NTNU
Norwegian University of
Science and Technology

Bayesian Safety Analysis of Railway Systems with Driver Errors

Mohammed Manar Rekabi

Reliability, Availability, Maintainability and Safety (RAMS)
Submission date: June 2018
Supervisor: Yiliu Liu, MTP

Norwegian University of Science and Technology
Department of Mechanical and Industrial Engineering

NTNU

Faculty of Engineering
Department of Mechanical and Industrial Engineering

Bayesian Safety Analysis of Railway Systems with Driver Errors

Mohammed Manar Rekabi

Master Thesis 2018

Supervisor: Yiliu Liu
Co-supervisor: Lijuan Dai, Rambøll

Address:
NO-7491 TRONDHEIM
Norway

Org.nr. 974 767 880
Email:
mtp-info@mtp.ntnu.no
https://www.ntnu.edu/mtp

NTNU

Faculty of Engineering
Department of Mechanical and Industrial Engineering

Abstract

The main objective of this thesis is to improve safety in railway systems through studying and understanding the train drivers' tasks and their common errors.

A literature review is conducted to develop a deep understanding of driver errors, as well as to recognise the different methods and techniques used to identify and quantify these errors. The most important issue is that of finding a method that can be used to build a model to quantify drivers' errors, taking into consideration the types of drivers' tasks and the characteristics of factors that can affect driver reliability.

Different approaches of classifying and analysing driver errors are reviewed, as well the factors that affect driver performance. The present thesis also explains the concept of hazard identification and presents different models used for illustrating accident causality particularly the STAMP model. A comprehensive overview of the STPA method under the STAMP model is presented, along with how it could be applied for controllers and humans. Quantitative risk assessment, along with some methods for quantifying human errors, are overviewed, and a Bayesian network is selected to study the effects of the identified driver errors.

After a detailed assessment of the literature, STPA is found as a suitable method of hazard identification. A Bayesian network is employed to model the hazardous events and quantify safety analysis. The benefits of applying these methods in railway systems and in the context of human error are also discussed.

The case study aims to present a detailed quantitative safety analysis at ERTMS system levels 1 and level 2, including driver errors. The STPA and Bayesian methods are implemented to identify the hazards and quantify the probability of hazards when trains fail to stop at red signals. The data used in this quantitative analysis depends mainly on assumptions.

Finally, several avenues for further research are also discussed.

Contents

Table of Figures

Table of Tables

Chapter 1

Introduction

Railways play a significant role in public transportation around the world. This creates a need to execute railway operations at higher speeds, in safer environments and in a more efficient manner. In order to achieve this, new standards and specifications have been developed, especially in signalling and controlling systems. For example, the European Railway Traffic Management System (ERTMS) standard was developed and designed to ensure interoperability, safety, and maximum utilisation of track capacity; this standard aims to bring more benefits to the European railway system and to boost international freight and passenger transport.

Although there is an urgent need for these new developments and technology in railway systems, the issue of safety is still receiving the greatest attention and is considered an essential requirement for railway transportation. The primary risks in modern railway systems are still similar to the conventional ones, including derailment and collision, which arise mainly from speed limits being exceeded or trains failing to stop at a signal set to danger (i.e. a red signal); the latter is called Signal Passed at Danger (SPAD).

In fact, there are numerous factors affecting safety in railway systems, such as procedures, regulations, working conditions, technical problems, safety management, and human error [6].

1.1 Background

The introduction of new technologies and digitalised solutions in railway systems has led to the increased complexity of these systems, and thus to the emergence of new types of unintended system performance or unpredicted system behaviour. There are also changes to the way in which various tasks are achieved, including those performed by personnel such as train drivers, who change the way they perform their roles from an ordinary way to a supervisory way due to automation; this requires a high level of attention and cognitively complex decision-making. That means that new technologies create new modes of both machine failures and human errors.

There are many risk analysis techniques, both quantitative and qualitative, used to determine risk levels; however, the quality of the results of these quantitative techniques depends primarily on the data and its sources. That means building an efficient model that can be used to analyse safety in new railway systems requires accurate, complete, and specific information. This information is about the reliability of various system components in addition to information about human reliability. Indeed, acquiring accurate information about human reliability is not an easy process,

since the value of human reliability depends on the estimated values of factors that impact on human errors and the dependencies between them.

Consequently, it is crucial to find a model that can be used for safety analysis and takes into consideration both the various factors that impact on safety and the dependencies among these factors, as well as having low sensitivity to the accuracy of values of these factors.

1.2 Objectives

The main objective of this paper is to study and analyse the safety in railway systems with a principal focus on human errors, especially driver errors. This objective will be realised by accomplishing the following sub-objectives:

- Understand the importance of human error in railway systems;
- Introduce the duties of train drivers, along with their performance;
- Identify the hazards related to train drivers;
- Clarify the concepts involved in quantitative risk assessment and summarise some methods and techniques used to analyse human error;
- Identify a suitable method to build a model for quantitative safety assessment.

1.3 Limitations

This thesis aims to find a new way to achieve quantitative safety assessment related to driver errors in railway systems. Because of time limitations and study simplification, the scope of this thesis has been narrowed down to include only ERTMS system levels 1 and 2 and train driver errors related to the occurrence of SPAD, while all other human errors and components in the railway system have been ignored. Moreover, all external hazards, including those that can be created by passengers, weather, and other components in the railway system (e.g. brake systems) are not investigated here. Although a huge number of causal scenarios can be determined by systems theoretic process analysis (STPA), the number of these scenarios has been limited to include only the most common scenarios that have a substantial impact on safety. In addition, a technical study of the ERTMS system encompasses only the most important components in the system. Good data sources are rare due to the fact that the ERTMS system is new and there is a paucity of data related to driver errors regarding this system; as a result, estimated values are used in analysis.

1.4 Approach

The thesis begins with an overview of human error in the railway system in order to assess the impact of train drivers on safety, as well as to distinguish the various factors and causes that impact driver performance. A literature review of hazard identification techniques is then carried out to facilitate an understanding of hazard concepts, recognise the differences in accident causality models, and select an appropriate hazard identification method for ERTMS system. A new hazard identification method (STPA) is selected and explained in detail in order to give a brief overview of its applications. Several scientific databases are used in the course of the literature review, including ScienceDirect, Scopus, Compendex etc. Relevant railway standards and regulations are also studied. For quantitative safety analysis, different methods related to human errors are reviewed and discussed to identify the most suitable method for quantifying safety in railway systems. In the case study, the hazardous event SPAD in ERTMS system levels 1 and 2 is chosen,

and a quantitative safety analysis of driver errors is implemented. Finally, a few suggestions for future research are presented.

1.5 Structure

The remaining chapters of this thesis include a general explanation of human errors in railway systems, especially driver errors, and a discussion of the factors that impact train driver performance and the causes that lead to driver errors. Different accident causality models are then illustrated, and the choice of STPA as a suitable hazard identification method for the ERTMS system is justified. For quantitative safety assessment, a presentation of some methods related to human error and a detailed explanation of the Bayesian network is included. In order to apply the theoretical methods in a practical setting, a case study is presented, including scope, scenario, limitations, and assumptions. Finally, the conclusion is outlined, followed by some suggested avenues for future research.

Chapter 2

Human Errors in Railway Systems

Recently, there have been major technological developments in the railway industry around the world in order to meet the challenges of heavier traffic and the need for higher speed. High-performance diesel and electric locomotives are incorporating advanced capabilities such as modern signalling systems, automatic warnings, and centralised traffic control systems in order to ensure the high performance of railway operations. For example, ERTMS is gradually replacing the existing incompatible systems throughout Europe.

Safety issues in railways, including accidents and incidents leading to fatalities or injuries of passengers and/or employees during railway operations, are very important considerations. These issues stem either from technical or human errors.

2.1 Impact of human errors

Many investigations and analyses have been conducted into railway transportation accidents so as to identify vulnerabilities in railway systems and reinforce railway safety [7], Analysis of data from these investigations suggests that human errors are the most significant source of accidents or incidents in railway systems [8]. For example, at least 75% of fatal accidents in European railway systems between 1990 and 2013 occurred due to human errors. Investigation of accidents in the US between 2007-2017 further shows that more than 37% of all train accidents could be, to some extent, attributed to human errors. The ratio of accidents associated with human errors increases to more than 80% of all major railway accidents worldwide [9].

Human errors can lead to hazardous events such as exceeded speed, signal passed at danger (SPAD), or signalling or dispatch errors [10]. Analysing human errors is an extremely difficult process because it requires taking a range of variables and estimations into consideration; during this process, various types of methods and techniques with different properties can be used.

The role of a train driver is considered as the most important role in the railway system and has a high impact on railway safety. To analyse driver performance accurately, the focus should be on possible errors made by drivers, along with the drivers' main goals and tasks.

2.2 Classification of human errors

Human errors can be classified into two broad categories: active and latent errors [11]. Active errors, the effects of which are felt almost immediately, are associated with frontline operators of

the system such as train drivers, signallers and controllers. Latent errors, the adverse consequences of which may be hidden in the system for a long time, only become clear when they combine with other factors to breach the system's defences; for instance, human errors related to design, procedures, maintenance, and management are errors of this type[11].

Moreover, human errors can be further classified according to the context of the incident. For example, if an error occurs when an operator conducts a task under specific conditions, this error can be classified according to the operator (train driver, signaller, etc.), type of task, and the conditions under which the task is executed (e.g. location, equipment used, etc.) [12].

Another classification method involves the cognitive processes of the operator, such as his perception, memory, and ability to make the correct decision when he conducts his tasks. This classification concentrates on external and internal factors such as time pressure, knowledge, and fatigue, which can influence the operator and lead him to commit errors [12].

In short, there are many methods and techniques used to classify human errors; the choice of a suitable technique depends primarily on the type of error involved and the aim of the classifications.

2.3 Approaches to the analysis of human errors

Human reliability analysis (HRA) is a framework used to express the probability of human errors occurring in a system, as well as to identify the causes and consequences of these errors [13]. Many kinds of HRA techniques (such as Technique for Human Error-Rate Prediction (THERP), Human Error Assessment and Reduction Technique (HEART), Human Factors Analysis and Classification System (HFACS), etc.) have been developed to quantify human performance. However, this quantification is not easy because it can be affected by a large number of factors, known as performance shaping factors (PSFs). The values of PSFs are highly dependent on the judgment of experts and there is insufficient evidence to suggest that these values will necessarily change or remain constant during railway operations [13]. In addition, the differences between persons also play a role. All these issues cause the quantification of human errors to be associated with a high level of uncertainty.

To improve safety in railway systems, it is important to make these systems more tolerant of human errors. This tolerance will be realised through simplifying human tasks in order to reduce error probability and adding more barriers in designs. These barriers can increase the recoverability of a railway system when human errors occur, as well as contain the consequences that emerge if an accident happens [11].
Since train drivers are considered most important for railway safety, the rest of this thesis will focus on the performance of and errors committed by of this type of railway system stakeholder.

Chapter 3

Train Driver Performance

Various types of equipment and technology have been introduced to railway operation systems. For instance, automatic train protection (ATP) systems correct human errors by stopping a train when necessary [14], while automatic warning systems (AWS) give train drivers an audible and visual indication of the status of the signal ahead [15]. Despite this, the duties and responsibilities of train drivers are still the same. In this chapter, a train driver's role will be analysed in depth, the impact of train driver errors on safety will be reviewed, and a train driver's duties will be demonstrated, along with the errors associated with these duties. In addition, the sources leading to driver errors will be identified.

3.1 Impact of train drivers on railway system safety

The percentage of accidents caused by driver error is very high compared with other types of human error. For example, in a country like the UK, which is home to one of the oldest, densest, and busiest networks in Europe, accidents due to driver error made up more than 50% of all accidents occurring in the UK railway system between 1945 and 2012 [10]. The statistics derived from Eurostat presented in Table 1 show that most accidents that caused fatalities or injuries in Europe in 2016 were associated with driver error in one way or another.

It can be concluded that drivers have the most important role in railway systems. Analysis of driver performance, along with the context and conditions under which they execute their tasks or activities, is therefore essential for enhancing safety in railway operations.

3.2 Analysis of train drivers' duties and errors

The role of a driver can be summarised as controlling the train along its route by receiving the stream of usability signs and signals from lineside, while at the same time interacting with the displays and controls provided within the cab [16]. This means that a driver's task is to integrate the various sources of information available to him in order to achieve the following goals:

- Moving the train according to the authority of movement;
- Moving the train within the safe speed limits, and
- Making safe and accurate scheduled stops.

Many studies and research projects have been conducted to identify and classify driver errors in railway systems using different tools, methods, and scenarios. These studies depend on either accident/incident investigation reports or simulations and test observations.

Table 1: Number of persons killed and injured by type of accident and category of persons [17]

Type of Accidents	Number of persons											
	Killed				Injured				Total			
	Passengers	Employees	Other	Total	Passengers	Employees	Other	Total	Passengers	Employees	Other	Total
Collisions	28	13	3	44	64	8	5	77	92	21	8	121
Derailments	2	2	7	11	13	2	12	27	15	4	19	38
Accidents involving level-crossings	0	3	253	256	1	3	214	220	1	6	469	476
Accidents to person caused by rolling stock in motion	12	14	625	651	76	21	341	438	88	35	966	1089
Fires in rolling stock	0	0	0	0	1	1	0	2	1	1	0	2
Others	2	0	0	2	0	14	0	14	2	14	0	16
Total	44	32	888	964	155	49	574	778	199	81	1462	1742

For example, one study conducted at the Queensland Rail Driver Training Centre (DTC) aimed to address and classify driver errors, as well as to determine the relationship between those errors and fatigue. This study tested twenty male train drivers in rail simulators consisting of a realistic cabin with fully operational control panels and authentic sounds. Different scenarios and work conditions were applied during the test. The results of this research showed that drivers can commit three major types of errors during their tasks, as follows [18]:

- Brakes are applied wrongly (too early or too late);
- Failure to respond to in-cab station protection and vigilance systems;
- Driving the train at a speed that exceeds the limit.

Another study aimed to identify the types of human errors that caused incidents/accidents in Australia between 1998 and 2006. The study analysed the reports of investigations released by the Australian Transport Safety Bureau [7]. This study used two techniques. The first of these was the Human Factors Analysis and Classification System (HFACS). This technique includes four levels: failure of organisational influences, supervisory factors, preconditions for unsafe acts, and unsafe acts. These levels are further broken down into sub-categories as shown in Fig. 1.

The HFACS technique is used in this study to identify errors according to their root causes. The main causes of driver errors were as follows:

- **Unsafe act errors** due to decision-making, skill-based, and routine factors.
- **Preconditions for unsafe act**, which include the condition of the driver (e.g. poor health, both mental and physical) and environmental factors.
- **Unsafe supervisory factors,** i.e. when inadequate supervision occurs.
- **Organisational influences**, which contains two factors: organisational climate (policies) and organisational process (procedures and oversight).

The classifications of the causes of driver errors according to this study are marked in yellow in Fig 1.

The second technique is retrospective and predictive analysis of cognitive errors (TRACEr). This technique incorporates two tools: a predictive and a retrospective version. The predictive version

is used to identify and classify possible errors, while the retrospective version is used for incident investigation.
The most obvious finding from this analysis is that major errors made by train drivers tend to occur either when drivers failed to detect and respond to signals (e.g. drivers failed to stop the train at a red signal; 'train stopping errors') or when drivers could not judge aspects of the train correctly (e.g. the speed of the train, its location, and other situations that could lead to exceeding the speed limit; 'train driving errors').

The results of the TRACEr technique reveal that the impact of errors depends on both the speed of error detection and the effectiveness of error recovery. Most accidents occurred because the drivers either did not detect the error or detected it too late. However, the accuracy of these results depends on the quality of the investigation and the reliability of the accident reports.

Since the driver error is the last link in a chain that could lead to an accident, it is reasonable to understanding how accidents can happened and identify the underlying causal factors.

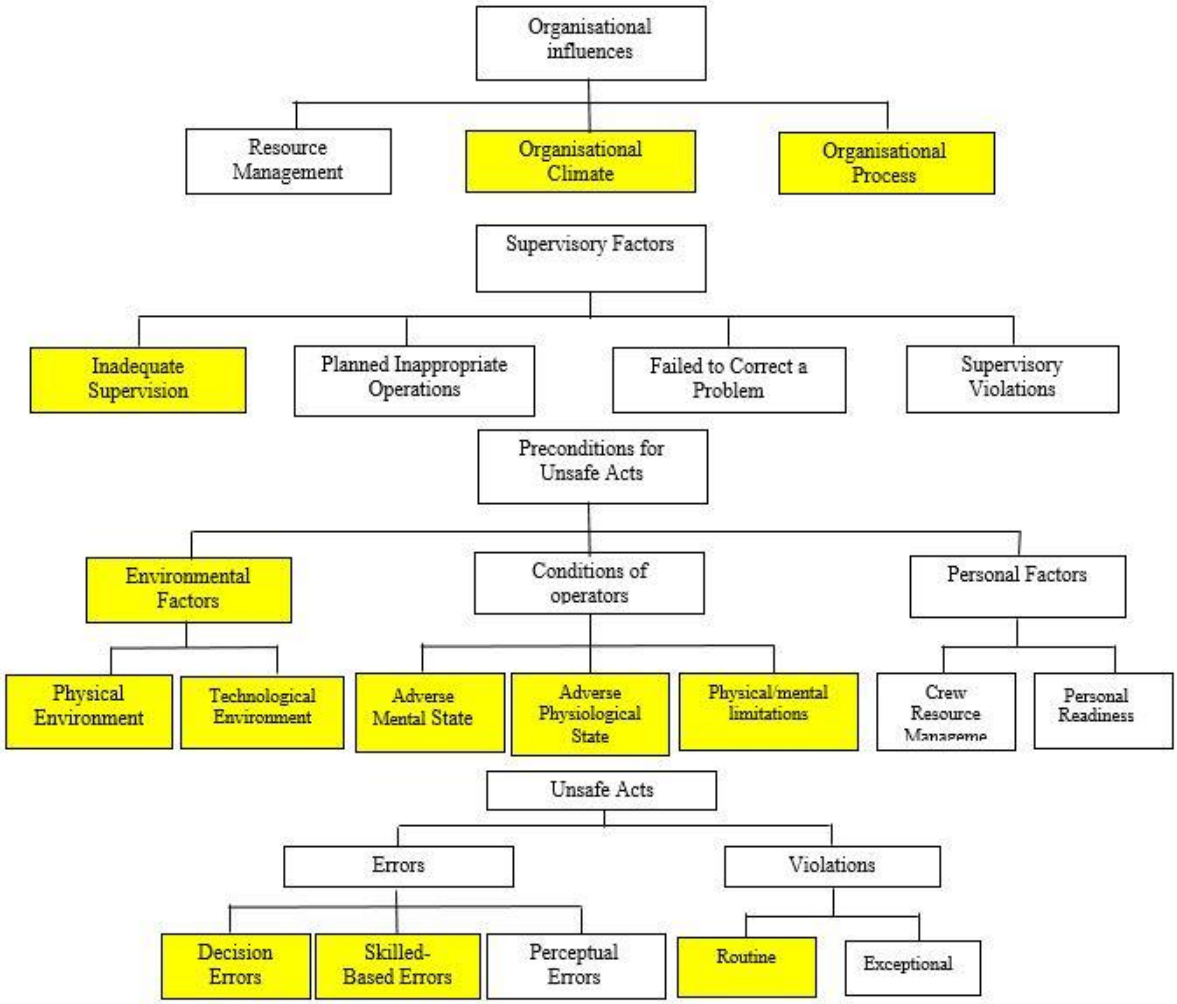


Figure 1: The HFACS framework [4]

3.3 Identifying the underlying causal factors of driver errors.

To improve railway system safety and reduce the probability of train driver errors, the underlying causal factors of these errors should be determined. In order to achieve that, it is important to understand how the driver carries out his roles and how errors can arise as a result. It is obvious that a driver's primary task is a visual task, i.e. monitoring the dynamic scene visually both inside the train cab and outside; communicating with other crew members on board is also important. Accordingly, the underlying factors causing train driver error can be summarised as follows [19]:

- Inadequate communication with the train crew or traffic manager who covers communications, supervision, and checking in with other persons who collaborate with the train driver;
- Poor interaction with cabin instrumentation, equipment, and/or any other material that can be used to carry out tasks, in addition to any difficulties in recognising lineside signals due to environmental issues;
- Weak compliance with rules, procedures, and routine on the part of the driver;
- A lack knowledge and necessary experience of the part of the driver.

These underlying causal factors of driver errors are illustrated in Fig. 2.

To reduce the errors that could be committed by a train driver during his duties, it is important to understand the root causes of these errors. Errors can be classified according to their root causes as follows [16]:

- Limiting time for executing the task: for example, workload. If more than one action is required to be performed in the same time span, the driver will divide the available time between activities rather than performing the two actions simultaneously.
- Limiting resources within the cognitive system, as more complex tasks demand more attention. For example, reading the lineside signal in the presence of sighting hazards requires more attention than reading in normal conditions.

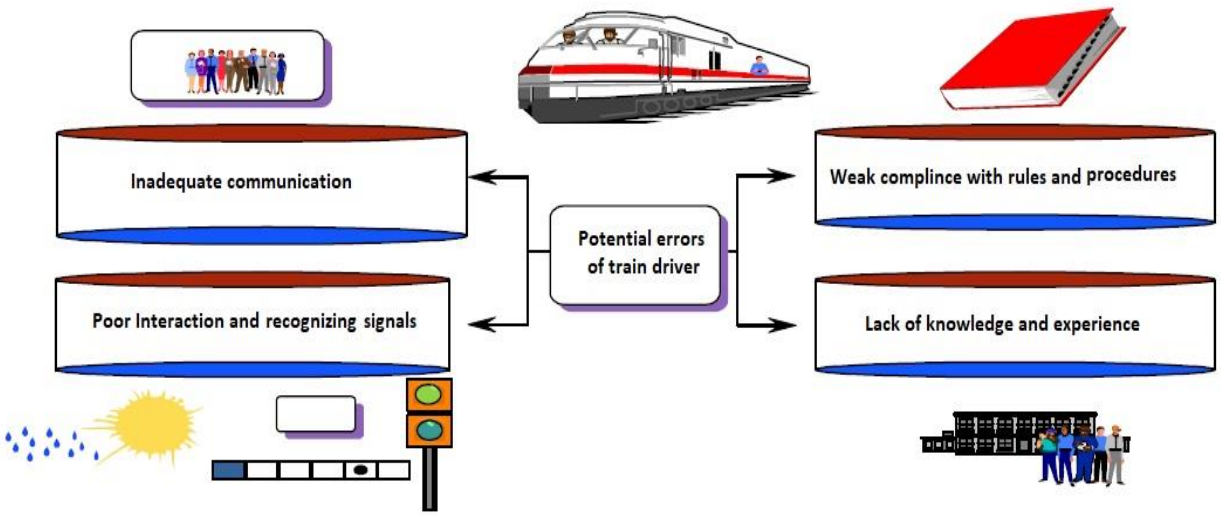


Figure 2: Underlying causal factors of train driver errors (modified from [4])

Hence, train driver performance depends on how and when the driver controls the train's speed, observes signs, signals and other visual targets, responds to safety devices, and performs station activities [16].

Although the importance of underlying and root causes of errors has been established above, these factors are insufficient in some cases; this is because these underlying and root causes do not include hazards that arise from drivers themselves.

It is important to note that there is very little to no literature that makes a direct link between the quantitative safety analysis of train drivers and the mental state of those drivers. This means finding the relation between the probability that a driver will take an unsafe action and their ability to duly interact with the system; this is accomplished by monitoring and observing the exact data they need, interpreting this data properly, developing an accurate mental image of system according to this data, and matching their objectives with safety considerations.

In order to conduct quantitative safety analysis for railway systems, including errors made by train drivers, it is important and necessary to identify all types of hazards and understand their nature. This is because hazards can arise in many different ways and can take various forms, as explained above. It is also important to model these hazards correctly so that it is possible to predict the probability of hazardous events.

Chapter 4

Hazards Identification for Train Drivers

A hazard is defined as an activity or combination of activities or set of circumstances that may produce an accident with the potential to harm life, health or property. Hazard identification includes the systematic investigation of all potential hazard sources and the recording of hazards identified. This means identifying all possible ways in which people or property may be harmed through the actions of a train driver [20].

Railway system technology has changed rapidly in recent years, introducing unknowns into the system and creating new paths to losses; moreover, the operation of some new railway systems is so complex as to include different types of complexity, meaning that information about potential system behaviour of the system is sometimes incomplete. Furthermore, digital technology and software are used widely in railway systems, leading to increased sharing control of systems between humans and automated devices. These issues make the relationship between humans and machines more complex, with the result that new distributions of human errors are appearing and new factors that may lead to railway system accidents are emerging [21]. In turn, this creates new hazards for train drivers during their handling of all normal and abnormal situations.

Traditional hazard identification techniques are unable to deal with all these new types of errors and hazards. For example, many recent accidents for which drivers have been blamed could be labelled more precisely as resulting from flaws in the environment where drivers operate [21].
Although it is generally understood that safety is increased by increasing system or component reliability, this is not true in all cases, as a system can be reliable but unsafe. This can be noticed in complex systems, when accidents often arise from interactions among components that are all functioning as they should. A system can also be safe but unreliable, as in a safe-fail system. In addition, these two properties may even conflict in some cases; that is, making the system safer may decrease reliability, while enhancing reliability may decrease safety [21].

The above highlights a need for a new approach to identify hazards that should be avoided in a system. This new approach should be able to identify all of the various types of hazards, including those resulting from interactions between components, system complexity, the use of a new digital technology, and human behaviours, which are in turn influenced by social, organisational and environmental factors. To arrive at this approach, a suitable model of accident causality should be established to provide a baseline for understanding how accidents can occur and highlight the causal factors.

4.1 Accident Causality Models

An accident causality model, which is a theory about how accidents occur, may be used for a number different purposes, including [5]:

- **Accident investigation**: understanding why the accident happened and how to identify the potential deviations that may lead to accidents;
- **Accident prevention**: proposing changes that prevent deviations or failures that may lead to accidents;
- **Risk assessment**: providing an input to quantitative risk assessment methods.

There are many accident causality models; this diversity in models provides us with the ability to focus on different aspects of accidents and access a variety of conceptualisations of accident characteristics. In this chapter, four accident casualty models will be presented and discussed: three of them (Energy and Barrier model, Domino Model, and Swiss Cheese Model) are traditional models, while the fourth is a new model (Systems Theoretic Accident Model and Processes, or STAMP).

4.1.1 Energy and barrier model

Energy and barrier models are based on the idea that accidents can be prevented by separating uncontrolled energies from vulnerable targets [5]. There are four basic elements in this model: energy source, barriers (where different types of barriers exist, such as physical, functional, symbolic, and immaterial), energy pathways (pathways from the energy source to the vulnerable assets), and assets exposed to the energy (including people, property, the environment, and so on). These elements are shown in Fig 3. These models are popular in practical safety management.

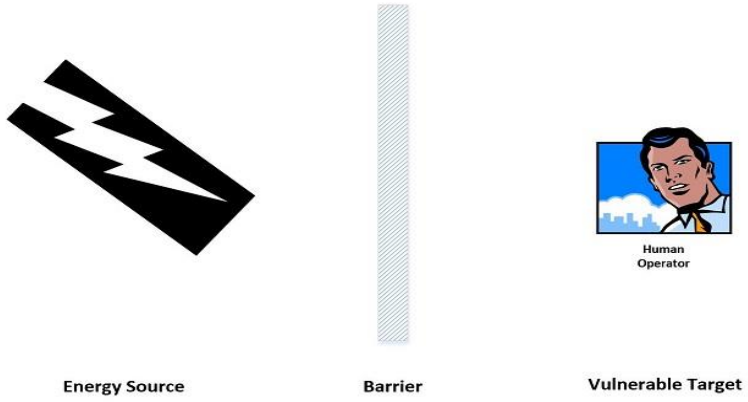


Figure 3: Energy and barrier model

4.1.2 Domino Model

The domino model describes accident causation as a chain of discrete events that occur in a particular temporal order; in short, the accident results from a linear progression of events that occur one after the other [22]. This model is suitable for losses caused by failures of physical

components or human errors in relatively simple systems; however, its capability to explain accident causation in more complex systems is limited, because it describes accidents in far too simple a manner [23].
This model includes five factors in the accident sequence: social environment, fault of the person, unsafe acts or conditions, accident, and injury.

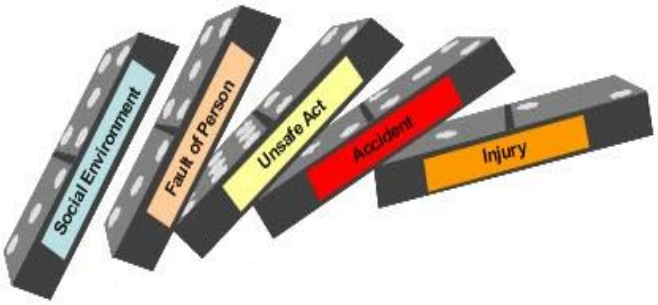


Figure 4: Domino model

These factors are arranged in a domino fashion, such that if the first domino falls, this will lead to the fall of the entire row (see Fig. 4).

4.1.3 Swiss cheese model

The Swiss cheese model is a chain of events causality model. It considers the system as having a series of barriers, represented by slices of cheese, and each barrier as having unintended weaknesses, as represented by holes. Hence, an accident is the result of many factors (manifest and latent) combined in unsafe ways such that all holes are aligned [5]. This concept is further explained in Figure 5.

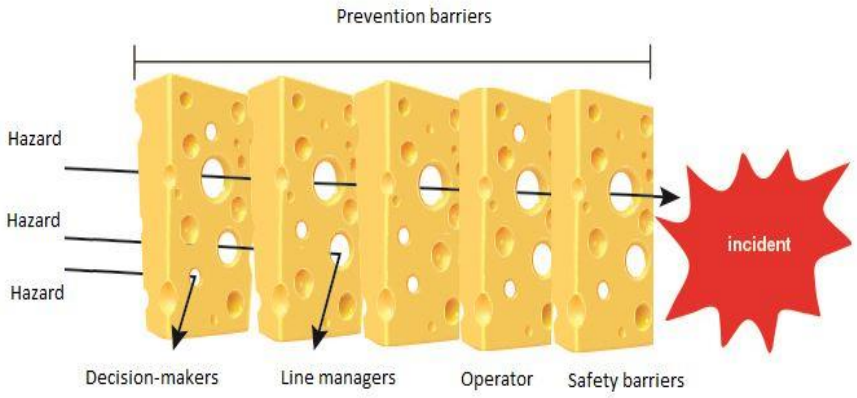


Figure 5: Reason's Swiss cheese model [5]

The accident in this model could be prevented by adding more layers (barriers) or by improving the existing barriers (patching the holes).

These traditional accident causality models have some points of weakness. For example, in the domino model, the accident is considered to be the result of a single cause; if that single cause can be identified and removed, the accident will not occur. In reality, however, accidents always have more than one single cause [5]. Moreover, the Swiss cheese model does not take dependencies between barriers into consideration, which leads to the incorrect conclusion that equipment or humans alone are incorrectly blamed for an accident. This model also treats humans very similarly to other components in the system, despite the fact that human error is very complicated and emerges as complex phenomena within the normal operational variability of a system. For instance, driver fatigue is considered a "cause" of accidents in this model, but a driver being fatigued while driving a train does not always lead to an accident, and accidents may occur without drivers being fatigued [24].

In summary, inter-dependencies between barriers from different barrier systems are omitted from these models, and their perspectives are fundamentally based on linear progression of failures to an accident, despite the fact that accidents may occur due to complex interactions; in addition, the human behaviour is treated similarly to other system components. These models are therefore not good enough for application to new, complex systems, since a good model should explain not only what kind of error might occur but also why it might occur and how it can be prevented.

4.1.4 Systems-Theoretic Accident Model and Processes (STAMP)

This model, which is based on system and control theory, attempts to describe the characteristic performance on the level of the system as a whole rather than in terms of cause-effect mechanisms [5].

The STAMP model has a different vision of system, safety, and accident compared with traditional accident causality models. This is because it treats the system as a set of dynamic processes that adapt continually in order to react to changes in itself and its environment. Safety is defined as controlling the behaviour of and interactions among the system components, and an emphasis is placed on enforcing behavioural safety constraints rather than preventing failures of components; hence, the concept of safety is reformulated as a control problem rather than a reliability problem, while an accident is the result of a complex process that leads to violation of the system's safety constraints [2].

The STAMP model incorporates three main concepts that are used to analyse and describe systems: safety constraints, hierarchical control structures, and process model [2]. In more detail:

- **Safety constraints** are the basic concept in STAMP and can be passive (physical barrier) or active (detection, measurement, and diagnosis). They are enforced by the control loops between the various levels of the hierarchical control structure, so that losses will occur if the safety constraints are not successfully enforced.
- **Hierarchical safety control structures** are used to describe the composition of systems where each level imposes constraints on the activity of the level beneath it. Control processes, which operate between levels, are used to control the processes at lower levels in the hierarchy.
- The **process model**, which is an important part of control theory, aims to model the process being controlled in order to control it effectively. This model includes three types of information:
    1. Relationship among the system variables (control laws);

2. The current state (the current values of the system variables);
3. How the process can change state.

Process model is used to determine the needed control actions, and is updated through various forms of feedback. In summary, process models play an important role in understanding why accidents occur and why humans provide inadequate control.

It makes sense to give a brief summary of the control process concept in STAMP: it is operating at interfaces between levels and includes four types of conditions (goal, action, observability, and model). The goal is a safety constraint that must be enforced by a controller, while the action condition and observability condition are presented by (downward) control channels and (upward) feedback or measuring channels consecutively. The model condition is a model of the process being controlled [2].

Fig. 6 shows the general form of a hierarchical control structure in the design and operation phases.

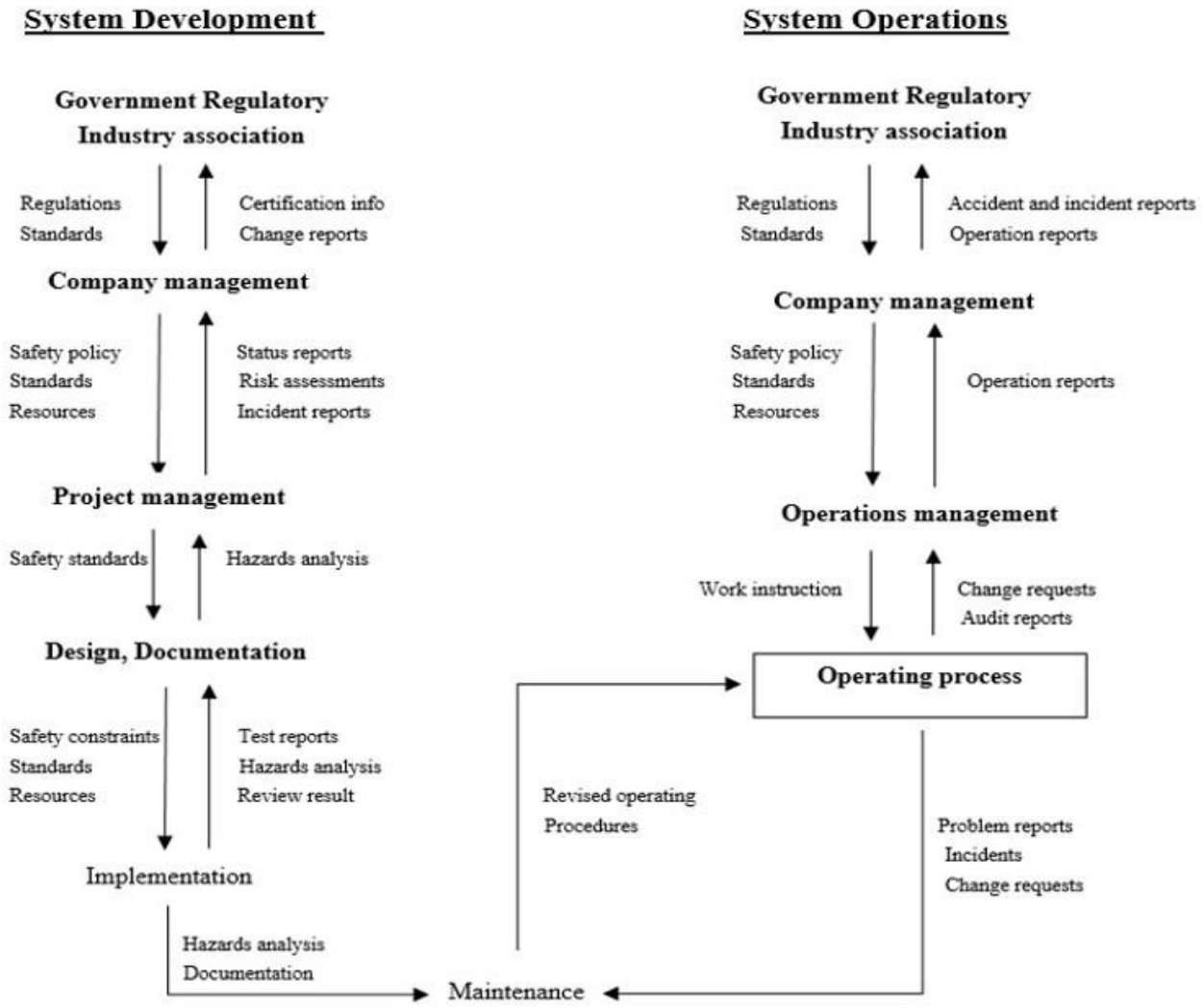


Figure 6: General form of a model of sociotechnical control [2]

From the above, it can be concluded that STAMP can be conducted in two stages:
- Development of the hierarchical control structure, which includes identification of the interactions between the system components and the determination of safety constraints;
- Classification and analysis of flawed control (constraint failures).

The causal factors of hazards in the STAMP model can be classified as shown in Fig 7 [2]:
- Unsafe control inputs and other relevant external information sources (represented by 1);
- Unsafe control algorithms (represented by 2);
- Inconsistent, Incomplete, or Incorrect Process Models (represented by 3);
- The behaviour of actuators and controlled processes (represented by 4).

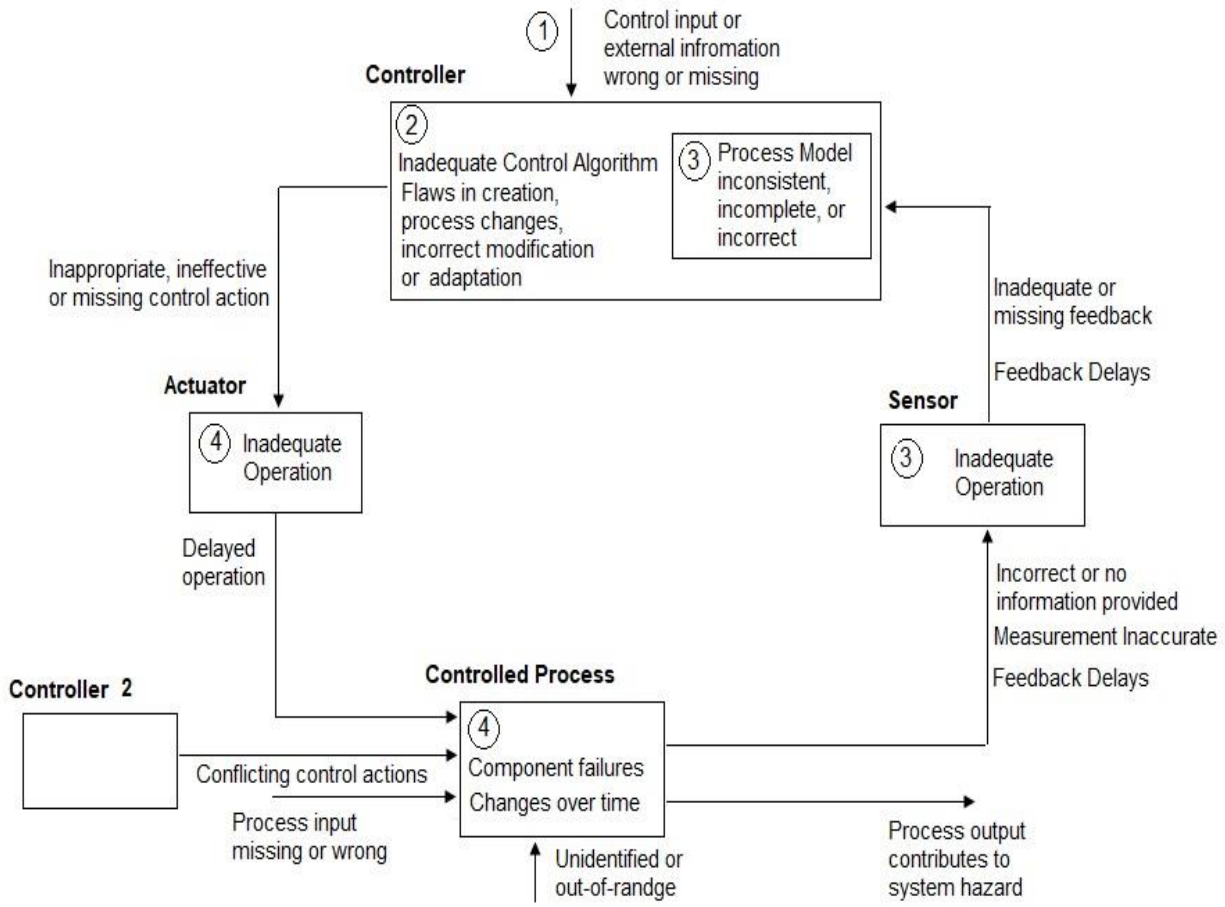


Figure 7: A classification of control flaws leading to hazards [2].

In this model, accidents occur when inadequate control is provided. Inadequate control occurs for different reasons, such as missing constraints, inadequate commands for safety control, commands that were not executed correctly at a lower level, or inadequately communicated or processed feedback about constraint enforcement [2].

If humans are involved in the control structure, context and behaviour-shaping mechanisms also play an important role in causality [2]

Modern railway systems such as ERTMS greatly affect and simplify the role of train drivers by changing their role to primarily involve obtaining comprehensive data about the system by monitoring the specific cab signalling display, making decisions according to this data, and enabling some functions through some buttons and tools in the cab [25]. This makes the ERTMS system highly dependent on software programs, and there is significant interaction among both its components and the system with human [26]. By examining the structure of ERTMS and the interactions between driver and machine, it can be observed that new types of hazards are created, and the ordinary accident causality model will no longer be suitable for these types of systems; thus, a new type of causality model (such as STAMP) is necessary.

This also creates a need for new hazard identification techniques that take into consideration the state of the driver himself: is he in a good enough state that allows him to monitor and observe exactly the data he needs? Is he able to interpret this data correctly and build a valid view of the situation? Does he understand the system and know how it behaves according to the data that he obtained? Is he in good condition, and does he have enough ability to make the correct decision? In order to answer these questions, as well as other questions related to the ERTMS system, a new approach to hazard analysis will be introduced. This approach is called system theoretic process analysis (STPA) and is based on the STAMP causality model.

4.2 Systems theoretic process analysis (STPA)

STPA, a hazard analysis technique based on the STAMP accident causality model, aims to identify the potential causes of accidents that can lead to losses so that they can be eliminated or controlled [21].

STPA was designed not only to identify component failures, but also to address the errors that can result from design or software flaws, interactions among various components, cognitively complex human decision-making, and organisational, social, and management factors contributing to accidents. Accordingly, it can be said that STPA has the ability to recognise hazards that cannot be identified by older hazard identification techniques [27].

The main difference between STPA and other traditional hazard analysis techniques is the model employed. In STPA, a systems-theoretic causality model is used rather than the chain-of-events causality model used in other techniques; this means that it depends on a functional control diagram rather than a physical component diagram [21]. Hence, STPA can be conceived of as a top-down hazard analysis technique that includes a set of steps from the basic diagram to the determination of the way control actions might provoke hazards [28]. The following sections describe the STPA process.

4.2.1 The STPA process for controller

To begin STPA, the goals of the analysis should first be identified (determining the accidents to be prevented and defining the hazardous events that could lead to those accidents); this means setting the scope of the analysis. The hierarchical safety control structures that describe the systems are then built, after which safety constraints are determined. Following this, inadequate control actions that may lead to hazards are identified (step 1 in STPA). Inadequate controls include [27]:

- A control action required for safety not being provided or followed;
- An unsafe control action being provided;
- A control action being provided too early or too late (at the wrong time);
- A control action required for safety being stopped too soon or applied too long.

Finally, it is determined how each control action that may lead to hazards could occur (identifying causal scenarios - step 2 in STPA). This is accomplished by examining the parts of the control loop and the external inputs to see if they could cause it [27].

To explain how the STPA process is executed, a highly simplified example will be presented. In this example, the train is stopping at the station and should not move before all doors are fully closed. In this case, the function of the controller is to prevent the train from moving if the doors are not fully closed. STPA will be applied to identify the hazards associated with this situation. The process begins with the following:

1. Hazardous event: passengers could fall from the train when the train begins to move from the station.
2. Safety constraint: the breaks should be active when the doors are not fully closed.
3. Hierarchical safety control structure: a structure of the system including the components of the system, control instructions (provided by each component), potential feedback, control operations by the controller, and instructions from the driver. This structure is shown in Fig. 8.

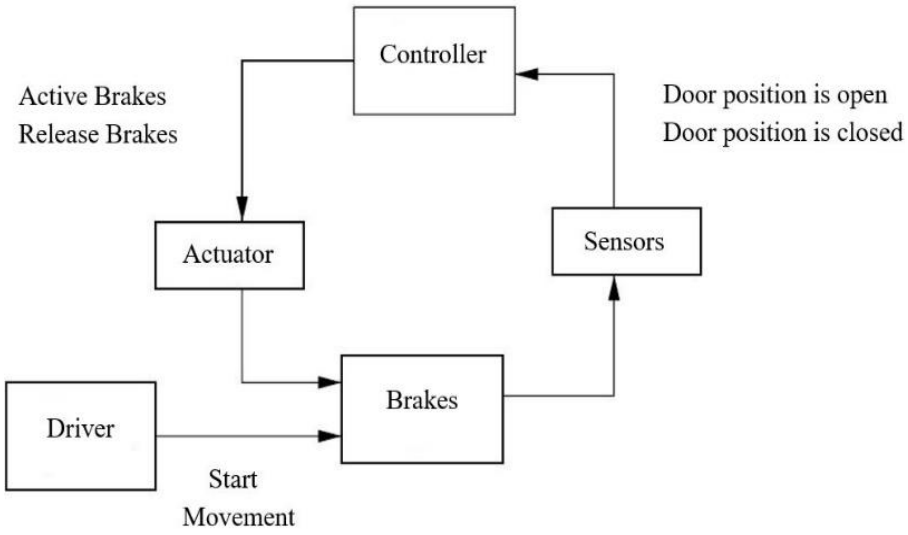


Figure 8: Hierarchical safety control structure for preventing the movement of the train when doors are not fully closed

The functional requirements of the controller are:
- Detect when the door is opened and activate the brakes;
- When the door is closed, release the brakes.

4. Identifying unsafe control actions to determine inadequate controls that can lead to hazards.

There are four types of control actions that could create hazards (step 1):
- 'Activate brakes' command is not given when the door is opened.
- The door is opened, and the controller waits too long to activate the brakes;
- A 'release brakes' command is given while the door is open;
- A 'release brakes' command is provided too early (when the door has not yet fully closed).

The unsafe control actions are shown in Table 2. The situation when the doors are closed is neglected, because there are no hazards present when the doors are closed.

Table 2: Unsafe control actions that cause hazards

Control Action	**Not providing causes hazard**	**Providing causes hazard**	**Wrong timing causes hazard**	**Stop too soon or applied too long**
Actice brakes	Brakes not activated when doors are open	Not hazard	Doors opened controller waits too long to active brakes	Not applicable for (discrete comand**)**
Release Brakes	Not hazard	Brakes released when doors are open	Controller release brakes too early, doors not fully closed	Not applicable for (discrete comand**)**

5. Determining how unsafe control actions could occur (identifying causal scenarios) (step2):

This step aims to identify the scenarios leading to the unsafe control actions (hazards) that violate the safety constraints [29]. For each unsafe control action identified in previous step, all parts of its control loop should be examined to determine whether they participate in or contribute to this unsafe action. As an example, for the unsafe control action 'brakes not activated when the door is opened', the hazards could result from each part in the control loop (controller, communication channels, actuator, and sensor). From the controller, a hazard could emerge if the process model incorrectly shows that the door is closed and/or that the brakes are activated when this is not the case, or if feedback about the state of the doors or the brakes is not received by the controller. From the communication channels, a hazard could emerge if the 'activate brakes' command was sent but not received by the actuator; from the actuator, if the command is received but is not implemented, is implemented after some delay, or is implemented incorrectly; from the sensor, if

one opened door is not detected by the door sensor, there is an unacceptable delay in detecting the open door, or the sensor fails or provides spurious feedback.

These causal analyses are shown in graphical form in Fig. 9. Moreover, control flaws could be identified by using a general graph that includes classification of control flaws (Fig 7).

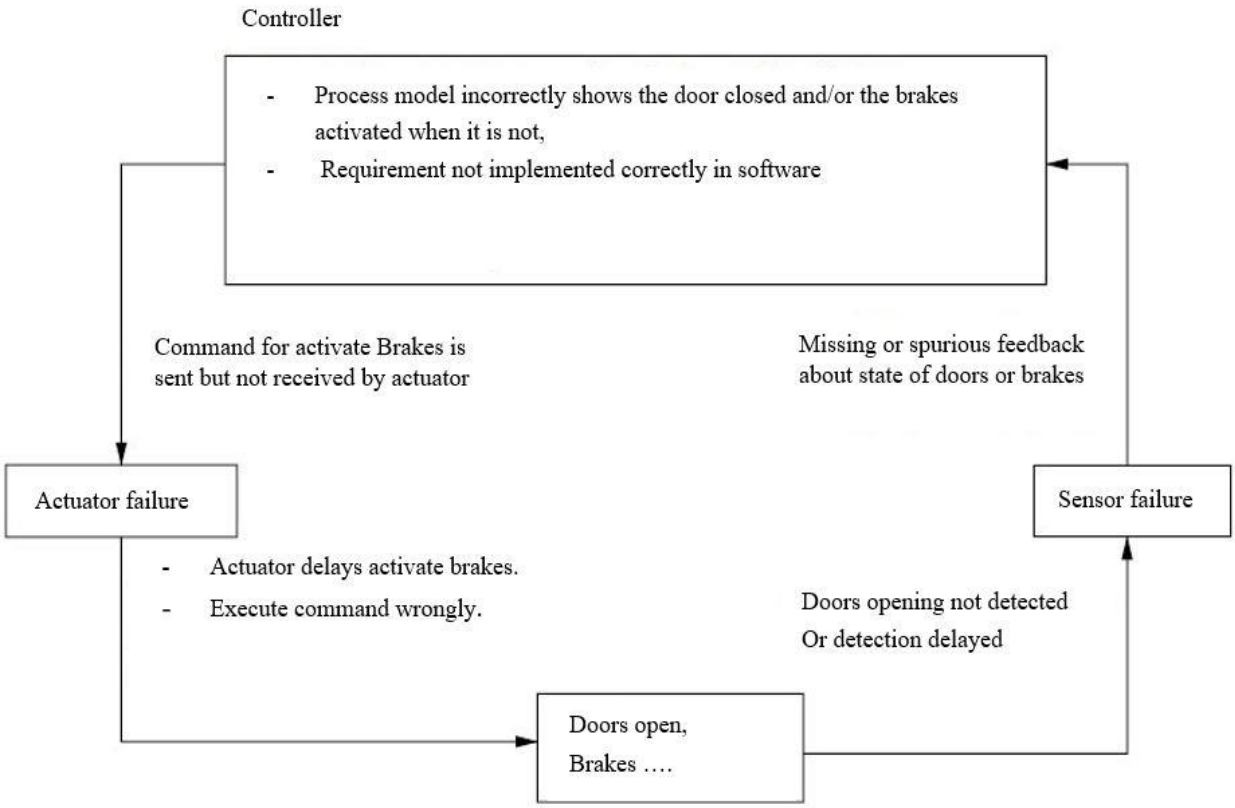


Figure 9: Example of identifying causal scenarios of unsafe actions

After explaining the STPA process in a technical system, it is important to also examine the STPA process for human, especially considering that the STPA technique takes a different view of human errors. STPA considers these errors to be a product of the environment in which they occur, and to always be influenced by this environment; hence, reducing human errors depends on the mechanisms and factors that shape human behaviour, as well as the context in which human actions take place and decisions are made [30].

4.2.2 STPA process for humans

Humans in STPA are treated in the same way as automated controllers when unsafe actions (step 1) are determined. However, the causal analysis scenario generation is more complex, because human behaviour is illustrated by using an additional process model (automated controller) as illustrated in Fig 10. Moreover, human errors are considered as the result of incorrect behaviour,

which is modelled in terms of the conditions, environment, and objectives of the decision-maker. Accordingly, identifying the factors that contribute to the creation of incorrect models and understanding the human's thinking and motivations are basic components of generating causal analysis scenarios in STPA [21].

Feedback loops are the best way to model train drivers errors as they employ dynamic control algorithms that change as a result of feedback (weather conditions, current speed) and goals (obeying the speed limit or arriving at the destination at a required time). In many cases, these dynamic algorithms can make the difference between rules, procedures and actual behaviours of drivers that lead to hazards [21]. Moreover, some factors like fatigue and tiredness can have an impact on drivers' ability to perform mental simulations and make optimal choices [31].
Hence, to identify the causal scenarios that lead to hazards, it is important to know what current data train drives have about the system, to what extent drivers believe this data is correct, and how drivers chose the control action to perform [32].

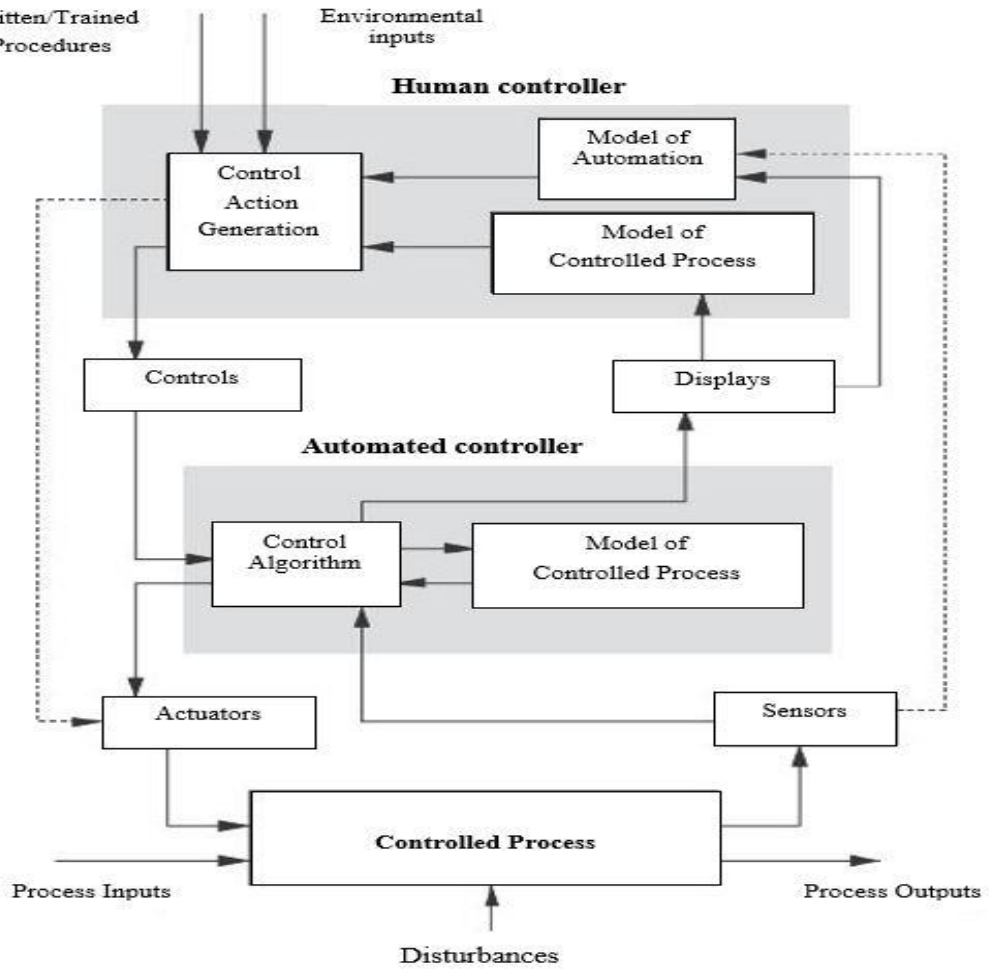


Figure 10: Human controller model [3]

Almost all of a driver's work is a mental act based on knowing the current state of controlled processes such as current speed, signals, and characteristics of the train and track, understanding the mechanism in which they are changed, and selecting the correct action. Accordingly, the above figure is the best representative of a driver's work mechanism. It can be concluded that the best way to estimate human errors and determine the factors that impact human behaviours is to understand how flaws in mental processes occur and how the driver selects the control actions.

4.2.2.1 Flaws in mental process model

The train driver has a mental model of the system that is affected by the available current information about the variables. This information is derived from interfaces, displays, and lineside signs; sometimes this information could be lacking (e.g. a driver fails to check all available information) or could include unnecessary or incorrect data (driver has insufficient experience to determine what data is important for a particular situation). This leads to the formation of an incorrect mental model and can thus cause hazards. . Furthermore, mismatches between the driver's beliefs about the process state and the actual process state are common causes of hazards; for example, a driver who believes that automatic train protection (ATP) is 'on' when it is 'off' will often take unsafe action. It can extend the causes of an incorrect mental model to encompass wrong beliefs about what the system can do and what the system will do in response to driver actions. The formation of a mental model is influenced by received training as well as any instruction manuals or other documentation provided [32]. Accordingly, to ensure a high level of safety in railway systems a correct mental model of driver about the controlled process and the model of automation should be created and sustained.

4.2.2.2 Control action selection

Control actions made by drivers depend on many factors, such as time pressure, context, environment, and personal properties (e.g. fatigue, stress, expectations, experience, skills, etc.) [32]. Moreover, the driver's goals play an important role in determining control actions; for example, if the driver's main goal is not safety but rather arriving at the destination on time, this could lead him to violate the speed limit. In addition, if there is a possibility of choosing one control action among alternative control actions, it is not always immediately obvious which action is better, as this depends on many factors, especially the experience and skills of the driver, the type of situation (novel, complex or routine), and time pressure. Thus, when the driver has enough skills and experience with the system, he will take actions rapidly and automatically (skilled-based decisions); this may lead to unsafe control actions if a driver takes a familiar action where some other action would be better. On the other hand, if a driver takes action depending on rules and procedures (rule-based decisions), an unsafe action could be taken if there are inconsistencies in the system. In the case that a driver relies on his knowledge and mental model when he takes action (knowledge-based decisions), the unsafe actions emerge from his mental models being inaccurate or incomplete [32].

Depending on both the concepts of how control actions can be selected and the flaws in mental process models, the causality scenarios for hazards can be generated.

After determining the hazards associated with train drivers and their causes, it is important to conduct quantitative risk assessment to provide more evidence as to what extent the railway operation system is safe. The importance of risk assessment and how it can be executed will be discussed in the next chapter.

Chapter 5

Quantitative Risk Assessment

Since the time and location of driver-related accidents are unknown and cannot be predicted, preventative measures must be applied in all cases to improve the safety level in railway systems, especially when there is the potential for driver errors.

In order to determine the extent to which the system is safe, quantitative risk assessment techniques should be applied to evaluate the risk accompanying the driver's tasks. This means estimating both the probability of the driver errors that lead to different accident scenarios and the consequences of these accidents.

Indeed, quantifying driver errors remains a very difficult issue because of the large number of factors affecting driver performance (i.e. PSFs), and the variability among persons, in addition to the lack of valid data on driver errors. These factors make modelling and quantifying these errors a complex process. A significant body of research exists to address and classify the factors that cause the occurrence of human error in railway systems; moreover, many methods and techniques have been used to quantify the risk associated with human tasks. In this chapter, more details about these subjects will be provided.

5.1 Performance shaping factors (PSFs) of train drivers

Following an extensive literature review related to performance-shaping factors (PSFs) of railway operators, it can be observed that several studies have been conducted in the field of human performance to determine and classify the PSFs that impact railway operators. It should be noted that these classifications are based on different views. Some examples will be presented to explain these differences.

The first example is a project drawn from the EPSRC Rail Research UK program. The projects conducted real investigations of experts and drivers to identify the factors that impact drivers' ability to maintain and perform their activities in detecting, recognising and acting on signals and signs. The results showed that the most important factors are route knowledge (training - familiarity), in-cab environment (noisy - comfortable), workload (high - low), and psychological components (e.g. vigilance - fatigue), as well as the procedures and violations [33].

A second study classified the important factors that cause human error in a different way. In this paper, the factors were classified into four categories: human habitude, the desire to do something without any reason, the physical condition of the driver (such as impairing effects of drugs or liquor), inefficient training, or sensory defects such as acuteness of hearing, colour-blindness,

acuteness of vision, illness, etc.), and the mental condition of the driver (e.g. any anxiety, depression, or other mental impairment) [8].

A third analysed about 479 reports of railway accidents and incidents to derive a list of 43 factors that contributed to human error. These factors were classified into seven main categories: dynamic personal factors, personal factors, task factors, team factors, organisational factors, system factors and environmental factors [9]. The researchers also investigated the interactions among these factors (dependencies); a dependency was established when at least one PSF has an influence on, or is influenced by another factor within the same category (inner dependency, such as that of fatigue on distraction) or in a different category (outer dependency, such as that of familiarity on distraction) [9].

The results obtained from these studies and research works can be used to highlight areas of concern, and subsequently to develop appropriate targeted mitigation measures that take into consideration the different PSFs and the dependencies among them.

5.2 Quantitative risk assessment methods and techniques

Quantitative risk assessment methods in the domain of human error aim to quantify human performance and calculate the probability that human errors will arise [34]. There are numerous methods used in human reliability analysis. The first generation of these methods focused on characteristics of the tasks themselves to estimate human errors [35], For instance, the technique of human error rate prediction (THERP) is considered one of the principal and most widely used methods for quantitative human reliability analysis [5], This technique aims to quantify human error probability (HEP) within different human tasks, such as those of a train driver. Another example of a first generation method is the human error assessment and reduction technique (HEART), which aims to analyse human tasks and identify their HEP value by applying a set of nominal HEPs and weighting factors [5]. The second generation of methods focuses on the contextual conditions (human factors) under which a given action is performed rather than the characteristics of the task itself [35]. One example, the cognitive reliability and error analysis method (CREAM), supposes that the probability of human error depends directly on the level of control that the human has over his actions [35], The degree of this control is assessed by the cognition model [5].

The main weak point in these methods (first and second generations) is that they neglect the interdependences among the PSFs despite high degrees of overlap being observed among them. This limited capability to model the dependencies and quantify their impact on human performance points to the importance of finding new methods that will be able to quantify both the human factors and their dependencies.

One example of these methods is the human performance railway operational index (HuPeROI), which was developed by integrating the analytic network process (ANP) and success likelihood index methodology (SLIM) techniques. This method aims to estimate the relative likelihoods of actions caused by human error for various operational scenarios by quantifying the impact of each factor on human performance and accounting for all dependencies, both direct and indirect, amongst these factors [9]. To enable this approach to provide error probabilities for the different types of erroneous actions, at least two calibration probabilities of erroneous actions should be defined [9].

Another approach is the Bayesian network (BN), which is characterised by its ability to model uncertain things (e.g. random variables), use different sources of data (e.g. expert judgements and historical data) to score its variables, and include the dependency among its variables in an effective and practical way [36]. This characteristic makes BN the best choice for modelling and quantifying driver errors. Moreover, BN is considered one of the best methods for modelling systems with complex structure because it depends on a causal and graphical model with explanatory and predictive capability. This enables us not only to predict the probability of hazardous events, but also to explain why such hazardous events can happen [37]. This property makes BN an appropriate choice for modelling systems such as ERTMS.

Given the various advantages of Bayesian network in modelling and quantifying both human errors and physical components of the ERTMS system, BN will be used in this thesis to estimate train driver errors and conduct safety assessments of the whole ERTMS system. More detailed information about the BN method will be presented in the next chapter.

Chapter 6

Bayesian Network

A Bayesian network (BN) is used to illustrate the causal relationships between key factors (causes) and one or more final outcomes in a system using a graphical model [5]. BN is a popular choice for qualitative and quantitative risk assessment in complex systems (e.g. computer science, railways, decision support systems, etc.) because of its ability to effectively incorporate multiple sources of data (from experts, observations, and accident investigations), as well as to include all types of dependencies into a single model in order to predict error probability [38]. It is therefore considered an efficient tool to describe the interactions among uncertain variables, and enables engineers to identify critical nodes in a model when it is updated by new information (evidence) [36].

A BN is composed of a directed acyclic graph (DAG) and conditional probability tables (CPTs). The DAG means that cycles are not allowed in the network. A BN is represented by a finite set of nodes (variables that a states or conditions) and a set of directed arcs (denoting causal influence between nodes), while CPTs are a set of conditional probability tables that express the strength of the relationships between the variables [5].

6.1 Directed acyclic graph (DAG)

A DAG consists of nodes and arcs. Nodes represent random variables. Two types of nodes can be recognised in DAG: a root node (parent node, i.e. does not have parents) and a child node (has one or more parents). Both of these are drawn as ovals or circles on the graph [5]. In general, the value of the random variable (state) is a discrete distribution with two or more possible states. The sum of the probabilities of all states within the same node must equal one. For instance, a node A that has two possible states would have the probabilities $Pr(A) = P$ and $Pr(\underline{A}) = 1 - P$. In many Bayesian network models, nodes have only two states to reduce the complexity of the computation [5].

For their part, arcs are direct links between nodes (parents and child) represent statistical dependences between variables (nodes). They also indicate the direction of influence, meaning that a value taken by child node depends on the values of its parent nodes [38].
An example of a Bayesian network diagram is shown in Fig. 11. In this figure, nodes A, B, and C are parents (root nodes), nodes D and E are children, and node F is the end node. To calculate the probabilities of each state of each node, the relationships and dependencies between nodes should be determined according to the following rules [5].

1- Node F will be independent of its ancestors when we know the states of its parents. This means that if the state of node D is known, knowledge about the state of node A will not provide any further information about the probability of the states of node F.
2- Nodes D and E are both influenced by node B, so they are seen to be dependent. However, in a Bayesian network, each node is considered as conditionally independent in the graph if the states of all its parents are known. Accordingly, calculating the probability of states of node D requires only knowledge about the states of nodes A and B.
3- When there is no arc between two nodes that means these nodes are conditionally independent. This situation appears between nodes D and E in Fig 11.

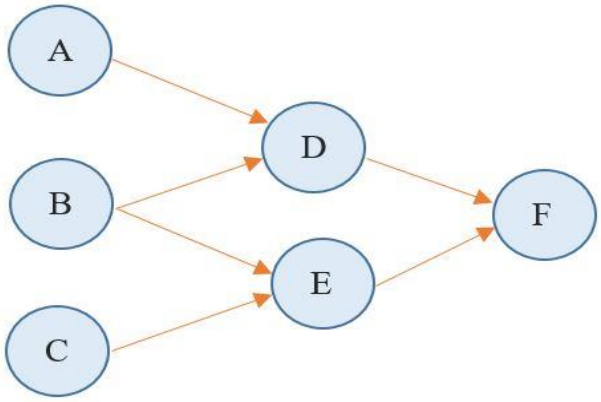


Figure 11: Bayesian network [5]

6.2 Conditional probability tables CPTs

A conditional probability table must be associated with every node in a Bayesian network to provide the probability of each state of the variable (node) based on the possible combination of the states of its parent nodes. Accordingly, the number of parent nodes determines the size of the conditional probability table. In the case where the node has no parents, its conditional probability coincides with its marginal probability [5]. The values included in CPTs depend on both experts opinion and available data [39]. An example of a conditional probability table is presented below. Taking node D in figure 11 as example, a conditional probability table for this node is displayed in Table 3. It is assumed that the variables of nodes A, B and D have only two possible states (0 and 1) and that necessary data to build CPTs is available. From the table, it can be observed that the sum of probabilities of all states for node D in each row is equal to 1. The equation used to calculate the probability of node D being in state (1) is as follows [37]:

$$\Pr(D=1) = \Pr(D=1 \mid A=0 \cap B=0) \cdot \Pr(A=0 \cap B=0) + \Pr(D=1 \mid A=0 \cap B=1) \cdot \Pr(A=0 \cap B=1) + \Pr(D=1 \mid A=1 \cap B=0) \cdot \Pr(A=1 \cap B=0) + \Pr(D=1 \mid A=1 \cap B=1) \cdot \Pr(A=1 \cap B=1)$$

Table 3: Conditional probability table for node D

Parents		**Pr (D = d | Parents)**	
A	B	1	0
0	0	0.1	0.9
0	1	0.15	0.85
1	0	0.70	0.30
1	1	0.85	0.15

6.3 Building the Bayesian network model

Developing a Bayesian network model involves four steps [40]:

1- Specifying the end node (hazardous event) and identifying the variables (nodes) that may influence the end node;
2- Identifying the arcs that represent the relationships (dependencies) between the variables (nodes). After this step, a qualitative structure of Bayesian network is built;
3- The states of each node should be defined;
4- The marginal or conditional probability table is assigned to each node. This means that the quantitative information is determined, after which a numeric calculation is executed.

In many applications where the Bayesian network model is applied, human factors can be included and modelled. Accordingly, a Bayesian network can be considered an adequate approach for analysing safety in a complex system where human errors are taken into consideration.

The Bayesian network is considered a suitable approach to model human performance (for instance, train driver in a railway system), because it has the ability to [37]:

1- Use multiple sources of data to estimate the values of PSFs;
2- Include different PSFs with various probability distributions (different numbers of states) in the model;

Take dependency among PSFs into consideration;

3- Determine which PSFs have a significant influence on the final risk.

In the next chapter, the techniques and methods identified in the above literature review are implemented via a case study, which discusses the event of passing a red signal (also known as signal passed at danger, or SPAD) in the ERTMS system levels 1 and 2. In this case study, a quantitative safety analysis including human errors will be conducted using a Bayesian network.

Chapter 7

Case Study

Train drivers safely pass tens of thousands of signals every year. Only on very rare occasions does a signal passed at danger (SPAD) event occur; if this happens, a serious accident (collision or derailment) with many fatalities could ensue. One effective way to improve railway system safety is to diagnose the causes of SPAD and treat them properly. Field investigations and analysis of data from previous accidents show that most SPADs occur due to a combination of operational factors, environmental conditions, factors associated with human performance, and interactions between components themselves [41].

Therefore, the basics of evaluating safety in a railway system regarding SPADs, where ERTMS operational levels 1 and 2 are used, involve identifying the associated hazards by taking a wide range of factors into consideration (especially factors associated with human behaviours) and conducting a quantitative safety analysis by calculating the probabilities of hazardous events occurring.

Since the ERTMS operational levels 1 and 2 are used in our case, it makes sense to collect information about the systems and technologies used to prevent, correct, or contain driver errors.

7.1 European railway traffic management system (ERTMS)

European railway sectors have different signalling and control systems in different European countries. As these systems were developed on a national basis without common technical and operational standards, there are more than fifteen different railway signalling systems currently in existence throughout Europe [25]. These differences in systems create a significant challenge for the interoperability of trains across Europe and have created a need for the development of a set of new, common functional and technical specifications in order to ensure railway interoperability across Europe and enhance safety in railway transportation; this is particularly importance given the emergence of high-speed trains [25]. Many groups and projects have been set up to develop various traffic management and train control specifications in order to fulfil new railway system requirements. The major project resulting from these efforts is called ERTMS. The ERTMS is a recent European standard for modern railway systems that aims to improve the safety, reliability, performance, and interoperability of European rail network [42]. ERTMS system consists of heterogeneous, distributed components that are classified into three groups [43]:

- **European Train Control System (ETCS)**, which includes a signalling system consisting of an onboard train subsystem and trackside infrastructure and is responsible for the safe movement of trains;

- **European Traffic Management Layer (ETML)**, which is a traffic management system aimed at optimising the flow over the network;
- **Global System for Mobile Communications for Railway (GSM-R)**, which is an international wireless communications standard that allows for radio communication between the two on-board ETCS subsystems and trackside infrastructure.

According to many articles and authors, ETCS and GSM-R are considered the most important parts of ERTMS. The ERTMS/ETCS specifications define four application levels of ERTMS/ETCS operation; the main difference between these levels is the manner of interaction between trackside equipment and the trains [25]. Different equipment is used at each level and three main subsystems can be recognised [43], these subsystems are:

- **Lineside subsystem**: aims to provide geographical position and movement authorities to the on-board subsystem;
- **On-board subsystem**: located on the train and responsible for control activities;
- **Trackside subsystem**: monitors the trains' movement.

These subsystems and their components are shown in Fig. 12. A brief description of these subsystems and components will be presented below.

7.1.1 The lineside subsystem

The lineside subsystem, which is distributed in every block section along the tracks, consists of EuroBalise (Balise), Euroloop (Loop), and Lineside Electronic Unit (LEU). It communicates with on-board and trackside subsystems to provide the necessary information to trains in every block section [43].

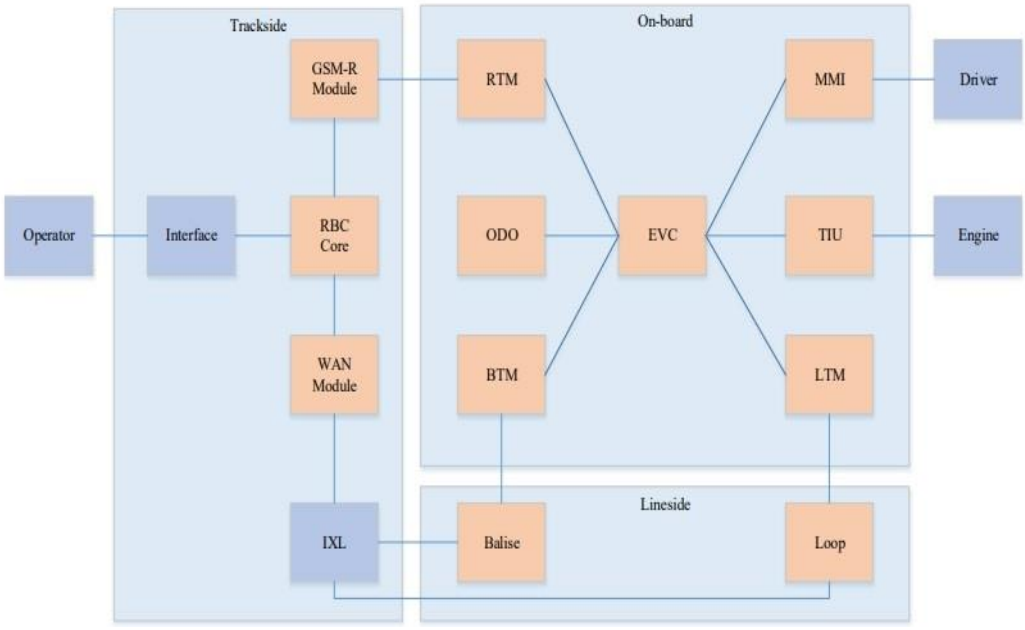


Figure 12: ERTMS/ETCS architecture [1]

EuroBalise (Balise)

An electronic device placed between the track lines. They are organised into groups of two or more. It is used as a discontinuous unidirectional communication system from the lineside to the on-board for sending messages/telegrams about the position of train, and can also be used as a milestone for detecting train location. In addition, it has ability to receive information from the trackside subsystem [43].

EuroLoop

An extension of EuroBalise used to replicate the Balise message over a longer distance.
It can be employed in the ETCS Level 1 only [43].

Lineside Electronic Unit (LEU)

Consists of some electronic devices. It is used in ETCS Level 1 only as interface between the EuroBalise and trackside equipment [1].

According to Level 1 specifications, the communication between trains and the trackside subsystem occurs via signals transmitted using EuroLoop and EuroBalise. In Level 2 specifications, the main communication system is EuroRadio protocol using GSM-R within specific frequencies [43].

7.1.2 Onboard subsystem

The main function of the onboard subsystem is ensuring the safe movement of trains by notifying the driver and starting the proper braking procedure when a dangerous situation occurs. It also calculates the speed profile using necessary information such as train and track characteristics and movement authorities (permission to cross one or more block sections), which are received from the trackside subsystem [1]. The onboard subsystem is mainly composed of seven components (European vital computer, man-machine interface, train interface unit, odometer system, radio transmission module, loop transmission module, and Balise transmission module). More details about these components will be provided later in this section.

European Vital Computer (EVC)

EVC, the onboard computer that forms the core of the onboard subsystem, aims to control all the train's functions to guarantee the safety of traffic. Its functions are based on both the information received from the trackside subsystem and the data from onboard sensors. It interacts with the driver through MMI. It is designed to be a fail-safe computing system [43].

Man-Machine Interface (MMI)

Sometimes called the driver-machine interface (DMI) [43], MMI is used to provide an adequate interaction between the train driver and the on-board subsystem by displaying signals and indicators on the monitor, as well as enabling specific functions via a series of keys and buttons.

Train Interface Unit (TIU)

An interface unit between onboard subsystems and the train. It receives signals from the train (such as the forward signal, the backward signal, brake feedback and so on), forwards them to EVC and then receives information from EVC (such as braking applied instructions, traction removal instructions and so on) that it forwards to different devices on the train [44].

Odometer system (ODO)

A technique for estimating the train's speed and position based on the data received from several types of sensors (wheel angular speed sensors, radar Doppler speed sensors and mono-axial accelerometers) [45].

Radio Transmission Module (RTM)

A link between the GSM-R network and mobile train radio device. It uses EuroRadio protocol and operates within GSM-R frequency range [43].

Loop Transmission Module (LTM)

Reads the data from the track loop via EuroLoop protocol [43].

Balise Transmission Module (BTM)

Reads data from Balises via EuroBalise protocol [43].

It can be observed that three types of communication protocols (EuroRadio, EuroLoop, and EuroBalise) are used by onboard components for communicating with other subsystems.

7.1.3 The trackside subsystem

The trackside subsystem aims to monitor and control the movements of trains to ensure a safe distance between them. This can be achieved by sending and receiving data from onboard subsystems at regular intervals. The subsystem consists of four major components, which are concentrated in some locations: these components are the Radio Block Centre (RBC) (level 2 only), GSM-R (level 2 only), Wide Area Network (WAN), and the interlocking system (IXL)) [43]. The most important components in this subsystem are the RBC and GSM-R.

Radio Block Centre (RBC)

A computer-based system designed to control railway traffic in ERTMS Level 2 by receiving information such as block occupancy, route set, etc. from the interlocking system (IXL) and then sending messages (including movement authorities) to trains within its controlled area. The RBC uses two types of communication to exchange data: GSM-R, to communicate with the onboard subsystem, and WAN, to communicate with other RBCs or interlocking systems [1].

The information is exchanged among RBCs to maintain the continuous train operation. The exchange train from one RBC to another is called 'handover'.

GSM-R

A radio communication system that allows the transmission of voice and data between track and train in ERTMS Level 2, using a specific range of frequencies dedicated for railway applications [1]. The communications between train and RBC via the GSM-R system are shown in Fig 13.

The ERTMS/ETCS system has four application levels, these levels are defined according to the type of equipment utilised and the way information is exchanged between the trackside and onboard units, as well as the process of their respective functions [1]. The levels are well-defined according to the infrastructure and required performance. This case study will focus on only two levels of the ERTMS/ETCS, namely levels 1 and 2.

Figure 13: Exchange the information between RBC and Train

7.1.4 ERTMS/ETCS - LEVEL 1

A signalling system designed to be compatible with conventional signalling systems and that aims to provide automatic train protection functions (ATP) by using Balises (Eurobalises) and transmission loops (Euroloops) [46]. ERTMS/ETCS level 1 with its different components is shown in Fig 14. It can be observed that lineside signals and train detectors are maintained, while communication between trackside and train is ensured by Balises (Eurobalises), which are located along the track next to lineside signals at required distances and connected to the train control centre through the lineside electronic unit (LEU). Their role is to transmit track description data and movement authority to the onboard subsystem. The onboard computer (EVC) continuously monitors and calculates the maximum speed of the train and the braking curve, as well as determining the next braking point if needed. This is achieved by relying on train braking characteristics and the data sent by Balises [25]. This information is displayed on the MMI to make it available to the driver.

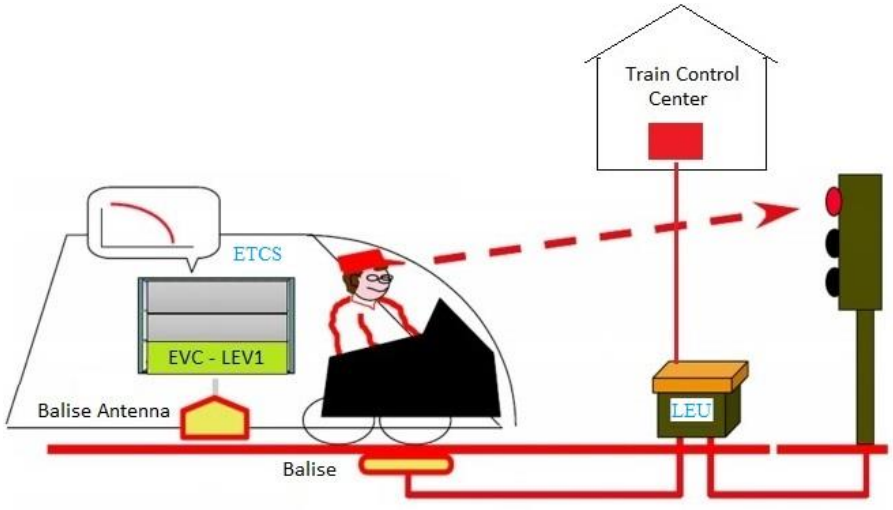


Figure 14: ERTMS/ETCS Level 1

7.1.5 ERTMS/ETCS - LEVEL 2

A digital radio-based signalling system functioning as a train protection system. Accordingly, all necessary data, such as speed profile and movement authority (which depends on track-specific data and the status of specific signals identified by using conventional track circuits on the route ahead) are transmitted to the EVC unit directly from an RBC via the GSM-R link. The Euroradio protocol is used to achieve this link. From the other side, the exact position, speed, and direction of the train is sent periodically to RBCs from the onboard system via GSM-R link [43]. ERTMS/ETCS level 2 is thus a highly sophisticated system that monitors the train's travel and advises the driver if he passes a red (danger) signal or exceeds a speed limit. In this system, lineside signals are optional and Balises are used only as reference points for correcting distance measurement errors; this is because their functions are limited to the transmission of static messages, such as location, track profile and speed limit, to the onboard subsystem [25]. ERTMS level 2 is the most popular and highly recommended train control system, as it improves safety and increases the line capacity by reducing headways and enabling higher operational speed. The structure of ERTMS/ETCS level 2 is shown in Fig 15.

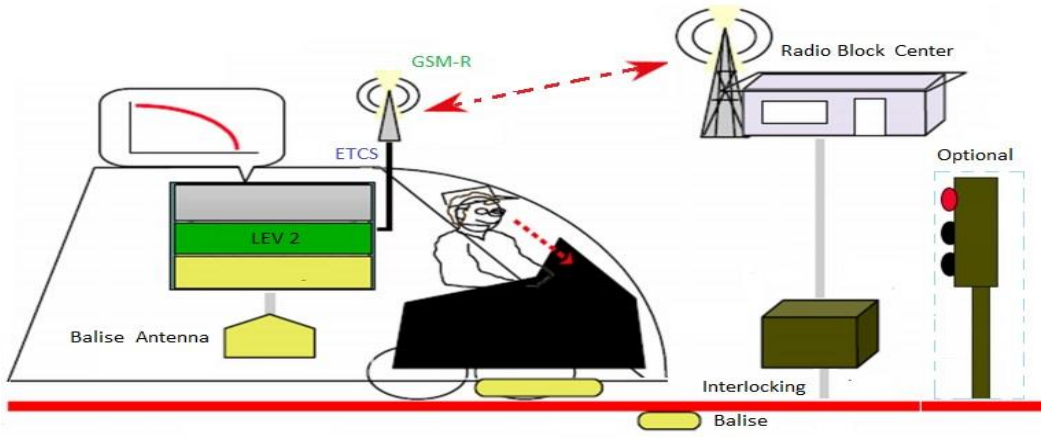


Figure 15: ERTMS/ETCS level 2

A summary of the various equipment needed for ERTMS/ECTS operation levels 1 and 2 is presented in Table 4.

Table 4: Equipment used in ERTMS/ECTS operation levels 1 and 2

ERTMS/ECTS Operation level	Data Transmission	Lineside Electronic units	Lineside Signals	Track Circuits	Radio Block
Level 1	Balises + Loops	Yes	Yes	Yes	No
Level 2	Balises + Radio	No	No	Yes	Yes

Now that a basic overview of the components and functions of ERTMS/ETSC operational levels 1 and 2 has been provided, it is important to understand the concept of Signal Passed at Danger (SPAD) in the railway system.

7.2 Signal Passed at Danger (SPAD)

In order to understand how SPADs can occur, it first is necessary to understand the concept of a 'block' and the signalling systems in the operational environment of train driving. Railway lines around the world are divided into sections called blocks, each of which is protected by a signal. Accordingly, permission to enter the next block can be given to the train if and only if there is no other train in that block (a 'clear block') and the train's route is set correctly. In this case, the signal protecting the block is set to green; on the other hand, if a block is not clear, the signal protecting the block is set to red and the signal before is set to yellow (a yellow signal pre-alerts the train driver that the next signal will be red) [41].

However, the whole signalling mechanism is designed to be a fail-safe system (signals are set to red in case of problems). When the train fails to stop at a signal set to danger (a red signal), such an event is called signal passed at danger (SPAD). The responsibility for respecting the signal status is assigned to the train driver, as well as a protection system that brakes the train automatically when required.

Indeed, a train may need over a kilometre to stop; this is the rationale behind the rule that braking should be started at the point at which a yellow signal is reached. The distance a train requires to stop depends on the characteristics of the train, track, braking, and adhesion levels between train and track. That means that drivers must have a high level of attention and vigilance, and should get adequate training to allow them to understand the trains they operate. An illustration of signal spacing and braking performance is shown in Fig 16. The driver behaviour can be described as follows: if the signal sets to green, the driver does not have to take any action; if it sets to yellow, the driver must reduce speed to be ready to stop at the next signal; if it sets to red, the driver must stop before the next signal.

It can be observed that driving a train requires the drivers to perform many tasks, including paying close attention to the line ahead at all times, checking signals and the speed limit, understanding the information displayed, and controlling the speed of the train appropriately.

The scenario that will be studied in our case is as follows: a passenger train operating during the day; conditions of weather and visibility at the time of operation are good; no technical failures in the track itself or in the rolling stock, including the brake system. This means that the scope of analysis is limited to train driver errors and failures in the control and signalling system (ERTMS/ETCS levels 1 or 2) that might lead to SPAD. The operation mode is a full supervision mode; in this mode, the on-board ERTMS/ETCS equipment is responsible for train protection.

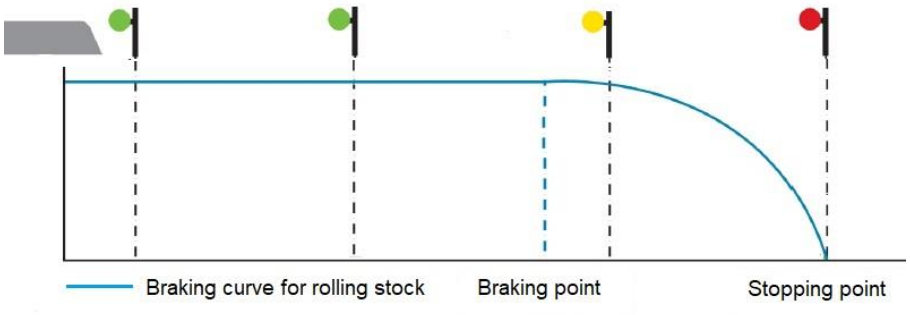


Figure 16: Signal spacing and train braking performance

7.3 Identifying hazards using STPA

The STPA method will be applied in our case study to identify the hazards that could lead to SPAD in both ERTMS/ETCS operational levels 1 and 2. In fact, this process of using the STPA method will be similar at both operational levels.

The consequences of an accident when SPAD occurs are also the same. These sequences are:

- Death, injury, and/or property damage resulting from a collision with another train.
- Injury or property damage occurring within the train because of incorrect braking technique (without a collision).

As we know, the process of hazard identification using STPA consists of five steps. These steps are as follows:

1- Hazardous events
   - The train enters a new block even though the signal is red, which may cause a collision. [H-1]
   - Incorrect braking technique (sudden braking) when there is a red signal for the next block, which subjects the passengers to sudden high forces that may lead to injuries. [H-2]

2- Safety constraints
   - The train should not enter the next block when the signal is set to danger (red signal) [SC-1]
   - The brakes should be used correctly (gently) during train braking when the signal is set to danger (red signal) [SC-2]

3- Hierarchical safety control structure
   This structure includes the components of the ERTMS/ETCS levels 1/2 and the interactions between them, as well as the interactions between the components and driver. This structure is shown in Fig 17 for ERTMS/ETCS level 1, and Fig 18 for ERTMS/ETCS level 2.

It can be observed that there is a difference between the functional requirements of the driver and functional requirements of the controller. The functional requirements of the driver are:

- Detect when the line signal is yellow (the next will be red) and activate the brakes;
- Apply the brakes correctly (gently) and ensuring the train stops before the next block.

While the functional requirements of the controller are:

- Detect when there is a need for braking and the driver does not brake;
- Respond to a need for braking by applying the braking correctly (gently) and ensuring the train stops before the next block.

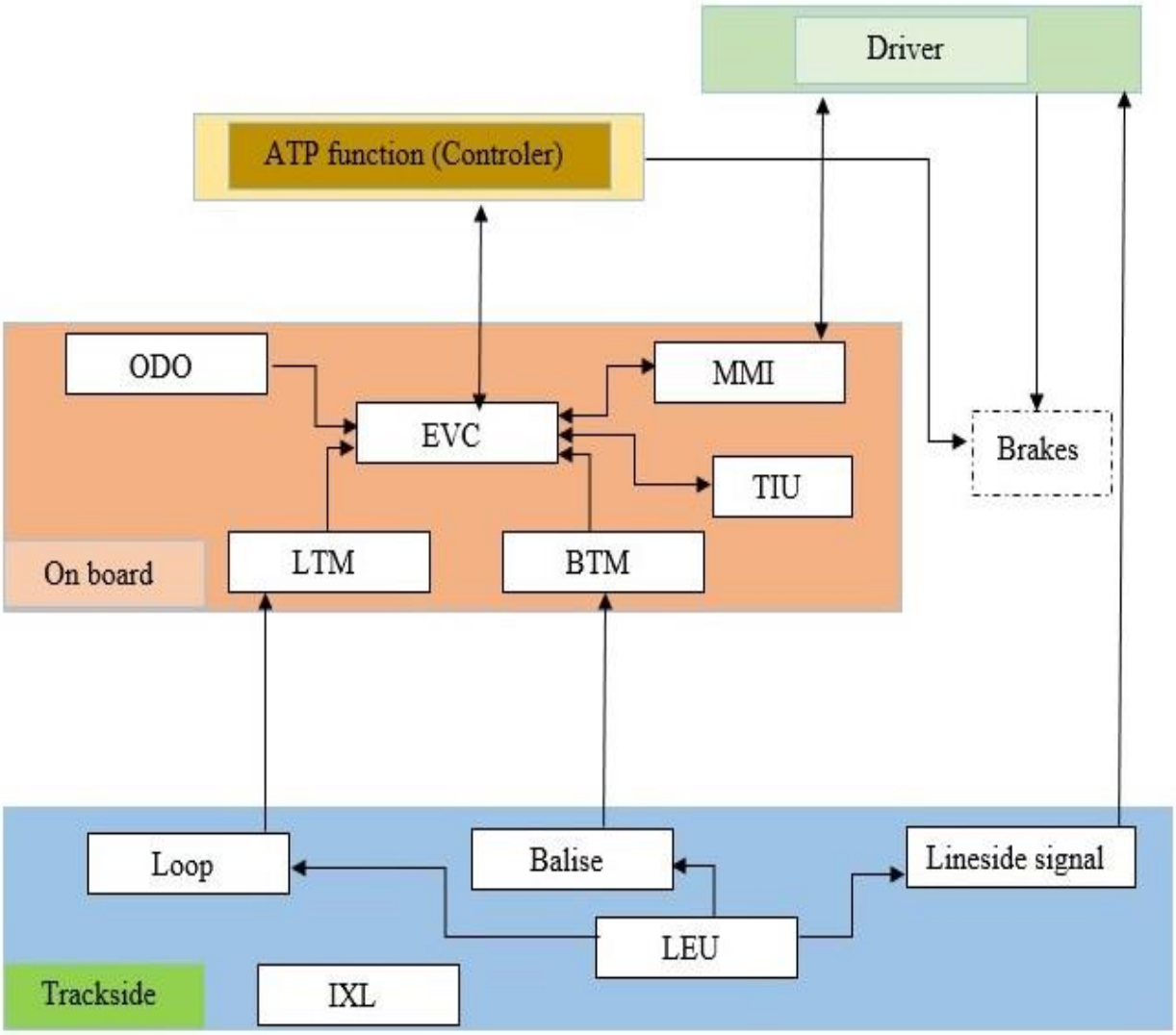


Figure 17: Hierarchical safety control structure of ERTMS/ECS level 1

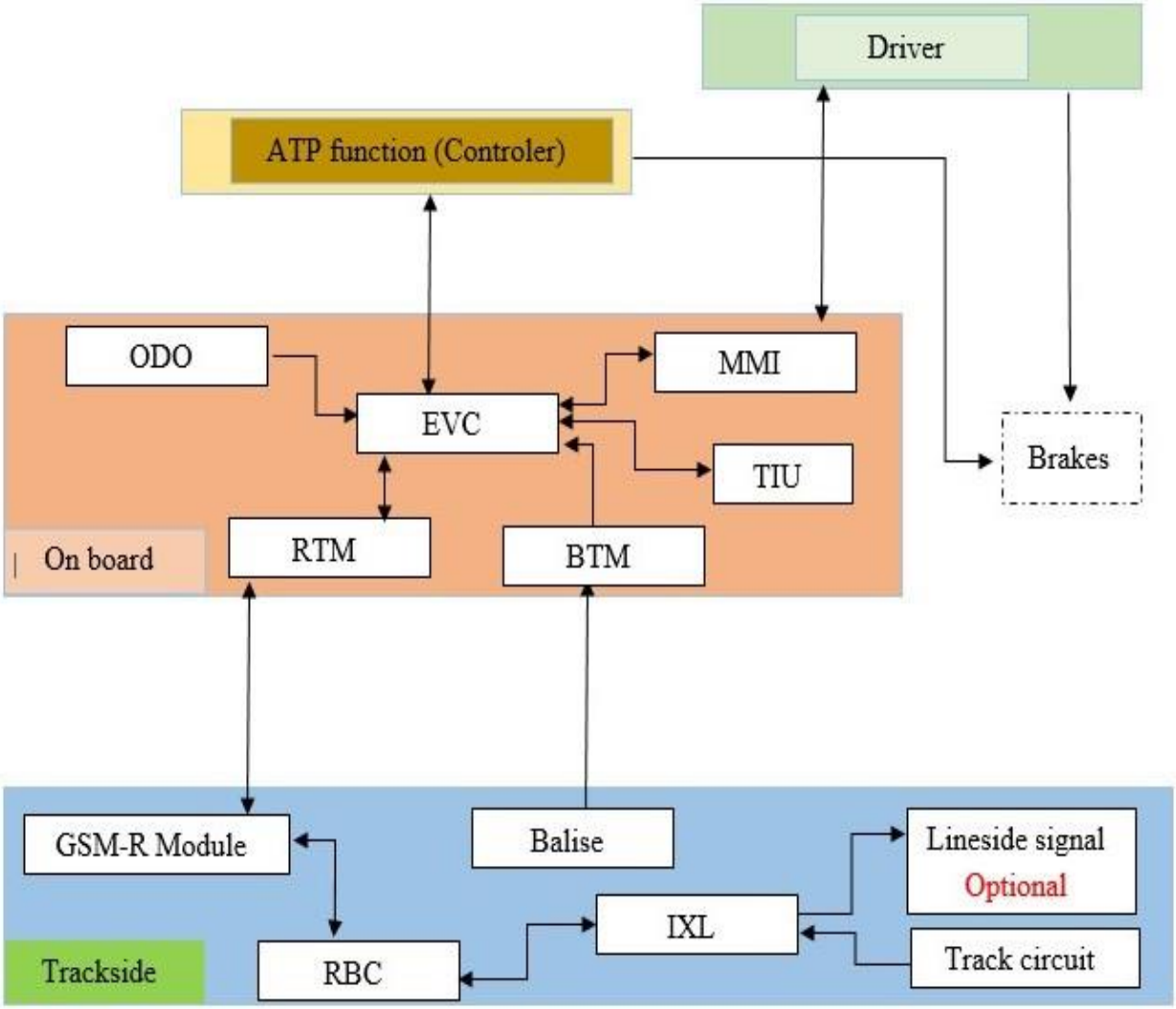


Figure 18: Hierarchical safety control structure of ERTMS/ECS level 2

4- Identifying unsafe control actions (UCAs)

The driver is responsible for braking, while the ATP is responsible for protecting the train; this means that it steps in when the braking is not applied by the driver as needed. For the two hazardous events [H-1] and [H-2], the unsafe control actions of both the driver and the ATP will be examined to identify instances in which safety constraints may be violated. UCAs may in fact be caused by various scenarios, including driver errors, component failures, unexpected interactions between components, and missing or delayed feedback from sensors. Table 5 presents UCAs identified for braking actions in ERTMS/ETCS levels 1/2. The UCAs for both ERTMS/ETCS levels 1 and 2 are identical because the braking action is identical; the difference between these two systems is limited to the communication between onboard and trackside components.

Table 5: Unsafe control actions related to braking in ERTMS/ETCS levels 1/2

	Not providing causes hazard	Providing causes hazard	Wrong timing causes hazard	Stop too soon / Applied too long
Brake (Driver)	Driver does not brake when the next signal is red. [H-1]	[Not hazard]	Driver brakes too soon when the next signal is red [not hazard]. Driver waits too long to brake when the next signal is red. [H-2] , [H-1]	Driver continues braking for too long when the next signal is red. [not hazard] Driver does not brake for long enough to avoid SPAD when the signal is red. [H-1]
Brake (ATP)	ATP does not brake (when the next signal is red, and driver did not brake). [H-1]	[Not hazard]	ATP brakes too soon (when the next signal is red, and driver did not brake). [Not hazard]. ATP waits too long to brake (when the next signal is red, and driver did not brake). [H-2] , [H-1]	ATP continues braking for too long when the next signal is red, and driver did not brake). [not hazard] ATP does not brake for long enough to avoid SPAD (when the signal is red and driver did not brake). [H-1]

5- Determining how Unsafe Control Actions could occur (identifying causal scenarios)

Here we will look at only some examples (not all) of causal scenarios related to the unsafe control actions mentioned in table 5. The UCAs are:

- UCA1: “Driver does not brake when the next signal is red”.

One of the various scenarios related to UCA1 can be described as follows: UCA1 may occur when the driver fails to brake because he expects that the next signal will be green (does not notice the yellow signal (lineside - level 1, in cab - level 2)).

The first scenario explaining the driver’s behaviour is that the driver has familiarity with this route and the signal was green at all previous times when he passed it, so the driver thinks the signal will be green this time as well (an incorrect belief about the current state of the system). This belief is formed from his expectation, and he selects the control action depending on his current mental model of the process (knowledge-based decision).

The second scenario for UCA1 is that the driver does not check the status of the signal because he believes the ATP system is active and that there is no failure in the ERTMS/ETCS system; this entails that the ATP system will apply the brakes if requires. The driver arrives at this belief because he incorrectly supposes that ERTMS/ETCS is capable of constantly conducting self-diagnosis and will alert him if there is any failure. In reality, however, this is not the case (driver has an incorrect belief about what the system can do).

Many other scenarios can be used to describe the causes of UCA1. In general, a range of factors (such as fatigue, inattention, expectation, and lack of training) could contribute to the occurrence of UCA1.

- UCA2: “ATP system does not react appropriately to the driver’s behaviour (driver does not stop train when required)”.

The ATP system will be responsible for applying the train’s brakes when braking is necessary and the driver has failed to do it. There are many possible scenarios for UCA2 arising in response to one or more failures in the ERTMS/ETCS system. These failures could result from any of the parts of the system (components, communication channels, and missing or delayed feedback from sensors); these failures vary according to the ERTMS/ETCS operational level.

For level 1, failure can occur if the data indicating the need to brake is not sent to ATP function (controller) from EVC (because of failure in EVC itself). Also, a UCA2 could result if the command to activate the brakes does not reach the brakes (failure in ATP function (controller) or in the communication channel between the controller and brakes). Moreover, the failure can occur if information about the status of the next block does not reach the EVC at all; this could happen due to a failure in one or more components (track circuit, IXL, LEU, LTM, and BTM) or communication channels (Balise - BTM, Loop - LTM, BTM - EVC, and LTM - EVC).

For level 2, the failure related to EVC and ATP function can occurred in a similar way as for level 1. However, the failure which prevents the status of the next block from reaching the EVC occurs in a different way, either because of the failure in one or more components (track circuit, IXL, RBC, GSM-R module, and RTM) or in one of two communication channels (GSM-R module – RTM and RTM - EVC).

- UCA3: “Driver waits too long to brake when the next signal is red”.

There are many potential scenarios in which this UCA3 might arise. For example, the driver knows the next signal is red and the ERTMS/ETCS system displays (via MMI) the speed profile and correct point for beginning to brake. However, the driver does not begin to apply the brakes at the correct point because he does not trust the system (incorrect mental model about what the system can do); alternatively, depending on his information about the current state of the system, he may believe incorrectly that characteristics of the train and its brakes allow him to start braking after more time has elapsed (lack of training).

The second scenario is that the driver knows the next signal is red, but he has neither sufficient experience nor training to recognise the information provided by the ERTMS/ETCS system that illustrates the speed profile and determines the point at which braking should commence. Consequently, the driver depends on his limited experience to determine when to apply the brakes (driver has insufficient information about the current state of the system).

The third scenario is that the driver doesn’t recognise the status of the next block because he is affected by fatigue, tiredness, or similar. Consequently, he does not know that the next signal is red at the correct time (wrong belief about the process state). After a while, the driver recognises his mistake and starts to heavily apply the brakes.

- UCA4: “ATP waits too long to brake when the next signal is red”.

In UCA4, the ATP system fails to apply brakes at the correct time due to a failure in the ERTMS/ETCS system. Indeed, there are many possible scenarios for UCA4. For ERTMS/ETCS system operational level 1, the failure can appear if the data from EVC incorrectly indicates to the ATP function (controller) that the train’s current speed is less than its actual speed (due to a failure in the EVC itself or feedback about the current speed from the ODO being inaccurate); alternatively, the data indicating the brakes should be applied is sent late to the ATP function (controller), which can occur due to long data processing time in the EVC or a significant delay before sending movement authorities from LTM or BTM to EVC. Another source of failure is a delay in sending a brake activation signal from ATP to the brakes.

For level 2, this failure can occur in a similar way as for level 1, but the main differences are in the trackside components and communication channel. Thus, the failure can result from a delay in RTM before sending the movement authority to EVC, extended data processing time in IXL and/or RBC before producing the movement authority sent to the GSM-R module, or a delay in communication channels (for example, the channels between the GSM-R module and RTM (GSM protocol) or between the track circuit and IXL (WAN network)).

- UCA5: “Driver does not brake for long enough to avoid SPAD when the signal is red”.

There are many scenarios associated with UCA5. For example, the driver is fully aware of the status of the next signal, begins to apply the brakes at the correct point, and stops the train without SPAD; however, when the driver sees another train pass his train on the opposite side, he releases the brakes and starts to move the train, passing the signal at red (i.e. does not wait until the signal turns green). The causes of this behaviour can be attributed to either the driver’s goal to arrive at his destination as soon as possible without making safety his highest priority (lack of safety culture, incorrect policies in the organisation), or the driver having an inaccurate mental model about the system, incorrectly believing that the block is free because he saw another train pass him (weak rules and procedures). Alternatively, the driver may believe that the system needs some time to

turn the signal green after the block becomes free. However, this is incorrect; the system turns the signal green directly after the block becomes free and switch points are adjusted correctly (wrong belief about system behaviour).

- UCA6: "ATP does not brake for long enough to avoid SPAD (when the signal is red and driver did not brake)".

Here, the ATP system detects the red signal and starts to apply the brakes at the correct point to stop the train without SPAD. However, hazards appear if the ATP fails to apply the brakes until the next block becomes free due to a failure in the ERTMS/ETCS system. There are many possible scenarios from which UCA6 may arise. For the ERTMS/ETCS system operational level 1, the failure can appear either if the data from EVC incorrectly indicates to the ATP function (controller) that the brakes should be released (failure in EVC itself) or a failure in the ATP function leads to release of the brakes. UCA6 can also occur if there is a failure in the track circuit or IXL, leading to incorrect information about the status of the block being sent to EVC (block is free when it is not).

For level 2, the failure that leads to UCA6 can occur in a similar way to that in level 1, with the addition of a failure in RBC, which could lead to a 'release brakes' command being sent before the block becomes free.

It is worth mentioning that the track circuit is included within the scope of the case study, although it is outside of the scope of the ERTMS system.

7.3.1 Summary of the results of hazard identification

Regarding the different causal scenarios that lead to unsafe control actions, we can classify the causes of hazardous events [H-1], [H-2] for ERTMS/ETCS system operational levels 1 and 2 in a simplified manner, as follows:

- ERTMS/ETCS system operational level 1.

At this level, the system components and human errors that lead to hazardous events can be divided into three groups: major components, secondary components, and selecting unsafe control actions.

The major components group includes three elements: IXL, Truck circuit, and LEU. A failure in one component of this group (Error1) leads directly to a hazardous event because their functions impact both the driver and ATP.

However, if there is no failure in the major components group, the hazardous event will happen only if there are failures in both of the other groups (secondary group and selecting unsafe control actions) (Error2).

The components included in the secondary group are Balise, loop, LTM, BTM, ODO, EVC, and ATP function.

While the 'selecting unsafe control actions' group encompasses two elements (i.e. environment and mental model), the environmental element is itself affected by three factors (organisation policies, the driver's goals, and time pressure during the driver's decision selection). The mental model element is affected by two subgroups (knowing current data about the system and knowing what the system can do). Many other factors (such as tiredness, fatigue, expectation, familiarity,

training, and trust in system) and components (MMI, line signals) impact on these two subgroups. Fig 19 illustrates this model using a Bayesian network.

- ERTMS/ETCS system operational level 2

The same level 1 model can be used for level 2 with only minor changes. These changes include the major components and secondary components groups. The major components group in level 2 includes IXL, Truck circuit, RBC, GSM-R module and RTM, while the secondary components group encompasses ODO, EVC, and ATP function. The third group (selecting unsafe control actions) remains the same (only the line signal is neglected). Fig 20 illustrates this model using a Bayesian network.

Since the hazards related to SPAD in railway systems at ERTMS/ETCS system levels 1 and 2 have been identified, we can now suggest a model to represent the hazardous events associated with SPAD, taking into consideration the failure of components and driver errors. By using this model, we can quantify the safety of a railway system in the context of SPAD by using a Bayesian network.

7.4 Quantitative safety analysis regarding SPADs

A Bayesian network (BN) is a very effective method to map out all types of dependencies and illustrate the relationships between causes and final outcomes (i.e. hazardous events) in a system using a graphical model. A BN can quantify the safety assessment of a complex system by incorporating multiple data sources (experts, observations, and accident investigations). Consequently, it is considered a rational choice for this case study.

A Bayesian network model is built in three steps, as follows:

1- Building a Bayesian network diagram (including nodes and arcs)

This diagram consists of a directed acyclic graph showing the dependencies among the different factors by using arrows (links). To reduce complexity, in our case a simple model of the Bayesian network will be used. In this model, a driver's selection of a control action is impacted by many factors, such as tiredness, training, trust in system, etc. The action taken can be safe or unsafe; if unsafe, it can be corrected by the ATP system. Accordingly, Error 2 can happen only when there is both an unsafe control action and an error in the secondary group, while error 1 can happen only when there is a failure in one of the major group components.

2- Determining the states of root nodes and their probabilities

In our case, for simplicity, we will assume that all nodes have only two possible states, i.e. 1 and 0. Thus, node (X) = 1 if the event represented by this node happens and node (X) = 0 if the event does not happen. The probabilities of the events occurring over a period of 10^6 hours, which are represented by root nodes, are provided in table 6. These values will be used to analyse ERTMS/ETCS system operational levels 1 and 2.

3- Determining the conditional probability tables of other nodes

As we know, conditional probability tables are used to determine the probability of the states of each node. In our case, the values of these tables are arbitrary (experts or data analysis were not relied upon to determine the values of these tables). Since the number of parents of nodes determines the size of the conditional probability table for this node, the table size in our case will be no more than 4 or 8 rows, as the maximum number of parents is 3.

4- Calculating the probability of hazardous events

This calculations will depend on the values of the states of root nodes and the values in the conditional probability tables. In this case, Excel will be used to conduct this calculations.

- Bayesian network diagram

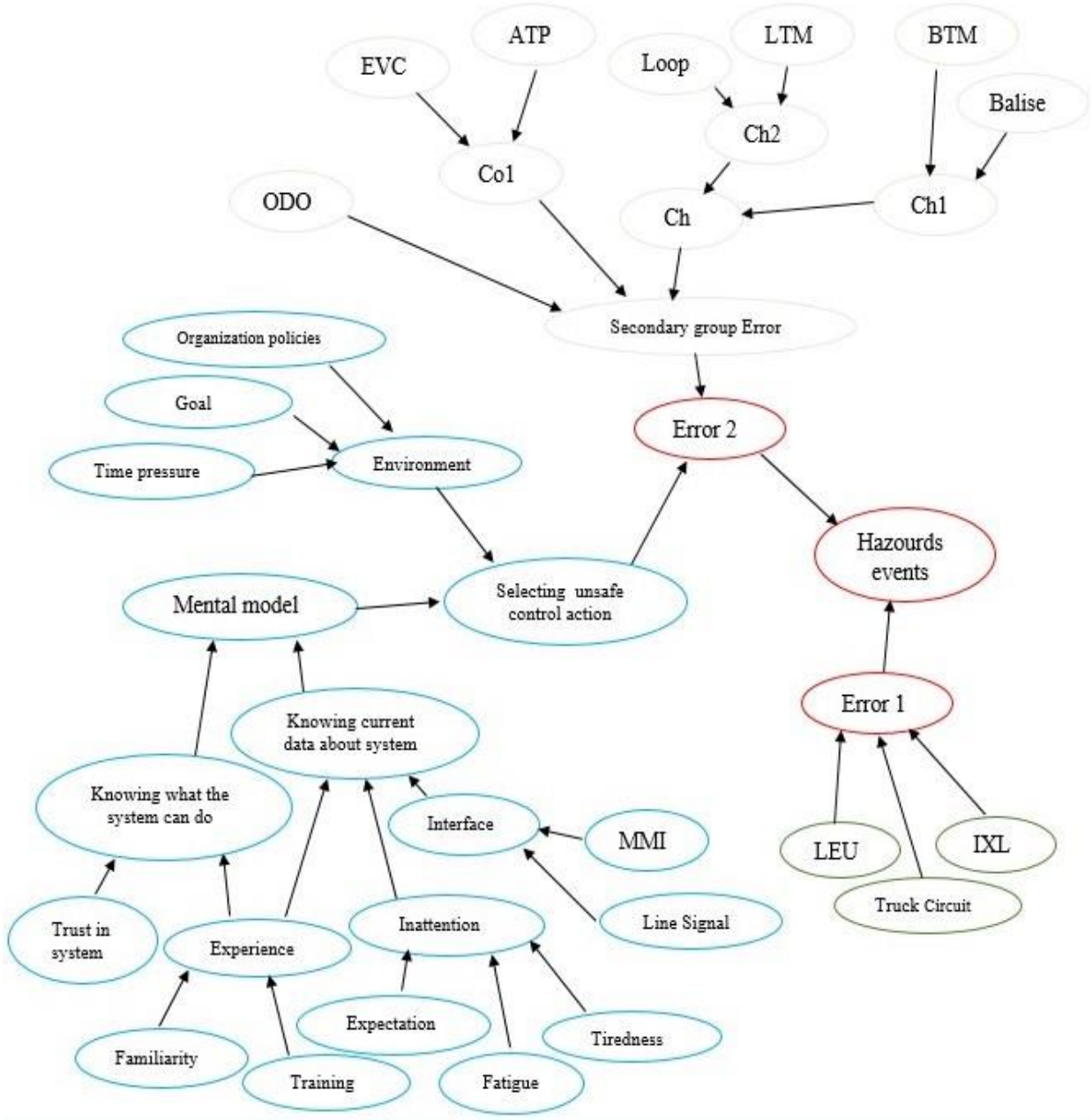


Figure 19: Model of hazardous events related to SPAD in ERTMS/ETCS level 1 using Bayesian network

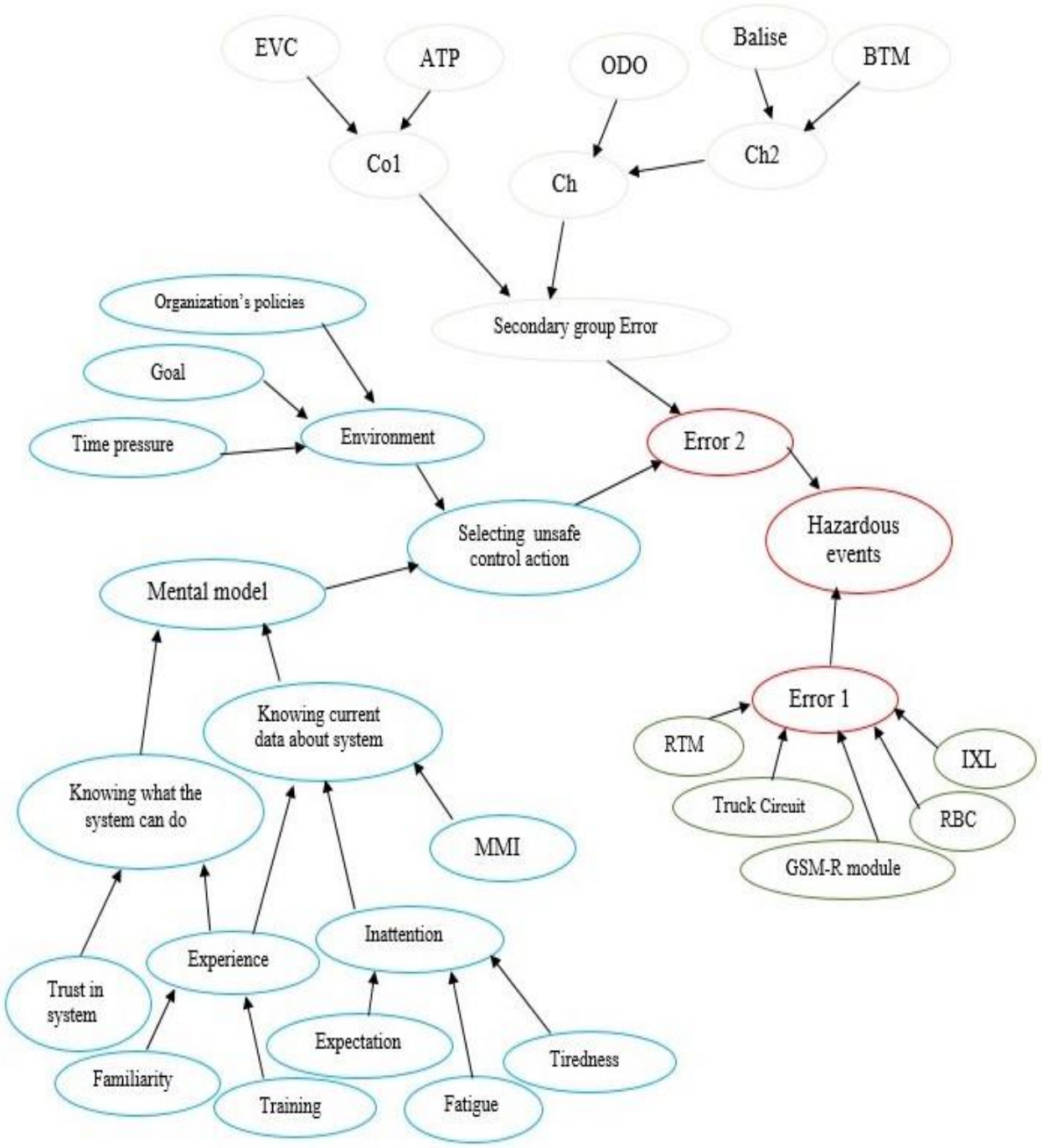


Figure 20: Model of hazardous events related to SPAD in ERTMS/ETCS level 2 using Bayesian network

- The probability of each state of root nodes.

Table 6: Probability of each state of root nodes in ERTMS/ETCS levels 1 and 2

The variable (Node)	Not happened Pr (X)	Happened Pr (X)	The event (Node)	Not happened Pr (X)	Happened Pr (X)
Tiredness	0.90	0.10	EVC (Failure)	0.98	0.02
Fatigue	0.85	0.15	ATP (Failure)	0.98	0.02
Expectation (bad impact)	0.90	0.10	ODO (Failure)	0.95	0.05
Training	0.15	0.85	Balise (Failure)	0.98	0.02
Familiarity	0.30	0.70	BTM (Failure)	0.98	0.02
Trust in system	0.15	0.85	RTM (Failure)	0.98	0.02
Goal (bad impact)	0.88	0.12	RBC (Failure)	0.98	0.02
LTM, LEU (Failure)	0.98	0.02	Loop (Failure)	0.98	0.02
IXL (Failure)	0.98	0.02	Truck circuit (Failure)	0.98	0.02
Time pressure	0.97	0.03	GSM-R Module (Failure)	0.98	0.02
MMI (Failure)	0.95	0.05			
Policies of organization (Bad impact)	0.86	0.14	Line signal (Failure)	0.96	0.04

- Determining the conditional probability tables
- Calculating the probability of each node: Using the following equation and the values for this equation, we can obtain these from the root nodes table and conditional probability tables.

If node X has two parents A and B, the probability of X = 1 is calculated as follows:

$$Pr(X=1) = Pr(X=1 \mid A=0 \cap B=0) \cdot Pr(A=0 \cap B=0) + Pr(X=1 \mid A=0 \cap B=1) \cdot Pr(A=0 \cap B=1) + Pr(X=1 \mid A=1 \cap B=0) \cdot Pr(A=1 \cap B=0) + Pr(X=1 \mid A=1 \cap B=1) \cdot Pr(A=1 \cap B=1).$$

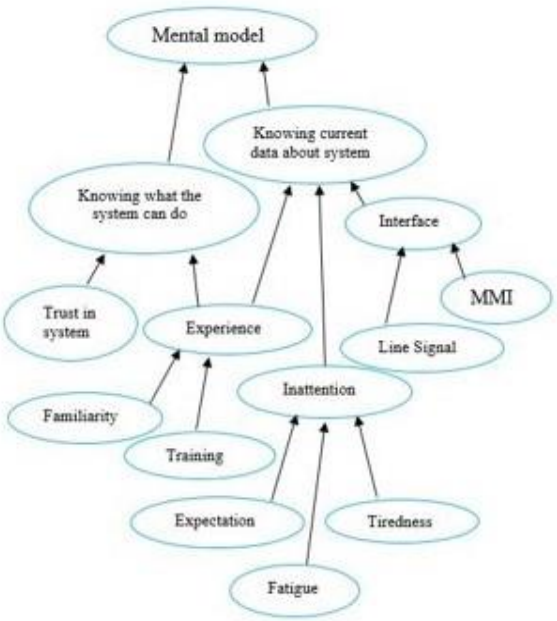
Moreover, the probability of X = 0 is calculated as follows:

$$Pr(X=0) = Pr(X=0 \mid A=0 \cap B=0) \cdot Pr(A=0 \cap B=0) + Pr(X=0 \mid A=0 \cap B=1) \cdot Pr(A=0 \cap B=1) + Pr(X=0 \mid A=1 \cap B=0) \cdot Pr(A=1 \cap B=0) + Pr(X=0 \mid A=1 \cap B=1) \cdot Pr(A=1 \cap B=1)$$

7.4.1 Quantitative safety analysis of ERTMS/ETCS level 1 related to SPAD

Tiredness	Fatigue	Expectation (bad impact)	Inattention	
			Pr (X)	Pr (X)
1	1	1	0.01	0.99
1	1	0	0.10	0.90
1	0	1	0.30	0.70
1	0	0	0.35	0.65
0	1	1	0.40	0.60
0	1	0	0.50	0.50
0	0	1	0.60	0.40
0	0	0	0.80	0.20

Training	Familiarity	Experience	
		Pr (X)	Pr (X)
1	1	0.05	0.95
1	0	0.25	0.75
0	1	0.40	0.60
0	0	0.85	0.15



Experience	Trust in system	Knowing what the system can do	
		Pr (X)	Pr (X)
1	1	0.20	0.80
1	0	0.35	0.65
0	1	0.40	0.60
0	0	0.95	0.05

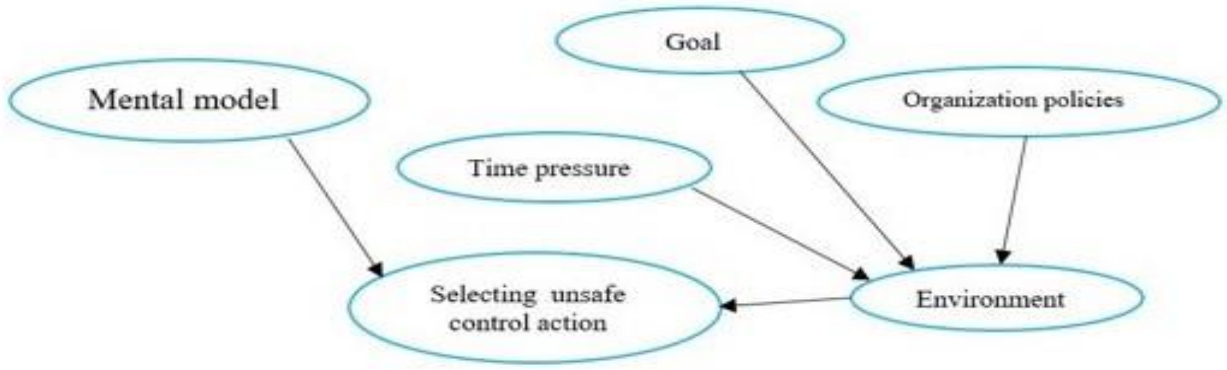
MMI (failure)	Line signal (failure)	Interface (failure)	
		Pr (X)	Pr (X)
1	1	0.00	1.00
1	0	0.20	0.80
0	1	0.30	0.70
0	0	0.95	0.05

Inattention	Interface (Failure)	Experience	Knowing current data about system	
			Pr (X)	Pr (X)
1	1	1	0.99	0.01
1	1	0	1.00	0.00
1	0	1	0.93	0.07
1	0	0	0.98	0.02
0	1	1	0.95	0.05
0	1	0	0.99	0.01
0	0	1	0.15	0.85
0	0	0	0.60	0.40

Knowing current data about system	Knowing what the system can do	Mental model	
		Pr (X)	Pr (X)
1	1	0.00	1.00
1	0	0.35	0.65
0	1	0.45	0.55
0	0	0.99	0.01

Figure 21: Model of mental model using Bayesian network and related conditional probability tables – ERTMS level 1

The probability of a correct mental model is 0.653546164, while the probability of an incorrect mental model is 0.346453836.



Goal (bad impact)	Time pressure	Organization's policies (bad impact)	Environment	
			Pr (X)	Pr (X)
1	1	1	0.99	0.01
1	1	0	0.92	0.08
1	0	1	0.90	0.10
1	0	0	0.85	0.15
0	1	1	0.70	0.30
0	1	0	0.60	0.40
0	0	1	0.50	0.50
0	0	0	0.10	0.90

Mental model	Environment	Selecting unsafe control action	
		Pr (X)	Pr (X)
1	1	0.97	0.03
1	0	0.60	0.40
0	1	0.55	0.45
0	0	0.05	0.95

Figure 22: Model of selecting unsafe control action using Bayesian network and related conditional probability tables - ERTMS level 1

The probability of a good environment is 0.74752672, while the probability of an environment that is not good is 0.25247328.

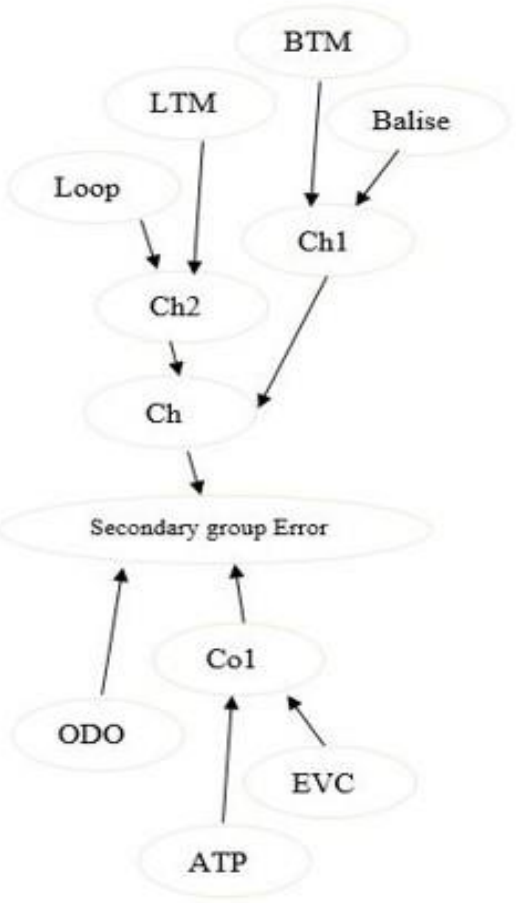
The probability of selecting a safe control action is 0.719703131, while the probability of selecting an unsafe control action is 0.280296869.

BTM (Failure)	Balise (Failure)	Ch1	
		Pr (X)	Pr (X)
1	1	1.00	0.00
1	0	1.00	0.00
0	1	1.00	0.00
0	0	0.00	1.00

Loop (Failure)	LTM (Failure)	Ch2	
		Pr (X)	Pr (X)
1	1	1.00	0.00
1	0	1.00	0.00
0	1	1.00	0.00
0	0	0.05	0.95

Ch1	Ch2	Ch	
		Pr (X)	Pr (X)
1	1	0.10	0.90
1	0	0.70	0.30
0	1	0.90	0.10
0	0	1.00	0.00

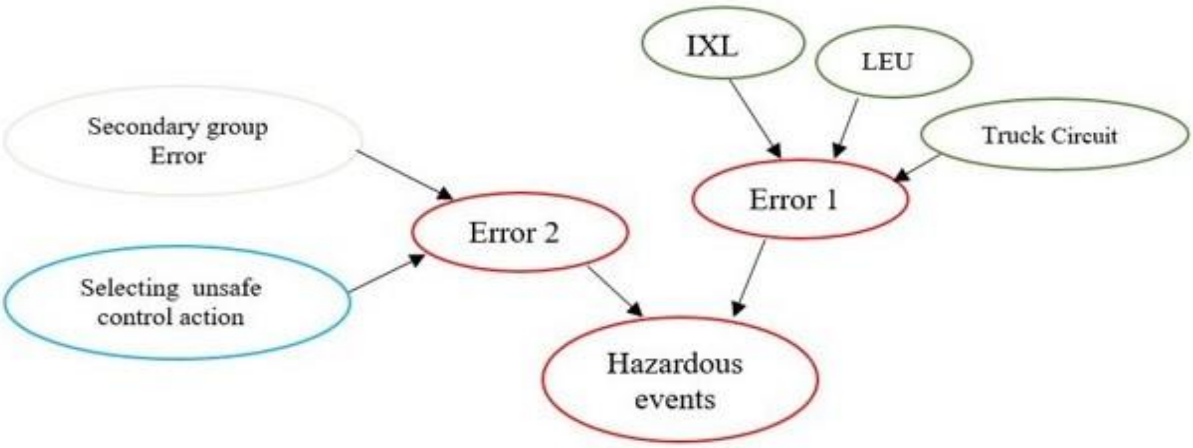
ATP (Failure)	EVC (Failure)	Co1	
		Pr (X)	Pr (X)
1	1	1.00	0.00
1	0	1.00	0.00
0	1	1.00	0.00
0	0	0.15	0.85



ODO (failure)	Co1	Ch	Secondary group error	
			Pr (X)	Pr (X)
1	1	1	0.85	0.15
1	1	0	0.00	1.00
1	0	1	0.00	1.00
1	0	0	0.00	1.00
0	1	1	0.90	0.10
0	1	0	0.00	1.00
0	0	1	0.00	1.00
0	0	0	0.00	1.00

Figure 23: Model of secondary group error using Bayesian network and related conditional probability tables - ERTMS level 1

The probability of secondary group error is 0.401058786



Selecting unsafe control action	Secondary group error	Error 2	
		Pr (X)	Pr (X)
1	1	0.00	1.00
1	0	1.00	0.00
0	1	1.00	0.00
0	0	1.00	0.00

IXL (failure)	LEU (failure)	Truck circuit (failure)	Error 1	
			Pr (X)	Pr (X)
0	0	0	1.00	0.00

Error1	Error2	Hazardous Event	
		Pr (X)	Pr (X)
1	1	0.00	1.00
1	0	0.00	1.00
0	1	0.00	1.00
0	0	1.00	0.00

Figure 24: Model of Hazardous events using Bayesian network and related conditional probability tables - ERTMS level 1

The probability of Error 2 is 0.112415522
The probability of Error 1 is 0.058808
The probability of a hazardous event is 0.16461259

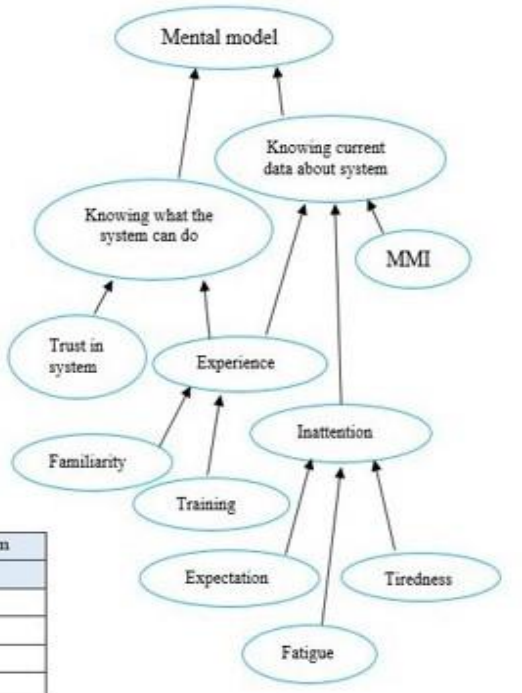
7.4.2 Quantitative safety analysis of ERTMS/ETCS level 2 related to SPAD

The quantitative safety analysis for ERTMS/ETCS level 2 is similar to that for level 1. The difference will be limited to some values in the conditional probability tables. Because level 2 involves continuous supervision of train movement with continuous communication, which is provided by GSM-R, this leads to a reduction in human errors, as the data will be available to the driver for a longer time, thus reducing the inattention and time pressure and giving the driver more time to make a correct decision. In our ERTMS/ETCS level 2 model, lineside signals are omitted.

Tiredness	Fatigue	Expectation (bad impact)	Inattention	
			Pr (X)	Pr (X)
1	1	1	0.15	0.85
1	1	0	0.30	0.70
1	0	1	0.45	0.55
1	0	0	0.50	0.50
0	1	1	0.55	0.45
0	1	0	0.70	0.30
0	0	1	0.80	0.20
0	0	0	0.90	0.10

Training	Familiarity	Experience	
		Pr (X)	Pr (X)
1	1	0.05	0.95
1	0	0.25	0.75
0	1	0.40	0.60
0	0	0.85	0.15

Inattention	MMI (Failure)	Experience	Knowing current data about system	
			Pr (X)	Pr (X)
1	1	1	0.95	0.05
1	1	0	1.00	0.00
1	0	1	0.85	0.15
1	0	0	0.92	0.08
0	1	1	0.80	0.20
0	1	0	0.85	0.15
0	0	1	0.00	1.00
0	0	0	0.70	0.30

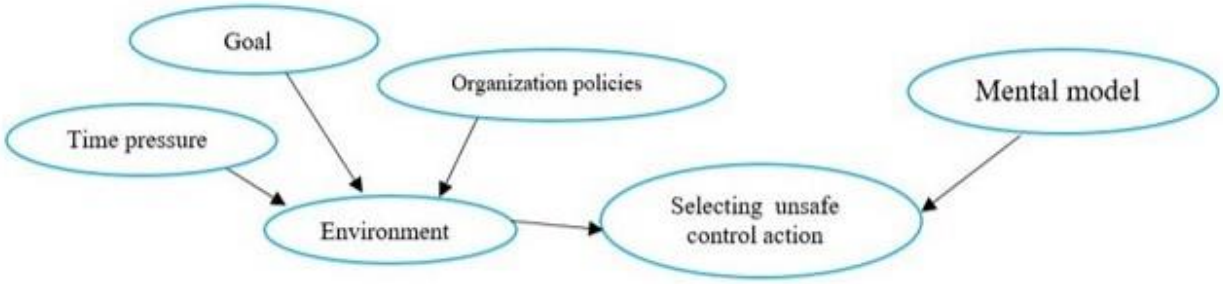


Experience	Trust in system	Knowing what the system can do	
		Pr (X)	Pr (X)
1	1	0.10	0.90
1	0	0.25	0.75
0	1	0.15	0.85
0	0	0.60	0.40

Knowing current data about system	Knowing what the system can do	Mental model	
		Pr (X)	Pr (X)
1	1	0.00	1.00
1	0	0.25	0.75
0	1	0.30	0.70
0	0	0.90	0.10

Figure 25: Model of mental model using Bayesian network and related conditional probability tables - ERTMS level 2

The probability of a correct mental model is 0.866879, while the probability of an incorrect mental model is 0.133121.



Goal (bad impact)	Time pressure	Organization's policies (bad impact)	Environment	
			Pr (X)	Pr (X)
1	1	1	0.95	0.05
1	1	0	0.80	0.20
1	0	1	0.85	0.15
1	0	0	0.70	0.30
0	1	1	0.60	0.40
0	1	0	0.50	0.50
0	0	1	0.35	0.65
0	0	0	0.07	0.93

Mental model	Environment	Selecting unsafe control action	
		Pr (X)	Pr (X)
1	1	0.97	0.03
1	0	0.70	0.30
0	1	0.75	0.25
0	0	0.15	0.85

Figure 26: Model of selecting an unsafe control action using Bayesian network and related conditional probability tables - ERTMS level 2

The probability of a good environment is 0.806337, while the probability of an environment that is not good is 0.193663.

The probability of selecting a safe control action is 0.879917, while the probability of selecting an unsafe control action is 0.120083.

BTM (Failure)	Balise (Failure)	Ch2	
		Pr (X)	Pr (X)
1	1	1.00	0.00
1	0	1.00	0.00
0	1	1.00	0.00
0	0	0.00	1.00

ODO (Failure)	Ch2	Ch	
		Pr (X)	Pr (X)
1	1	0.15	0.85
1	0	1.00	0.00
0	1	0.00	1.00
0	0	0.10	0.90

Co1	Ch	Secondary group error	
		Pr (X)	Pr (X)
1	1	0.00	1.00
1	0	1.00	0.00
0	1	1.00	0.00
0	0	1.00	0.00

ATP (Failure)	EVC (Failure)	Co1	
		Pr (X)	Pr (X)
1	1	1.00	0.00
1	0	1.00	0.00
0	1	1.00	0.00
0	0	0.00	1.00

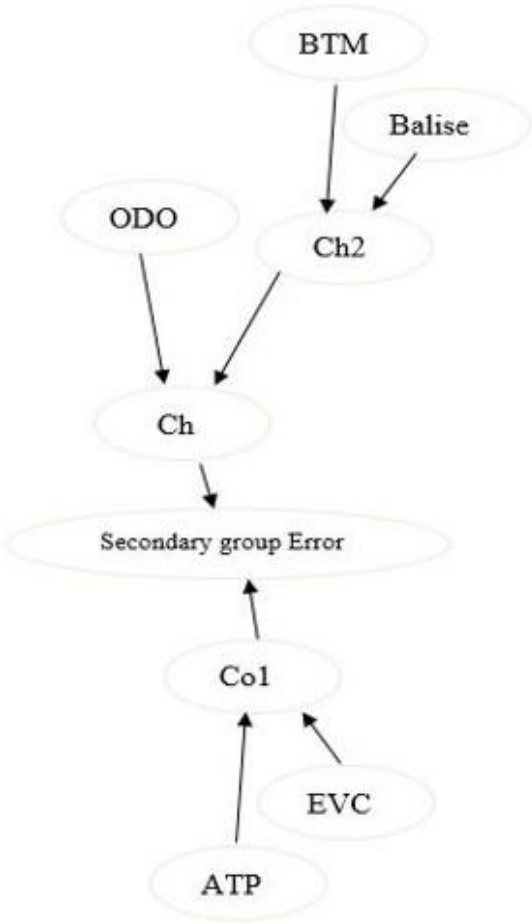
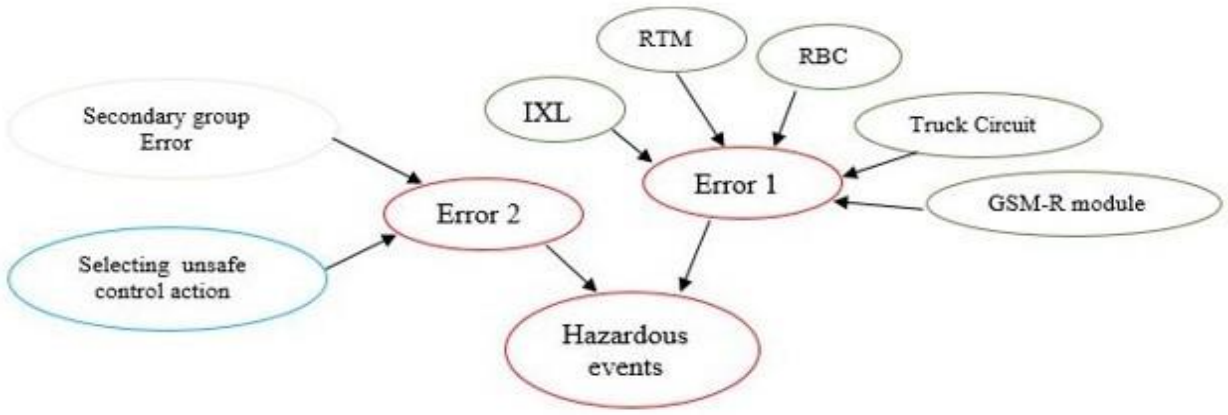


Figure 27: Model of secondary group error using Bayesian network and related conditional probability tables - ERTMS level 2

The probability of secondary group error is 0.052032.



Selecting unsafe control action	Secondary group error	Error 2	
		Pr (X)	Pr (X)
1	1	0.00	1.00
1	0	1.00	0.00
0	1	1.00	0.00
0	0	1.00	0.00

IXL (failure)	RBC (failure)	RTM (failure)	Truck circuit (failure)	GSM-R module (failure)	Error 1	
					Pr (X)	Pr (X)
0	0	0	0	0	1.00	0.00

Error1	Error2	Hazardous Event	
		Pr (X)	Pr (X)
1	1	0.00	1.00
1	0	0.00	1.00
0	1	0.00	1.00
0	0	1.00	0.00

Figure 28: Model of hazardous events using Bayesian network and related conditional probability tables - ERTMS level 2

The probability of Error 2 is 0.006248.
The probability of Error 1 is 0.096079.
The probability of a hazardous event is 0.101727.

7.4.3 Summarising the result of safety risk analysis of ERTMS/ETCS related to SPAD

The comparison between the results of the quantitative safety analysis of ERTMS/ETCS levels 1 and 2 related to SPAD are shown in table 7.

Table 7: Comparison of the safety between ERTMS/ETCS level 1 and level 2 related to SPAD including human errors

ERTMS/ETSC	Wrong mental model	Selecting unsafe control action	Error 2	Error 1	Hazardous event
Level 1	0.346454	0.280297	0.112416	0.058808	0.164613
Level 2	0.133121	0.120083	0.006248	0.096079	0.101727

From the results in the table above, we can observe that ERTMS level 2 is safer than ERTMS level 1 (as the probability of a hazardous event in level 2 is lower than for level 1). The increase in safety comes about as a result of keeping the train driver continuously informed about the states of signals ahead through RBC and GSM-R systems; this gives him enough time to make the correct decision, thus reducing the probability of errors. In ERTMS level 1, on the other hand, the driver is informed about the states of signals ahead only when he looks at the lineside signals, which can be affected by many factors related to the state of the driver and the weather conditions. Also, we can observe the probability of driver errors (selecting unsafe control actions) in ERTMS level 2 is lower than for level 1 for the same reason.

On the other hand, the number of critical components in ERTMS level 2 is higher than in level 1. Therefore, the probability of errors being caused by these components (error 1) is higher in level 2 than level 1. The reliability of these components is thus a critical issue and should always be as high as possible.

7.5 Sensitivity analysis

Sensitivity Analysis is a tool used to study and analyse the impact of variables (inputs) on output, where the output is function of several inputs [47]. The aim of sensitive analysis in our model is to determine how the output value (which presents the probability of hazardous event SPAD) can be changed when we change probability of states of one variable (factor), so that we can make the probability of ideal value is (1) for one variable and keep the probability of the rest of the variables as they are in table 6. We then repeat this process with different variables (factors) and copy the value of the probability of hazardous events for each variable. Completing this process will yield Table 8, which gives us the values of hazardous events for ERTMS/ETCS level 1 and level 2 when we use ideal values with one variable.

Conducting sensitive analysis allows us to evaluate the importance of variables (nodes) in the model through identifying the critical nodes that have the highest impact on safety. Once these nodes are identified, we can obtain the maximum increase in the system's safety level by improving the reliability of these nodes.

From the results in Table 8, it can be observed that:

- The best improvement in system safety is obtained when we cause the driver's objective (goal) to align with the 'safety first' concept.
- EVC is the most critical physical component in the system, as increasing its reliability has the greatest impact on improving the safety of the system as a whole.

Table 8: Probabilities of hazardous events related to SPAD when the probability of ideal value of some variables is (1)

The variable (Node)	Probability happened Pr(X)	ERTMS/ETCS Probabilities of hazardous event	
		Level 1	Level 2
Tiredness	0	0.162279	0.101596
Fatigue	0	0.162279	0.101625
Training	1	0.161755	0.101534
Familiarity	1	0.161420	0.101511
Trust in system	1	0.162103	0.101586
Goal (Bad impact)	0	0.151651	0.100659
Organization polices	1	0.156933	0.101190
MMI (Failure)	0	0.162978	0.101602
Blaise (Failure)	0	0.161748	0.101446
RBC (Failure)	0	--	0.101842
EVC (Failure)	0	0.161388	0.099627
The original value		0.164613	0.101727

A wide range of factors can potentially influence the train driver's mental model, along with his ability to select the correct action. It should be noted that only some of these factors were incorporated in our suggested model in order to keep the model as simple as possible.

Moreover, the results of our calculation are approximate and not accurate, as we were unable to obtain accurate data from experts and accident investigations; consequently, we used estimated values.

Chapter 8

Conclusions and Perspectives

The safety analysis of complex dynamic systems that incorporates human errors is always challenging. Since the operation of the ERTMS system depends on the simultaneous coordination of several subsystems, components, and humans, it is regarded as a complex system. The present thesis performs safety analysis of ERTMS with driver errors, in which all the effects of various components and driver errors are considered.

8.1 Conclusions

Most train drivers' tasks in the ERTMS system are mental tasks and are thus exposed to errors emerging from flaws in the mental process model or in selection control action. Therefore, analysing safety in the ERTMS system in relation to train drivers depends heavily on new techniques of risk analysis, such as the STPA method. This method can be used effectively to identify all types of hazards associated with train drivers' tasks. Moreover, given its benefits, the Bayesian network is considered a suitable method for modelling and quantifying the different errors that can lead to hazardous events.

A literature review was conducted for several reasons, one of which was to identify the appropriate methods for performing hazard identification. Many authors have suggested different, albeit ordinary techniques for identifying hazards in railway systems based on reports, investigations and simulations. The ERTMS system is an advanced system with a high degree of interactions between its components, as well as between machines and humans; therefore, a new technique is needed. Accordingly, a method called STPA was selected. This method depends on accident causality models and functional control diagrams. Its main feature is its ability to cope with system complexity and help to identify all hazards related to software, technical components, train drivers, and the interactions between them, all in a convenient manner. In other words, STPA is able to identify all potential causes of accidents and the factors that lead to these causes, as well as to realise the different types of errors that could emerge as a result. In fact, STPA identifies a huge number of hazards; therefore, it is important to limit the results of STPA to include only the hazards that have a significant impact on safety.

Although many ordinary methods are used to quantify safety analysis related to human performance in different systems, most of these methods are not good choices to quantify safety in a complex and dynamic system such as ERTMS. Choosing a suitable method depends on the specific tasks to be studied, the aim of the analysis, and the quality of available data. However, driver performance relies on the values of many factors (PSFs); in general, these factors are neither

reliably accurate nor constant and can differ from one situation to another. Therefore, the Bayesian network is considered a suitable method for quantitative safety analysis of driver errors in ERTMS, due to its low sensitivity to the value accuracy of factors influencing driver performance. It is also able to use multiple data sources to determine the values of these factors, and also takes into account the dependencies among these various factors.

Accordingly, a quantitative safety analysis related to SPAD in ERTMS system levels 1 and 2 (including human errors) was performed as a case study to assess and compare safety between those two levels. The results of this analysis show that ERTMS level 2 is safer and less prone to driver errors than ERTMS level 1; however, it also contains more critical elements (such as GSM-R system and RBC) that have a significant impact on the continuity of ERTMS functioning, such that any failure in one of these components will stop the whole ERTMS system. Accordingly, it can be concluded that new systems with advanced technologies will improve safety only if their subsystems and components are reliable and interact with each other reliably.

A sensitive analysis was also implemented as part of the case study in order to recognise and identify the factors that have a substantial impact on human performance and on safety in the ERTMS system as a whole.

8.2 Perspectives for future researches

There are many possible avenues for further research that can be suggested as a result of the present thesis, including:

- Research can be implemented to determine all factors that impact driver performance in both the building of the mental model and the selection of control actions in ERTMS system levels 1 and 2. These factors can then be classified in groups according to the intensity of their impact. Therefore, according to the required accuracy of the results of safety analysis, the groups can be selected and the factors within these selected groups can be used to build a model of safety analysis.
- Another potential avenue would be a detailed technical study of the ERTMS system especially levels 1 and 2, in order to determine the reliability of their components, subsystems, and interaction between them. These reliability values can be used in the model of safety analysis instead of the estimated values used in the present thesis, leading to more precise safety analysis results.
- Furthermore conditional probability tables (CPTs) are very important and have a notable impact on the outcome of the Bayesian network. Various studies can be dedicated to identifying values of conditional probability tables for all factors in the safety analysis model; these values can then be considered as standards to be used in different countries and organisations to mitigate the variability in the safety analysis results.
- Moreover, several studies could be devoted to programming applications that depend on technical and human factors impacting on safety, models of safety analysis, and conditional probability tables. The role of these applications would be to obtain data related to driver state (human factors) from the driver (by asking him some questions before he starts his journey), along with data related to the technical components of the condition monitoring system. Based on this data, the application will calculate and directly display the probability of hazardous events. If this probability exceeds a predetermined level, the system will prevent the driver from starting his journey, or will give him permission to drive only in some modes of operation

(i.e. not all modes). This will lead to significant improvements in the safety of the ERTMS system.

References

1. Kalvakunta, R.G., et al., *Reliability Modelling of ERTMS/ETCS*. 2017, NTNU.
2. Leveson, N.G., *4.5.3 Coordination and Communication among Controllers and Decision Makers*, in *Engineering a Safer World - Systems Thinking Applied to Safety*. MIT Press.
3. Leveson, N., *Engineering a safer world : systems thinking applied to safety*, in *Engineering Systems Ser*. 2012, MIT Press: Cambridge, Mass.
4. Madigan, R., D. Golightly, and R. Madders, *Application of Human Factors Analysis and Classification System (HFACS) to UK rail safety of the line incidents.* Accident Analysis and Prevention, 2016. **97**: p. 122-131.
5. Rausand, M., *Risk assessment : theory, methods, and applications*. Statistics in practice. 2011, Hoboken, N.J: Wiley.
6. Rajabalinejad, M., A. Martinetti, and L.A.M.v. Dongen. *Operation, safety and human: Critical factors for the success of railway transportation*. in *2016 11th System of Systems Engineering Conference (SoSE)*. 2016.
7. Baysari, M.T., et al., *Classification of errors contributing to rail incidents and accidents: A comparison of two human error identification techniques.* Safety Science, 2009. **47**(7): p. 948-957.
8. Felipe, A., et al., *Application of evidential networks in quantitative analysis of railway accidents.* Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 2013. **227**(4): p. 368-384.
9. Kyriakidis, M., A. Majumdar, and W. Ochieng, *The human performance railway operational index-a novel approach to assess human performance for railway operations.* Reliability Engineering & System Safety, 2018. **170**: p. 226.
10. Kyriakidis, M., K.T. Pak, and A. Majumdar, *Railway accidents caused by human error: Historic analysis of UK railways, 1945 to 2012.* Transportation Research Record, 2015. **2476**(2476): p. 126-136.
11. Baysari, M.T., A.S. McIntosh, and J.R. Wilson, *Understanding the human factors contribution to railway accidents and incidents in Australia.* Accident Analysis and Prevention, 2008. **40**(5): p. 1750-1757.
12. Graziano, A., A.P. Teixeira, and C. Guedes Soares, *Classification of human errors in grounding and collision accidents using the TRACEr taxonomy.* Safety Science, 2016. **86**(C): p. 245-257.
13. Kim, Y., J. Park, and W. Jung, *A quantitative measure of fitness for duty and work processes for human reliability analysis.* Reliability Engineering and System Safety, 2017. **167**: p. 595-601.
14. Castillo*, E., et al., *A Markovian‐Bayesian Network for Risk Analysis of High Speed and Conventional Railway Lines Integrating Human Errors.* Computer‐Aided Civil and Infrastructure Engineering, 2016. **31**(3): p. 193-218.

15. McLeod, R.W., G.H. Walker, and N. Moray, *Analysing and modelling train driver performance.* Applied Ergonomics, 2005. **36**(6): p. 671-680.
16. Hamilton, W.I. and T. Clarke, *Driver performance modelling and its practical application to railway safety.* Applied Ergonomics, 2005. **36**(6): p. 661-670.
17. Eurostat. *Number of persons killed and injured by type of accident and category of persons in EU-28, 2016.* 2018; Railway safety statistics].
18. Dorrian, J., et al., *Simulated train driving: Fatigue, self-awareness and cognitive disengagement.* Applied Ergonomics, 2007. **38**(2): p. 155-166.
19. Cacciabue, P.C., *Human error risk management methodology for safety audit of a large railway organisation.* Applied Ergonomics, 2005. **36**(6): p. 709-718.
20. Rajayogan, R., *Development of a Quantitative Safety Risk Assessment Model for Rail Safety Management System*, in *School of Business University of Western Sydney*. 2012: Australia.
21. Leveson, N., *Engineering a Safer World: Systems Thinking Applied to Safety*. Engineering systems. 2012: United States: Mit Press.
22. *Accident Models*, in *Risk Assessment*.
23. Qureshi, Z.H., et al., *A Review of Accident Modelling Approaches for Complex Critical Sociotechnical Systems*. 2008.
24. Underwood, P. and P. Waterson, *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 and Prevention, 2014. **68**: p. 75-94.
25. Ghazel, M., *Formalizing a subset of ERTMS/ETCS specifications for verification purposes.* Transportation Research Part C, 2014. **42**: p. 60-75.
26. *The Use of a "Model‐Based Design" Approach on an ERTMS Level 2 Ground System*. 2014, Hoboken, NJ, USA: Hoboken, NJ, USA: John Wiley & Sons, Inc. 165-190.
27. Leveson, N.G., *8.2 The STPA Process*, in *Engineering a Safer World - Systems Thinking Applied to Safety*. MIT Press.
28. Plioutsias, A. and N. Karanikas, *Using STPA in the Evaluation of Fighter Pilots Training Programs.* Procedia Engineering, 2015. **128**: p. 25-34.
29. Leveson, N.G., *8.4 Determining How Unsafe Control Actions Could Occur (Step 2)*, in *Engineering a Safer World - Systems Thinking Applied to Safety*. MIT Press.
30. Leveson, N.G., *2.4.5 An Alternative View of Human Error*, in *Engineering a Safer World - Systems Thinking Applied to Safety*. MIT Press.
31. Dekker, S., *The field guide to understanding human error*. 2006, Aldershot: Ashgate.
32. France, M.E., *Engineering for Humans: A New Extension to STPA*, in *Aeronautics and Astronautics*. 2017, Massachusetts Institute of Technology. p. 110.
33. Wilson, J.R., et al., *The railway as a socio-technical system: Human factors at the heart of successful rail engineering.* Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, 2007. **221**(1): p. 101-115.
34. Akyuz, E. and M. Celik, *A methodological extension to human reliability analysis for cargo tank cleaning operation on board chemical tanker ships.* Safety Science, 2015. **75**: p. 146-155.
35. Marseguerra, M., E. Zio, and M. Librizzi, *Quantitative developments in the cognitive reliability and error analysis method (CREAM) for the assessment of human performance.* Annals of Nuclear Energy, 2006. **33**(10): p. 894-910.

36. Lee, S.-H. and J. Song, *Bayesian-network-based system identification of spatial distribution of structural parameters.* Engineering Structures, 2016. **127**: p. 260-277.
37. Mu, L., et al. *The prediction of human error probability based on Bayesian networks in the process of task*. in *2015 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*. 2015.
38. Groth, K.M. and A. Mosleh, *Deriving causal Bayesian networks from human reliability analysis data: A methodology and example model.* Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 2012. **226**(4): p. 361-379.
39. Grande, Z., et al., *Highway and Road Probabilistic Safety Assessment Based on Bayesian Network Models.* Computer-Aided Civil and Infrastructure Engineering, 2017. **32**(5): p. 379-396.
40. Castillo, E., et al., *Complexity Reduction and Sensitivity Analysis in Road Probabilistic Safety Assessment Bayesian Network Models.* Computer-Aided Civil and Infrastructure Engineering, 2017. **32**(7): p. 546-561.
41. Pasquini, A., A. Rizzo, and L. Save, *A methodology for the analysis of SPAD.* Safety Science, 2004. **42**(5): p. 437-455.
42. Flammini, F., et al. *Modelling system reliability aspects of ERTMS/ETCS by fault trees and Bayesian networks*. in *Proc. European Safety and Reliability Conference, ESREL*. 2006.
43. Flammini, F., et al., *A MULTIFORMALISM MODULAR APPROACH TO ERTMS/ETCS FAILURE MODELING.* International Journal of Reliability, Quality and Safety Engineering, 2014. **21**(01).
44. Tan, P., et al. *Design and Evaluation of Universal On-board Train Interface Unit*. in *2012 International Conference on Industrial Control and Electronics Engineering*. 2012.
45. Malvezzi, M., B. Allotta, and M. Rinchi, *Odometric estimation for automatic train protection and control systems.* Vehicle system dynamics, 2011. **49**(5): p. 723-739.
46. Barger, P., W. Schön, and M. Bouali, *A study of railway ERTMS safety with Colored Petri Nets*. Vol. 2. 2009.
47. Coupé, V.M.H. and L.C. van der Gaag, *Properties of Sensitivity Analysis of Bayesian Belief Networks.* Annals of Mathematics and Artificial Intelligence, 2002. **36**(4): p. 323-356.

Acronyms

ANP	Analytic Network Process
ATP	Automatic Train Protection
AWS	Automatic Warning System
BN	Bayesian Network
BTM	Balise Transmission Module
CPT	Conditional Probability Tables
CREAM	Cognitive Reliability and Error Analysis Method
CSM-R	Global System for Mobile Communications for Railway
DAG	Directed Acyclic Graph
ERTMS	Europe a European Railway Traffic Management System
ETCS	European Train Control System
ETML	European Traffic Management Layer
EVC	European vital computer
HEART	Human Error Assessment and Reduction Technique
HEP	Human Error Probability
HFACS	Human Factors Analysis and Classification System
HRA	Human Reliability Analysis
HuPeROI	Human Performance Railway Operational Index

IXL	InterLocking system
LEU	Lineside Electronic Unit
LTM	Loop Transmission Module
MMI	Man Machine Interface
ODO	Odometer system
PSFs	Performance Shaping Factors
RBC	Radio Block Centre
RTM	Radio Transmission Module
SLIM	Success Likelihood Index Methodology
SPAD	Signal Passed At Danger
STAMP	Systems-Theoretic Accident Model and Processes
STPA	Systems Theoretic Process Analysis
THERP	Technique for Human Error-Rate Prediction
TIU	Train Interface Unit
TRACEr	Technique for the Retrospective and predictive Analysis of Cognitive Errors
UCAs	Unsafe Control Actions
WAN	Wide Area Network