speed than the actual speed, this can be caused by a malfunctioning odometry.
- LS-30: Driver applies the acceleration control action too long, while the train is already on permitted speed, because the driver is distracted and the warning sound is broken/not heard.

Related to the control action (scenario categories 2.1. and 2.2.)

- LS-31: The acceleration control action is improper executed due to engine failure [H-1]
- LS-32: The acceleration control action is improper executed because the lever sticks, so acceleration is less or too much provided. [H-1]
- LS-33: Environmental factors, like a slope in the track, can cause the vehicle to drive too fast without acceleration. [H-1]
- LS-34: Environmental factors, like a slippery track, can cause a lack of acceleration. [H-1]

Loss Scenarios for braking

Related to UCA-11 (scenario categories 1.1. and 1.2.)

- LS-35: Driver does not provide the brake while train drives harder than permitted speed, because the speed profile indicates a slower speed than the actual speed, this can be caused by a malfunctioning odometry
- LS-36: Driver does not provide the brake while train drives harder than permitted speed, because past experience makes the driver think the train is coming from the same direction and the driver stops at the wrong place of the combining track.
- LS-37: Driver does not provide the brake while train drives harder than permitted speed, because the driver thinks that the train has a different length than the actual length and does not brake, due to habituation of driving with another length of the train on the same track.
- LS-38: Driver does not provide the brake while train drives harder than permitted speed, because the signage along the track is misinterpreted by the driver.

Related to UCA-12 (scenario categories 1.1. and 1.2.)

- LS-39: Driver provides the brake while train drives slower than or at the permitted speed, because the speed profile indicates a faster speed than the actual speed, this can be caused by a malfunctioning odometry

Related to UCA-13 (scenario categories 1.1. and 1.2.)

- LS-40: Driver provides the brake with an insufficient level of braking while train drives harder than permitted speed, because the driver is used to drive with other trains (a lighter/shorter train for example), which makes the driver think that the train can brake faster.

- LS-41: Driver provides the brake with an insufficient level of braking while train drives harder than permitted speed, because the speed profile indicates a slower speed than the actual speed, this can be caused by a malfunctioning odometry.

Related to UCA-14 (scenario categories 1.1. and 1.2.)

- LS-42: Driver provides the brake and stops the train before the train is in the right position in the combining track, because it is not clear for the driver where to stop exactly on the combining track. The driver can be used to combining with trains coming from the same direction, instead of combining with trains coming from opposite directions. The first driver often does not know in which direction the second train is arriving from.

Related to UCA-15 (scenario categories 1.1. and 1.2.)

- LS-43: Driver provides the brake too late (>TBD seconds) after driver receives speeding warning, because the driver is distracted and the warning sound is broken/not heard.

Related to UCA-16 (scenario categories 1.1. and 1.2.)

- LS-44: Driver stopped too soon with braking, while train is not yet standing still in the combining track, because the driver is used to drive with other trains (a lighter/shorter train for example), which makes the driver think that the train is already getting to the desired speed.
- LS-45: Driver stopped too soon with braking, while train is not yet standing still in the combining track, because the speed profile indicates no speed but the train still drives slowly, this can be caused by a malfunctioning odometry.

Related to the control action (scenario categories 2.1. and 2.2.)

- LS-46: The brake control action is improper executed due to engine failure [H-1]
- LS-47: The brake control action is improper executed because the lever sticks, so acceleration is less or too much provided. [H-1]
- LS-48: Environmental factors, like a slippery track, can cause a lack of deceleration. [H-1]

Loss Scenarios for confirming OSMA

Related to UCA-17 (scenario categories 1.1. and 1.2.)

- LS-49: Driver does not confirm OSMA, while train system suggests applying OSMA on the DMI and train drives into combining track, because the driver thinks that the combine track is positioned further away, due to experiences of other combine tracks on other platforms.
- LS-50: Driver does not confirm OSMA, while train system suggests applying OSMA on the DMI and train drives into combining track, because the driver does not pay attention to the DMI and the sound for new notifications on the DMI is missed or interpreted as a sound for another notification.
- LS-51: Driver does not confirm OSMA, while train system suggests applying OSMA on the DMI and train drives into combining track, because the driver is distracted by other messages on the control table or from outside, causing the driver to forget to confirm.

Related to the control action (scenario categories 2.1. and 2.2.)

- LS-52: Confirming OSMA is not executed, because the DMI touchscreen broke or is not sensitive enough for dirty/greasy/wet fingers. [H-2]

Loss Scenarios for switching the control current off

Related to UCA-18 (scenario categories 1.1. and 1.2.)

- LS-53: Driver does not switch the control current off, while the driver leaves the cab, because the driver is used to other trains and does not know how to switch of the control current of its train.
- LS-54: Driver does not switch the control current off, while the driver leaves the cab, because the driver is in a hurry and forgets it. No warning is given when driver leaves the cab

Related to UCA-19 (scenario categories 1.1. and 1.2.)

- LS-55: Driver switches the control current off, while the train still needs to be operated, because the accidently touched it or mistake it with another function.
- LS-56: Driver switches the control current off, while the train still needs to be operated, because the driver 1 thinks that the other train comes from the same direction to combine the trains. In the procedure for this other user process (user process 50), driver 1 switches its control current off if the train is standing still. So, both driver are switching its control current off and the trains cannot be combined. The first driver does not know in which direction the second train is arriving from.

Related to the control action (scenario categories 2.1. and 2.2.)

- LS-57: Switching of the control current is not executed, because the switch broke. [H-1]

Loss Scenarios for combining trains

Related to UCA-20 (scenario categories 1.1. and 1.2.)

- LS-58: Driver does not combine trains, while both trains are ready to combine, because driver 1 mixes up procedures (user process 48 and 50) and expects the other driver to combine the trains.
- LS-59: Driver does not combine trains, while both trains are ready to combine, because driver 1 does not know if train 2 is ready to combine (for example, if the control current is switched off)

Related to UCA-21 (scenario categories 1.1. and 1.2.)

- LS-60: Driver combines train while not following the combining procedure, because the type of train is different than usual and the driver is used to a different procedure.

Related to UCA-22 (scenario categories 1.1. and 1.2.)

- LS-61: Driver combines trains too early, while not all actions for preparations are done, because driver 1 does not know if train 2 is ready to combine (for example, if the control current is switched off)

Related to UCA-23 (scenario categories 1.1. and 1.2.)

- LS-62: Driver stopping too soon with combining trains, while not all combining actions are done, because the type of train is different than usual and the driver is used to a different procedure.
- LS-63: Driver stopping too soon with combining trains, while not all combining actions are done, because the driver receives only visual feedback of the physical state of the coupling and thinks that the trains are combined. Insufficient feedback is received by the driver.

Related to the control action (scenario categories 2.1. and 2.2.)

- LS-64: Combining trains is executed incorrect, causing incorrectly connected trains (for example, the electromechanical parts are not connected properly). [H-1]

Loss Scenarios for providing an OSMA

Related to UCA-24 (scenario categories 1.1. and 1.2.)

- LS-65: Trackside system not providing an OSMA while the train is ready to drive in the combining track, because RBC, IXL or GSM-R is malfunctioning.
- LS-66: Trackside system not providing an OSMA while the train is ready to drive in the combining track, because the train system sends a position report that indicates that the train is moving, but in reality, the train is standing still. This can be caused by an odometry error.

Related to UCA-25 (scenario categories 1.1. and 1.2.)

- LS-67: Trackside system providing an OSMA for the wrong track, because of a configuration error between procesleiding and the central safety system.

Related to the control action (scenario categories 2.1. and 2.2.)

- LS-68: Providing an OSMA is not executed due to GSM-R errors and information is partially/not transmitted. Those errors can be caused by power failure, hacking or interventions by jammers (for example 5G transmitters)[H-2]

Loss Scenarios for disconnecting the train from the RBC

Related to UCA-26 (scenario categories 1.1. and 1.2.)

- LS-69: Trackside system does not disconnect the train from the RBC, while the control current is shut off, because the End of mission is not received by the trackside system, due to GSM-R errors or train system not sending it.

Related to UCA-27 (scenario categories 1.1. and 1.2.)

- LS-70: Trackside system disconnects train from RBC, while the train is still operated by the driver, because connection between train and trackside system is disconnected (>TBD seconds) due to a GSM-R error.

Appendix H.

Interview protocol (in Dutch)

Bedankt voor het vrijmaken van tijd om mij te helpen voor dit afstudeeronderzoek. Dit interview neem ik graag op, om tijdens het interview goed te kunnen luisteren en achteraf pas te noteren wat er is geantwoord op de vragen. Deze opname zal alleen voor mijzelf bewaard worden en na transcriberen verwijderd worden. Alle geciteerde antwoorden zullen geanonimiseerd worden in het verslag.

Voorstellen

Ik studeer aan de TU Delft en ben momenteel de master Construction Management and Engineering aan het afronden, dit is een master die voortkomt uit de studies civiele techniek, bouwkunde en technisch bestuurskunde. Binnen de programmadirectie ERTMS mag ik een afstudeer opdracht doen over het aantonen van de betrouwbaarheid van het spoor vervoersysteem met ERTMS. Hierbij focus ik me voornamelijk op de interacties tussen ETCS, machinisten en treindienstleiders en de risico's die daarin treinvertragingsminuten kunnen veroorzaken. Hierbij kijk ik of de risicoanalyse methode STPA (Systems Theoretic Process Analysis) geschikt is om nieuwe risico's te identificeren en hoe dit dan toegepast kan worden binnen de programmadirectie ERTMS.

Doel interview

Het doel van dit interview is om ervaringen van het gebruik van STPA te verzamelen en onderzoeken wat ervaringsdeskundigen adviseren over hoe STPA toegepast kan worden binnen het spoor vervoersysteem met ERTMS.

Structuur interview

Het interview is onderverdeeld in drie stukken, eerst zal praktische achtergrond informatie gevraagd worden, om vervolgens in te gaan op een terugblik van de ervaringen die je hebt met STPA. Het interview sluit af met vragen over hoe STPA toegepast kan worden binnen het spoor vervoersysteem met ERTMS.

Mocht de beschikbare tijd voor het interview beginnen te dringen, dan zullen we een aantal vragen overslaan. Vier vragen zijn aangeduid met een P van prioriteit en zullen in ieder geval gevraagd worden.

1. Praktische informatie [10 min.]

- Datum:
- Naam:
- Werkervaring (projecten, jaren actief)
  - In het spoor:
  - Met betrouwbaarheid/risico analyse:
  - Met STPA:

2. Terugblik op STPA ervaringen [40 min.]

1. Waarom ben je begonnen met STPA te gebruiken?
2. Waarom vervolgens er ook weer mee gestopt? (of: Waarom gebruik je nog steeds STPA?)
3. Wat vond je het grootste voordeel van STPA? (eventueel in vergelijking met traditionele gevaren analyses als FMEA)
4. Wat vond je het grootste nadeel van STPA? (eventueel in vergelijking met traditionele gevaren analyses als FMEA)
5. **P:** Wat zijn de grootste lessen die je hebt geleerd door het toepassen van STPA?
6. Vond je STPA complex om te leren en uit te voeren als 'STPA leek'?
7. Hoeveel tijd en aandacht was je kwijt aan elke STPA stap? (1. Define purpose, 2. model control structure, 3. identify unsafe control actions, 4. identify loss scenarios)
8. (Wanneer STPA is vergeleken met een andere risico analyse.) Hebben jullie ervaren dat er nieuwe scenario's waren ontdekt die konden lijden tot verliezen. Of waren de (scenario's naar) gevaren al geheel bekend? Wat voor scenario's waren dat? (software/interacties/product/menselijk falen)
9. Hebben jullie tips voor het praktisch toepassen van de STPA uitkomsten? Waardoor je de geïdentificeerde gevaren kan mitigeren?

3. STPA toepassen binnen het spoor vervoersysteem met ERTMS [40 min.]

10. **P:** Wat zijn de succesfactoren om STPA te doen slagen binnen een organisatie? (uit praktijkervaring)
11. **P:** Welke onderdelen van het vervoerssysteem met ERTMS zijn de inspanning van STPA waard en welke onderdelen kunnen beter met andere technieken gedaan worden? (denk aan gebruikersprocessen, het gehele socio-technische vervoersysteem of technische systemen) Waarom?
12. Welke expertise moet je minimaal hebben voor het uitvoeren van STPA?
13. Hoe kan je STPA praktisch uitvoeren als je zelf niet (volledig) expert bent in het systeem of (gebruikers)proces dat je analyseert?
14. Hoe kan je het beste experts (voorbeeld: gebruikersprocessen experts zoals ontwikkelaars van gebruikersprocessen of ervaringsdeskundigen) betrekken bij STPA als ze STPA niet kennen?
15. **P:** Vind je dat de tijd/inspanning die STPA kost het waard om naast traditionele (huidige) gevarenanalyses ook STPA uit te voeren voor onontdekte faalscenario's?
16. Kan STPA de traditionele (huidige) gevarenanalyses volledig vervangen?

Afsluiting

Bedankt voor je tijd! Wanneer het onderzoek is afgerond zal ik een kopie toesturen.

Appendix I.

Interview transcripts (in Dutch)

Interview 1:

1. Praktische informatie

- Datum: 10-08-2022
- Werkervaring (projecten, jaren actief)
    - In het spoor:

Sinds eind 1990, vrijwel altijd voor Prorail met ERTMS.

- Met betrouwbaarheid/risico analyse:

Sinds 2000 en dan met name veiligheidsrisico's.

- Met STPA:

Sinds 2013 volg ik STPA. In 2015 heb ik STPA uitgeprobeerd op de ERTMS lijn de Hanzenlijn en gekeken naar tijdelijke snelheidsbeperkingen. Eerst heb ik de tijdelijke snelheidsbeperkingen helemaal uitgewerkt volgens de huidige methodes en toen heb ik geprobeerd om het nog een keer na te doen met STPA. Ik wist al ongeveer wat de uitkomst was en daarnaast speelde er een pilot op Amsterdam Utrecht waar er een tijdelijke snelheidsbeperking in de praktijk uitgeprobeerd was. Er werd daar gekeken of dat nou allemaal werkte zoals de procedures waren bedacht en ik wist ook al wel wat daaruit gekomen was en wat daar mis was gegaan. Dus Ik kan niet zeggen dat ik helemaal blanco met STPA bezig was. Dus dat bederft het experiment wel een beetje, maar het was voor mij om een beetje gevoel te krijgen hoe het nou werkte.

In 2021 uitgeprobeerd voor een Movares project. Hiervoor heb ik lessons learned uitgeschreven ter behoeve van een presentatie op de STAMP workshop 2021. We mochten deze presentatie helaas niet geven, omdat het project gestopt is.

Op dit moment pas ik het deels toe voor menselijk falen van treindienstleiders in het kader van verwarring procedures met ERTMS en bestaande baanvakken. Ik gebruik dan met name stap 3 van STPA. En ik heb me verdiept in de uitbreiding op STPA voor menselijk falen

2. Terugblik op STPA ervaringen

1. Waarom ben je begonnen met STPA te gebruiken?

Ik was eigenlijk aan het kijken naar methodes voor incident onderzoek en toen kwam ik STAMP tegen en STAMP heeft ook een tak voor incident onderzoek, CAST heet dat. Ik vind het gewoon leuk om nieuwe dingen uit te proberen, dus daarom ben ik ermee begonnen toen. Het leek ook wel een hele andere methode dan we tot dat moment gebruikten, dus Ik was heel benieuwd hoe het zou werken.

2. Waarom gebruik je nog steeds/weer STPA?

Ik gebruik het soms als ik de meerwaarde zie. Bijvoorbeeld als ik zie dat de veiligheidsrisico's beheerst worden door verschillende controllers en ik mogelijkheden zie om daarvoor een controlestructuur uit te schrijven.

Maar ik heb ook heel veel projecten waar ik STPA helemaal niet kan toepassen. Bijvoorbeeld wanneer je de ProRail voorschriften moet volgen. Of als je kijkt of iets veilig is met een kleine afwijking t.o.v. de ProRail voorschriften, daar is STPA niet geschikt voor.

3. Wat vond je het grootste voordeel van STPA? (eventueel in vergelijking met traditionele gevaren analyses als FMEA)

Ik vind STPA handig omdat het heel erg gestructureerd is. Aan het begin al met het opschrijven van losses. Het gaat zo gestructureerd, stapje voor stapje, mijn idee is dat je er niet omheen kan dat je het allemaal heel gestructureerd uitwerkt en dat je daardoor ook heel goed in beeld krijgt welke hazards er zijn en bijbehorende achterliggende oorzaken

Bij andere methodes ga je er veel oppervlakkiger overheen. Je begint vaak niet met het opschrijven van de losses en je zoekt niet zo gestructureerd naar oorzaken. Je doet dit wel bij andere methodes, maar veel korter. Je kijkt ook naar de invloed van de omgeving dat zie ik ook in geen enkele andere methode terug.

4. Wat vond je het grootste nadeel van STPA? (eventueel in vergelijking met traditionele gevaren analyses, bijvoorbeeld FMEA)

Het is veel werk. En het is lastig om een goede controle structuur op te zetten. En bij stap 4 genereerde het een ontzettende hoop loss scenario's waar veel dingen dubbel in zaten dus misschien heb ik dat niet handig aangepakt. Het werkt wel maar je moet je wel door een hele berg scenario's heen worstelen.

5. **P:** Wat zijn de grootste lessen die je hebt geleerd door het toepassen van STPA?

Opgestelde lessons learned:

Lesson 1: write down and periodically check all assumptions for not yet existing systems.
Lesson 2: make a good decision on the scope of the system (only inside what can be controlled).
Lesson 3: draw a good hierarchical control structure.
Lesson 4: make sure that you do not included similar unsafe control actions.
Lesson 5: check whether unsafe control actions or control actions should be used for the scenarios.
Lesson 6: put loss scenarios in a separate table and refer to this table.
Lesson 7: search for 2. causes of inadequate feedback/information during substep 1d. inadequate process model.
Lesson 8: be critical while working on scenarios for 3. control path and 4. scenarios related to the controlled process and postpone scenarios that depend on the actual implementation.
Lesson 9: before asking experts to contribute to the loss scenarios decide on the information shared during a meeting, e.g. the control structure.

6. Vond je STPA complex om te leren en uit te voeren als 'STPA leek'?

Ik worstelde vooral met die controlestructuur, als je dat niet goed hebt dan kom je ook niet verder.

Ik had toen niet helemaal door dat je STPA niet voor alle projecten zomaar toe kan passen. Je moet echt even goed nadenken of het überhaupt zin heeft. Bijvoorbeeld waar gebruikersprocessen een rol spelen en waar je verschillende partijen hebt die mee bijdrage aan het veilig houden van de hele situatie, daar is het goed toepasbaar.

En je raakt gemakkelijk het overzicht kwijt doordat je veel dezelfde loss scenarios krijgt bij het uitwerken van STPA.

7. Hoeveel tijd en aandacht was je kwijt aan elke STPA stap? (1. Define purpose, 2. model control structure, 3. identify unsafe control actions, 4. identify loss scenarios)

Ik was vooral veel tijd kwijt aan de controle structuur (stap 2) en aan het uitwerken van de loss scenarios (stap 4). Probeer overlap in de verschillende geïdentificeerde loss scenario's te voorkomen.

8. (Wanneer STPA is vergeleken met een andere risico analyse.) Heb je ervaren dat er nieuwe scenario's waren ontdekt die konden leiden tot verliezen? Of waren de (scenario's naar) gevaren al geheel bekend? Wat voor scenario's waren dat? (software/interacties/product/menselijk falen)

Omdat ik in 2015 al wist wat er allemaal mis was gegaan door de uitkomsten van de pilot, was ik beïnvloed en ik kan uit ervaring dus nog niet zeggen dat STPA echt nieuwe loss scenario's vindt.

9. Heb je tips voor het praktisch toepassen van de STPA uitkomsten? Waardoor je de geïdentificeerde gevaren kan mitigeren?

Volgens mij biedt de methode daar inderdaad geen oplossingen voor.

Ik heb in het begin van mijn safety carrière een cursus gevolgd waarin 7 stappen werden aangegeven voor veiligheidsanalyses en de laatste 3 stappen ging dan over het bedenken van oplossingen, maar daar komt STPA helemaal niet aan toe. STPA stopt als je de oorzaken hebt gevonden en ze bieden zelfs ook niet een soort ranking van welke loss scenario erger is dan de andere.

Er zijn 4 niveaus om gevaar te mitigeren zeg. Het beste is om de bron van het gevaar weg te nemen en de slechtste is dat je persoonlijke beveiligingsmiddelen gaat gebruiken om te zorgen dat je niet zo erg gewond raakt. Deze niveaus van mitigeren kan je leggen naast de oorzaken en kijken welke je dan kan gebruiken. Je kan elke loss scenario langs gaan en beslissen welke niveau van mitigatie toepasbaar is.

3. STPA toepassen binnen het spoor vervoersysteem met ERTMS [40 min.]

10. **P:** Wat zijn de succesfactoren om STPA te doen slagen binnen een organisatie? (uit praktijkervaring)

Je moet zorgen dat een paar mensen goed opgeleid zijn in STPA. Je moet de inhoudelijke experts (niet de STPA mensen) een beetje beschermen tegen alle details van STPA. STPA moet een vertaalslag krijgen voor de inhoudelijke experts, dan kan het wel goed werken. Ik zou zelf de controle structuur goed uitwerken en bij stap 4 experts betrekken. De experts dan niet lastig vallen met alle details van de methode.

Echte praktijkervaring heb ik alleen bij mijn huidige project. Daar gebruiken we stap 4 van de methode niet, omdat we heel specifiek naar bepaalde oorzaken zoeken. We gebruiken daar juist alleen stap 3 (identify unsafe control actions) waarbij we alle controle acties door treindienstleiders onderzoeken.

11. **P:** Welke onderdelen van het vervoerssysteem met ERTMS zijn de inspanning van STPA waard en welke onderdelen kunnen beter met andere technieken gedaan worden? (denk aan

gebruikersprocessen, het gehele socio-technische vervoersysteem of technische systemen) Waarom?

De gebruikersprocessen, omdat daarin juist de verschillende controllers al goed tot uiting komen.

Het ligt ook een beetje aan je doel, welke lagen wil je in detail bestuderen?

12. Welke expertise moet je minimaal hebben voor het uitvoeren van STPA?

Enige ervaring en praktische kennis met vergelijkbare methoden, bijvoorbeeld HAZOP. Dat je dat hebt uitgevoerd en geleid, dan heb je een beetje het gevoel van hoe je dat aanpakt. Dat je ervoor zorgt dat er geen spraakverwarring krijgt bij het uitvoeren van een STPA sessie met experts. En praktische kennis, dat je weet met hoeveel mensen je moet zitten om de analyse uit te voeren.

13. Hoe kan je STPA praktisch uitvoeren als je zelf niet (volledig) expert bent in het systeem of (gebruikers)proces dat je analyseert?

Zelf het voorwerk doen maar iedere keer bij die experts vragen of het nou klopt.

Stap 4 zou je het beste met experts uit kunnen voeren, maar dan moet je wel misschien keuzes maken dat je een paar stukken van die stap 4 overslaat als je veel aannames moet doen.

14. Hoe kan je het beste experts (voorbeeld: gebruikersprocessen experts zoals ontwikkelaars van gebruikersprocessen of ervaringsdeskundigen) betrekken bij STPA als ze STPA niet kennen?

Ik heb in mijn huidige project in het plan van aanpak een klein beetje uitleg gegeven over STPA.

15. **P:** Vind je dat de tijd/inspanning die STPA kost het waard om naast traditionele (huidige) gevarenanalyses ook STPA uit te voeren voor onontdekte faalscenario's?

Ja, maar je moet een beetje kritisch zijn in welke project dat dan wel of niet zinnig is.

Het is wel de enige methode die de omgeving ook echt expliciet beschouwt en is ook de enige methode die zo gestructureerd naar oorzaken zoekt, voor zover ik weet. Voor mijn gevoel is het wel de moeite waard, maar ik kan het niet onderbouwen met gevonden onontdekte faalscenario's.

16. Kan STPA de traditionele (huidige) gevarenanalyses volledig vervangen?

Nee. STPA biedt bijvoorbeeld geen enkele ondersteuning voor het kwantificeren van risico's. Zie onderstaande stappen van Yellow Book. Er is geen ondersteuning voor stap 5, 6 en 7. STPA kan allen voor de eerste 4 stappen gebruikt worden.

Op basis van het Yellow Book:

1. Systeemgrenzen bepalen
2. Hazardidentificatie
3. Oorzakenanalyse
4. Gevolganalyse
5. Beoordeling risico (risicomatrix)
6. Eventuele maatregelen bepalen
7. Nieuwe beoordeling risico

Interview 2:

1. Praktische informatie

- Datum: 10 augustus 2022
- Werkervaring (projecten, jaren actief)
    - In het spoor:

17 jaar

- Met betrouwbaarheid/risico analyse:

Richting de 20 jaar

- Met STPA:

Ik ken de methode STPA al heel wat jaren, maar nooit echt gebruik van gemaakt, tot 4 jaar geleden. Afgelopen 4 jaar ben ik gaan stoeien met de methode. Vooral gekeken naar STPA als modeleringstechniek, vooral om de gehele vervoersketen in beeld te brengen. Hierbij heb ik STPA niet tot in de laatste stap uitvoerig uitgevoerd, alleen de eerste twee stappen.

2. Terugblik op STPA ervaringen

1. Waarom ben je begonnen met STPA te gebruiken?

Om de architectuur van de gehele vervoersketen in kaart te brengen. Om vervolgens analyse erop toe te kunnen passen.

2. Waarom vervolgens er ook weer mee gestopt?

De typen hazards of risico's die we tegenkwamen waren voor mijn gevoel redelijk triviaal, terwijl je juist meer diepgang wilt bereiken met een veiligheidsanalyse of betrouwbaarheidsanalyse. De wijze waarop het in kaart wordt gebracht, hoe je controle loops ontwikkeld maakt de analyse voor mijn gevoel niet diep genoeg gaat. Zoals ze zeggen, you are scratching the surface.

3. Wat vond je het grootste voordeel van STPA? (eventueel in vergelijking met traditionele gevaren analyses als FMEA)

Als je kijkt naar analyses zoals FMEA of HAZOP, daar heb je een object nodig om die analyse te kunnen doen. STPA biedt jouw een model van domeinen die je wil onderzoeken, bijvoorbeeld met het vervoersysteem, dat doet FMEA of HAZOP niet. Die zijn altijd gericht op een object, je hebt een beschrijving waarop ik mijn analyse loslaat en STPA beetje de kans op dat systeem in beeld te brengen.

Modeleren is zeker een voordeel van STPA, als het gaat om het hoge abstractie niveau van de ERTMS programmadirectie

4. Wat vond je het grootste nadeel van STPA? (eventueel in vergelijking met traditionele gevaren analyses als FMEA)

Niet een nadeel, maar meer een uitdaging. De uitdaging is dat jouw model dusdanig rijk is aan informatie, dat je een betekenisvol analyse kan doen. Een model met weinig detail in de controle loops voegen niet veel toe aan risico's voor mijn gevoel.

Ik blijf erbij dat de echte diepgaande van de analyse ontbreekt.

5. **P:** Wat zijn de grootste lessen die je hebt geleerd door het toepassen van STPA?

Als het gaat over het in kaart brengen van een heel diffuus systeem zoals het vervoerssysteem in Nederland en dat gepositioneerd in een Europees context, dat STPA daar je goed bij kan helpen.

Als ik een bepaalde node of een bepaalde controlelus wil analyseren dat ik daarvoor andere technieken zou gebruiken. Dan zal ik eerder naar bijvoorbeeld FRAM kijken (een methode van Erik Hollnagel) daar kan je veel nauwkeuriger zo een keten modeleren.

Ik heb geleerd wat de grenzen zijn van STPA en wanneer ik beter naar een andere methode kan gaan.

6. Vond je STPA complex om te leren en uit te voeren als 'STPA leek'?

Ik ben eigenlijk een purist. Ik wil technieken goed snappen en correct toepassen, STPA is lastiger dan andere technieken die ik in het verleden heb gebruikt. FRAM is daar iets toegankelijker in, maar ook niet eenvoudig. Ieder techniek kost gewoon de nodige tijd om het te leren. Tegelijkertijd moet ik ook terugdenken aan een van mijn docenten aan de TU Delft, haar stelling was over STPA: don't try this at home.

Als je iets heel eenvoudigs pakt, zoals hoe ga ik brood roosteren en je pakt dat als proces, dan is het eenvoudiger om dat te modeleren in FRAM dan in STPA.

7. Hoeveel tijd en aandacht was je kwijt aan elke STPA stap? (1. Define purpose, 2. model control structure, 3. identify unsafe control actions, 4. identify loss scenarios)

Er gaat heel veel tijd in de controle structuur, dus stap twee. Bijvoorbeeld voor het gehele vervoersysteem modeleren door eerste een basismodel neer te zetten in een dag en dan ga je het nog verfijnen, dat kost gewoon nog een dag of twee. We hebben dit model nooit volledig doorgenomen, omdat het niet het doel was om alles door te nemen, dat gaat dat gaat gewoon heel veel tijd kosten, afhankelijk van de grootte van je model.

Je kan bijvoorbeeld inzoomen op de relatie tussen treindienstleider en machinist, dan ben je gewoon een paar dagen ermee bezig. Stap 1, defining the purpose is heel belangrijk om genoeg tijd in te stoppen.

Stap 3 en 4 van STPA heb ik nooit ten volle uitgewerkt. Ik heb ook nog nooit voorbeelden gezien van STPA die ten volle is uitgevoerd.

8. (Wanneer STPA is vergeleken met een andere risico analyse.) Hebben je ervaren dat er nieuwe scenario's waren ontdekt die konden lijden tot verliezen. Of waren de (scenario's naar) gevaren al geheel bekend? Wat voor scenario's waren dat? (software/interacties/product/menselijk falen)

Niet van toepassing, omdat de laatste twee stappen van STPA niet uitvoerig zijn uitgevoerd.

9. Hebben jullie tips voor het praktisch toepassen van de STPA uitkomsten? Waardoor je de geïdentificeerde gevaren kan mitigeren?

Ik maak veel gebruik de analysetechniek prisma. Deze classificeerd in termen van techniek, organisatie en mens. Vanuit de mens dan in termen van skill based, rule based and knowledge based fouten en vervolgens een bijbehorende maatregelen daar tegenover zetten. De classificatie actie matrix laat zien wat je in de techniek moet oplossen wat ik in de opleidingen moet doen en wat moet ik in de instructies moet veranderen.

Ik vind STPA heel krachtig als praatplaatje om een systeem goed in beeld te brengen.

3. STPA toepassen binnen het spoor vervoersysteem met ERTMS [40 min.]

10. **P:** Wat zijn de succesfactoren om STPA te doen slagen binnen een organisatie? (uit praktijkervaring)

Dan heb je een STPA goeroe nodig, iemand die het echt tot in de haarvaten goed kent. Diegene moet kunnen zeggen dat wat hier staat ook klopt en ervaring heeft met projecten waar STPA op is toegepast.

Ik vrees dat deze STPA goeroes niet zullen komen. Er zijn in de loop der jaren honderden analyse technieken ontwikkeld. Waarom worden er dan nog steeds maar 4, 5, 6 technieken gebruikt? Dit zijn technieken die zich hebben bewezen en men kent en echt snapt en waar men van overtuigd is dat deze resultaten leveren die we nodig.

STPA zie ik als een goede methode om inzicht te bieden in een complex systeem, maar niet krachtig genoeg om een goede analyse te doen met alleen maar 4 unsafe control action types.

11. **P:** Welke onderdelen van het vervoerssysteem met ERTMS zijn de inspanning van STPA waard en welke onderdelen kunnen beter met andere technieken gedaan worden? (denk aan gebruikersprocessen, het gehele socio-technische vervoersysteem of technische systemen) Waarom?

Eerst jezelf afvragen, welke delen van het vervoersysteem wil ik op een diepgaand niveau gaan analyseren, voor grote overkoepelende systemen, zoals het vervoersysteem kan je STPA gebruiken.

Voor interacties op gebruikersniveau, daar is je abstractie niveau in het model te beperkt voor. Mijn onderbuikgevoel zegt dat STPA toepassen op gebruikersprocessen niets anders oplevert dan wanneer ik de stappen vanuit de gebruiksprocessen aan zich ga beschouwen (met bijvoorbeeld een HAZOP).

Wanneer processen ontwikkeld worden, zoals gebruikersprocessen voor ATO, dan is STPA wel heel interessant. STPA kan een goede brugfunctie vormen tussen het abstracte of nog niet beschreven werkelijkheid en de uiteindelijke gedetailleerde gebruikersproces.

12. Welke expertise moet je minimaal hebben voor het uitvoeren van STPA?

Twee soorten personen nodig, diegene die echt STPA begrijpt en kan begeleiden en anderzijds heb je de domeinkennis nodig.

13. Hoe kan je STPA praktisch uitvoeren als je zelf niet (volledig) expert bent in het systeem of (gebruikers)proces dat je analyseert?

Gebruik experts op het domein.

14. Hoe kan je het beste experts (voorbeeld: gebruikersprocessen experts zoals ontwikkelaars van gebruikersprocessen of ervaringsdeskundigen) betrekken bij STPA als ze STPA niet kennen?

Kort uitleggen wat het doel van de STPA is en hoe het model opgebouwd wordt. Geef een eenvoudig voorbeeld om de regels uit te leggen.

15. **P:** Vind je dat de tijd/inspanning die STPA kost het waard om naast traditionele (huidige) gevarenanalyses ook STPA uit te voeren voor onontdekte faalscenario's?

Ik denk dat het je kan helpen om nog onontdekte faal scenario's te identificeren voor domeinen die minder goed bekend zijn. Bijvoorbeeld niet voor de huidige gebruikersprocessen, maar wel voor analyses voor systemen met ATO.

16. Kan STPA de traditionele (huidige) gevarenanalyses volledig vervangen?

Nee. Er is geen classificatie van de risico's, een risicomatrix met kans en ernst is in ieder geval nodig.

Interview 3:

1. Praktische informatie

- Datum: 10 augustus 2022
- Werkervaring (projecten, jaren actief)
  - In het spoor:

36 jaar

- Met betrouwbaarheid/risico analyse:

16 jaar

- Met STPA:

In 2015/2016 STPA gedaan op twee gebruikersprocessen

2. Terugblik op STPA ervaringen

1. Waarom ben je begonnen met STPA te gebruiken?

Samen met collega's van mijn vorige werkgever gekeken of STPA aangeboden kon worden door dat ingenieursbureau.

2. Waarom vervolgens er ook weer mee gestopt?

Binnen ProRail waren er geen mensen die STPA uitvoerden en het was ook lastig uit te leggen aan anderen, want het is een andere methode en heeft andere definities. Ook na verschillende presentaties en uitleggen sloeg het niet aan binnen de organisatie.

3. Wat vond je het grootste voordeel van STPA? (eventueel in vergelijking met traditionele gevaren analyses als FMEA)

De gestructureerde methode, werken met scenario's en de controle structuur opzetten laat snel zien waar geen/weinig feedback is.

4. Wat vond je het grootste nadeel van STPA? (eventueel in vergelijking met traditionele gevaren analyses als FMEA)

Grootste nadeel is dat collega's er niet bekend mee zijn.

De fouten die gemaakt kunnen worden in het opstellen van de control structuur, als deze fout gaat, dan gaat de rest van de analyse ook fout. Fouten in het begin lijden tot fouten aan het eind van de analyse.

5. **P:** Wat zijn de grootste lessen die je hebt geleerd door het toepassen van STPA?

Dat je door het modeleren van de controle structuur al ziet of er feedback mist. Daarnaast leer je goed het systeemdenken de systeem filosofie achter de hele methode.

6. Vond je STPA complex om te leren en uit te voeren als ‘STPA leek’?

Na het kijken van STPA tutorials denk je dat je het wel snapt, maar het is wel lastig als je het dan daadwerkelijk zelf gaat uitvoeren. Er zijn nu geen andere experts die de methode kennen, dus je moet alles helemaal zelf uitzoeken.

7. Hoeveel tijd en aandacht was je kwijt aan elke STPA stap? (1. Define purpose, 2. model control structure, 3. identify unsafe control actions, 4. identify loss scenarios)

Ik denk het identificeren van unsafe control actions en de scenario’s (stap 3 en 4), meer dan de eerste twee.

8. (Wanneer STPA is vergeleken met een andere risico analyse.) Heb je ervaren dat er nieuwe scenario's waren ontdekt die konden lijden tot verliezen. Of waren de (scenario's naar) gevaren al geheel bekend? Wat voor scenario’s waren dat? (software/interacties/product/menselijk falen)

Ik heb de processen niet met een andere risicoanalyse vergeleken.

9. Heb je tips voor het praktisch toepassen van de STPA uitkomsten? Waardoor je de geïdentificeerde gevaren kan mitigeren?

Je kan gebruik maken van een hazardlog. Hierin worden de hazard gedefinieerd, die hazards mitigeren we met maatregelen. Dat kunnen verschillende type maatregelen zijn, zoals eisen of procedures aanpassen.

3. STPA toepassen binnen het spoor vervoersysteem met ERTMS

10. **P:** Wat zijn de succesfactoren om STPA te doen slagen binnen een organisatie? (uit praktijkervaring)

Als de organisatie de methode accepteert en als mogelijkheid aanbiedt. Dat er genoeg collega's zijn die ervaring mogen opdoen en ermee aan de slag kunnen gaan. STPA moet de organisatie overtuigen dat het zijn tijd en geld waard is.

11. **P:** Welke onderdelen van het vervoerssysteem met ERTMS zijn de inspanning van STPA waard en welke onderdelen kunnen beter met andere technieken gedaan worden? (denk aan gebruikersprocessen, het gehele socio-technische vervoersysteem of technische systemen) Waarom?

Systemen waarbij je zelf verantwoordelijk voor bent, die je laat ontwikkelen en specificaties voor opstelt. Bij wet en regelgeving heb je zelf weinig invloed en is STPA dus ook minder bruikbaar voor.

12. Welke expertise moet je minimaal hebben voor het uitvoeren van STPA?

Kennis van STPA, kennis van veiligheidsanalyses, kennis van RAM en de systemen waar je naar kijkt.

13. Hoe kan je STPA praktisch uitvoeren als je zelf niet (volledig) expert bent in het systeem of (gebruikers)proces dat je analyseert?

Experts in het systeem, maar ook juist mensen die niet expert zijn uitnodigen. Soms heb je misschien mensen nodig die niet volledige kennis hebben over een proces, maar wel nieuwsgierig en kritisch zijn. Die kunnen dan zogenaamde domme vraag stellen, maar die eigenlijk juist heel slim zijn, omdat experts deze vanzelfsprekend achten.

14. Hoe kan je het beste experts (voorbeeld: gebruikersprocessen experts zoals ontwikkelaars van gebruikersprocessen of ervaringsdeskundigen) betrekken bij STPA als ze STPA niet kennen?

Betrekken bij het bedenken van scenario's de controle structuur. Uitleggen wat STPA is en welke stappen gezet moeten worden (hetzelfde als bij andere methodes, zoals bij FMECA of HAZOP).

15. **P:** Vind je dat de tijd/inspanning die STPA kost het waard om naast traditionele (huidige) gevarenanalyses ook STPA uit te voeren voor onontdekte faalscenario's?

Dan doe je dingen extra, volgens STPA vindt je dan toch nog nieuwe scenario's van hoe iets mis kan gaan.

16. Kan STPA de traditionele (huidige) gevarenanalyses volledig vervangen?

Volgens de bedenkers wel. Ik vond in het begin (in 2015) wel dat STPA nog in ontwikkeling was, maar durf nu niet te zeggen of dat nog steeds zo is.

Ik denk dat het toegepast kan worden binnen ProRail, maar dan moet het wel geaccepteerd zijn en genoeg mensen opgeleid zijn voor STPA. Controlerende instanties moeten het ook toestaan.

Een hazardlog is ook noodzakelijk om vervolgstappen uit te voeren met STPA.

Respondent 4 (author of this thesis):

1. Praktische informatie

- Datum: 17 augustus 2022
- Werkervaring (projecten, jaren actief)
  - In het spoor:

Een half jaar, de periode van mijn afstuderen.

  - Met betrouwbaarheid/risico analyse:

1 maand, in de laatste maand van mijn afstuderen heb ik STPA toegepast.

  - Met STPA:

1 maand, in de laatste maand van mijn afstuderen heb ik STPA toegepast.

2. Terugblik op STPA ervaringen

1. Waarom ben je begonnen met STPA te gebruiken?

Bij een vacatuur voor een afstudeeronderzoek bij ProRail werd STPA genoemd om te bekijken of en hoe STPA toegepast kan worden bij ProRail.

2. Waarom vervolgens er ook weer mee gestopt?

n.v.t.

3. Wat vond je het grootste voordeel van STPA? (eventueel in vergelijking met traditionele gevaren analyses als FMEA)

Voornamelijk de structuur en de handvatten om faalscenario's te identificeren. Het STPA handboek legt op een begrijpelijke manier uit welke stappen er steeds gezet moeten worden en voorbeelden worden daarbij gegeven. Hierdoor kan iemand die geen ervaringen heeft met het uitvoeren van risicoanalyses toch deze systematische aanpak volgen en zelf uitvoeren.

4. Wat vond je het grootste nadeel van STPA? (eventueel in vergelijking met traditionele gevaren analyses als FMEA)

Er wordt met STPA van alles geïdentificeerd of opgesteld: gevaren op systeem-niveau, systeembeperkingen, controle structuur, onveilige controle acties, controleur beperkingen en uiteindelijk faalscenario's. Dit is op zich positief, alleen weet ik niet precies wat ik met de geïdentificeerde faalscenario's moet. Na de analyse van STPA word je geheel losgelaten in hoe je de faalscenario's verder kan analyseren. Je weet niet of de scenario's acceptabel zijn of realistisch, als er ernst of kans aan wordt toegekend, dan zou dat al zeker helpen. Je wordt ook niet begeleid in hoe de verschillende scenario's gemitigeerd kunnen worden.

5. **P:** Wat zijn de grootste lessen die je hebt geleerd door het toepassen van STPA?

Hoe je een controle structuur kan opbouwen voor een systeem. Dat er in veel systemen controle en feedback mechanismes zijn die hiërarchisch gepositioneerd zijn. Een controle structuur gaf mij beter overzicht over hoe een systeem precies werkt.

En dat je op verschillende structurele wijzen risico's kan identificeren, dat je daarvoor geen ervaringsdeskundige voor hoeft te zijn. Je kan al risico's identificeren als een systeem nog niet bestaand en je ook geen kennis hebt van soortgelijke systemen.

6. Vond je STPA complex om te leren en uit te voeren als 'STPA leek'?

Nee, ik merk wel dat het lastiger is om STPA aan anderen uit te leggen dan een analyse die 'simpeler' is, zoals een HAZOP.

7. Hoeveel tijd en aandacht was je kwijt aan elke STPA stap? (1. Define purpose, 2. model control structure, 3. identify unsafe control actions, 4. identify loss scenarios)

Stap 1 koste me weinig tijd, dit kwam omdat ik het spoorvervoerssysteem daarvoor al goed had onderzocht en ik daardoor het systeem goed in kaart had. Het opstellen van de gevaren op systeemniveau was ook goed te doen, omdat ik wist dat ik wilde focussen op treinvertraging binnen een gebruikersproces.

Stap 2 was moeilijker, hiervoor moest er een goede controle structuur gemaakt worden, ik had veel voorbeelden gezien en elke verschilde meer dan ik had verwacht. Er moest dan ook een goede balans komen tussen specifieke feedback en controle mechanismes, maar niet te veel in detail treden bij de actoren zelf. Hierbij had ik ook experts nodig op het gebied van het gebruikersproces en daarvoor heb ik een workshop moeten organiseren.

Stap 3 koste mij weinig moeite, deze stap kon ik grotendeels zelf doen, zonder al te veel kennis te hebben van de praktijk.

Stap 4 koste mij de meeste tijd en aandacht. Voor het uitvoeren van deze stap had ik wederom experts nodig en het identificeren van scenario's kost veel aandacht.

Stappen 2 en 4 kosten voor mij de meeste tijd en aandacht, stappen 1 en 3 spraken meer voor zich en waren gemakkelijker uit te voeren.

8. (Wanneer STPA is vergeleken met een andere risico analyse.) Heb je ervaren dat er nieuwe scenario's waren ontdekt die konden lijden tot verliezen. Of waren de (scenario's naar) gevaren al geheel bekend? Wat voor scenario's waren dat? (software/interacties/product/menselijk falen)

n.v.t.

9. Heb je tips voor het praktisch toepassen van de STPA uitkomsten? Waardoor je de geïdentificeerde gevaren kan mitigeren?

Identificeer hoofdindicatoren van risico's. Hoe je dit moet doen is beschreven in hoofdstuk 6 van het STPA handboek. Deze staan los van de STPA stappen, maar kunnen de STPA uitkomsten wel praktischer maken.

3. STPA toepassen binnen het spoor vervoersysteem met ERTMS

10. **P:** Wat zijn de succesfactoren om STPA te doen slagen binnen een organisatie? (uit praktijkervaring)

De mensen waarmee je samenwerkt moeten begrijpen wat STPA is en hoe ze bruikbare informatie kunnen geven om deze analyse goed uit te voeren. Ik heb gemerkt dat het heel handig is om iemand te hebben die de gehele analyse al kent en het liefst ook al meerdere keren heeft uitgevoerd, zodat er met vragen over STPA gelijk naar diegene gegaan kan worden.

Go big or go home met de STPA, als de organisatie zich maar matig inzet voor STPA, dan zullen er waarschijnlijk ook alleen maar matige resultaten uit komen.

11. **P:** Welke onderdelen van het vervoerssysteem met ERTMS zijn de inspanning van STPA waard en welke onderdelen kunnen beter met andere technieken gedaan worden? (denk aan gebruikersprocessen, het gehele socio-technische vervoersysteem of technische systemen) Waarom?

Hier kan ik niet goed gegrond antwoord op geven.

12. Welke expertise moet je minimaal hebben voor het uitvoeren van STPA?

Kennis van de analyse en van het systeem wat je analyseert.

13. Hoe kan je STPA praktisch uitvoeren als je zelf niet (volledig) expert bent in het systeem of (gebruikers)proces dat je analyseert?

Experts van buitenaf betrekken.

14. Hoe kan je het beste experts (voorbeeld: gebruikersprocessen experts zoals ontwikkelaars van gebruikersprocessen of ervaringsdeskundigen) betrekken bij STPA als ze STPA niet kennen?

Het is noodzakelijk dat je diegene wel goed meeneemt in het gedachteproces en de definities die worden gegeven bij STPA. Anders krijg je miscommunicatie.

15. **P:** Vind je dat de tijd/inspanning die STPA kost het waard om naast traditionele (huidige) gevarenanalyses ook STPA uit te voeren voor onontdekte faalscenario's?

Hier kan ik niet goed gegrond antwoord op geven.

16. Kan STPA de traditionele (huidige) gevarenanalyses volledig vervangen?

Hier kan ik niet goed gegrond antwoord op geven. Ik denk het niet, omdat de analyse je niet helpt met mitigerende stappen.