Modelling of human and human-system interactions for railway safety

Individual Report
-Safety by Design

- Shrikanth Venkataramana
MSc Mechanical Engineering
Student Number: 2336464
January,2020

TABLE OF CONTENTS

1. Introduction

This report focuses on the human and human-system interactions which exist in the background of railway safety. Railways is a technical system and yet humans are as integral to it as any mechanical component. To ensure the smooth and safe running of railway operations without any harm to humans, it is essential to understand what are the impacts the system has on humans and how they interact. Integrating safety in human and railway interaction goes beyond the technical aspects and also encompasses non-technical knowledge. This report outlines a systematic view of integrating safety in the selected topic.

2. System of Interest

In this section, the system of interest is defined along with the subsystem, components, human and environmental factors involved. This helps in easier understanding of safety and hazard identification.
Currently, the trains in The Netherlands are at an automation level of GoA 1 which includes just manual train operation where a train driver controls the train's starting and stopping, motion of doors and handling of emergencies or unexpected diversions. [1] However it includes an ATP (Automatic train protection) which is a train protection system that measures the train speed and compares it with the permitted speed and informs the train driver when a brake is required.
Thus the system here in the report includes the train which consists of the rolling stock with its coaches, wheels and other mechanical and electronic parts which are in it. It also includes the railway tracks as well.

2.1 Subsystem

The subsystems of the SoI can be defined as structural or functional subsystems. Structural subsystems describe (groups of) components present in the system, while functional subsystems group the different functions of the system [2]. The latter will be more useful here.
Each of the subsystem interacts with humans of different groups in various ways this is shown in Figure 1. As a safety design engineer, it is important to understand how safe are these interactions and what hazards could emerge from them.

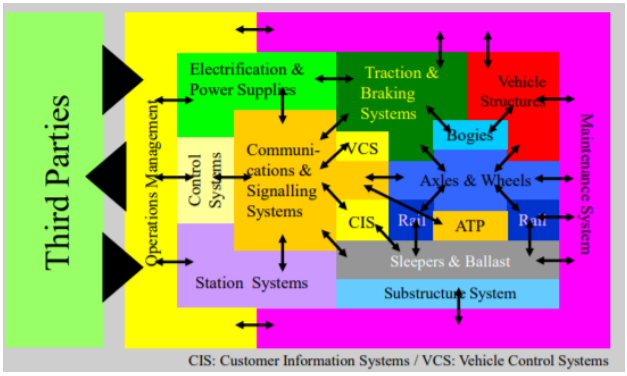

Fig 1: Subsystems and interaction with humans

The structural subsystems group the different components of the train which serve the same function and are [3]:

▪ ***Safety systems***: This subsystem contains components such as the emergency brakes, emergency doors, fire extinguishers and other physical safety features. The function of this subsystem is to maintain the safety of the humans in the train.

▪ ***Trackside control & signaling***: This subsystem consists of the components related to navigation and obstacle detection and signals coming from the environment. This encompasses the ATP as well. The function is to process the signals coming from the external environment accurately.

▪ ***Onboard control & signalin***g: This subsystem consists of the components related to the control and signaling onboard the train, such as provision of feedback to the train operator via an interface. The function of this subsystem is to process the signals coming from other components within the system such that the train operator can interpret them properly.

▪ ***Comfort facilities***: This subsystem contains the facilities providing passengers with facilities such as seats, trash cans, hygienic toilets and tables. The function is to provide ergonomic, and comfortable seating for the passengers.

▪ ***Climate control***: This subsystem consists of all components regarding climate control onboard the trains, such as air conditioning, ventilation systems and filter systems. The function of this subsystem is to provide a healthy and comfortable climate for the passengers.

▪ ***Communication system***: This subsystem contains all systems that communicate with the control center, the passengers and the coworkers. This includes the travel information channels. The function of this subsystem is to provide clear information that is specified for the receiver.

▪ ***Power supply***: This subsystem contains all components regarding the power supply from the electrical network to the train and its components. Its function is to safely provide power to the components as per its requirement.

▪ ***Physical***: This subsystem contains all physical parts a train needs to perform its function, that do not fall under the other subsystems. Components such as doors, wheels and windows are part of this group. Its function is to provide a safe unit which can transport people from one location to another. Also the railway tracks on which the entire train runs on is included here as it is a physical part needed for the train to function as defined above.

2.2 Components

Here, the components which come under each sub system is defined. This can give a coherent idea of what exactly is in the SoI and what are the hazards involved during the interaction. In figure 2 the system is mentioned with the subsystem and components of each subsystem.

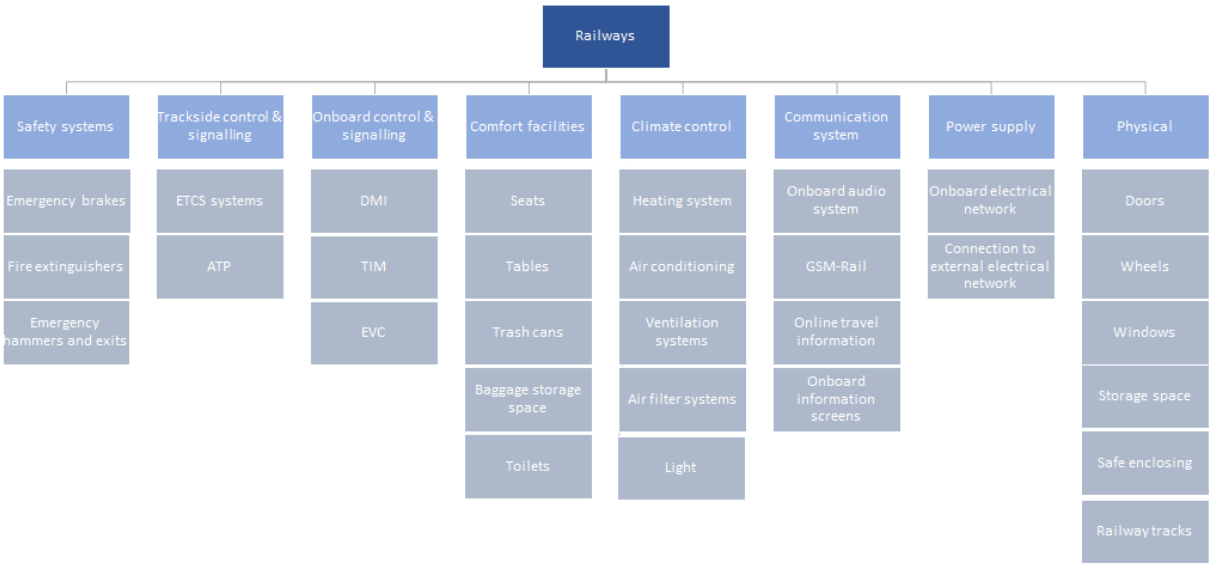

Figure 2: System of Interest with the subsystems and components

Most of the components are self-explanatory however a few require additional clarification. These include the components from trackside and onboard control and signaling such as ECTS. The European Train Control System (ETCS) transforms the external signals via the European Vital Computer (EVC) and shows them on the driver machine interface (DMI). The overall system includes parts which are external to the train. Onboard systems include EVC, DMI, BTM and GSM-Rail. Along with this, it consists of systems that locates the position of the train and an accelerometer. GSM-Rail is the system of radio communication for the entire railway system. It provides communication for signals, ATP and personnel. It uses frequencies of the radio network only accessible by railway systems. Automatic Train Protection is a system that collects signals and can override the system in critical situations, mostly based on speed.
The European Rail Traffic Management System (ERTMS) is a European program that standardizes safety and control of the rail traffic throughout Europe, this is an evolution from the ATS and ensures that a standard and common set of rules will be applied for cab signaling, security levels, interoperability all throughout Europe [4]. Above mentioned systems are an important part of that program. ERTMS can be applied at different levels and for autonomous trains the highest level, level 3, is required. This means also a train integrity meter (TIM) is present on the train, which measures of all train coaches are still connected. [3]

2.3 Human

The topic of this report stresses majorly on the human and human system interaction in railways. Humans here consists of various groups. Each group is a stakeholder and has certain expectations from the system when interacting with it and safety has to be designed as per their requirements.
These include the following major groups:

- ***Passenger***: This is the major group which uses the train to travel from a starting point to a destination. They deal with a wide range of hazards due to the varied situations they face which will be addressed later. Cost, comfortability and time consumed during travelling are key factors which determines whether a passenger would travel or not.
- ***Train operators***: These include the drivers, technicians and attendants. Their interest lies in ensuring that the overall operation of the train during their working hours is safe and information transfer is accurate, they also require well-functioning equipment and proper training.

- ***Government***: This includes both the local and national government which has keen interests in ensuring smooth functioning of railways as a means of boosting the economy and increasing the flow of people. Along with this, they look forward for less public investment and better safety standards as a cause of public satisfaction with their policies. They provide the necessary public infrastructure to railway companies to run the trains and try to implement important safety regulations and enforce hazard prevention if the railway company fails to do it.
- ***Railway company***: They are the key investors in the railway industry and focus on getting profits from the entire system. They perform the role of management. It is up to them to decide how humans will interact with trains since they are involved in manufacturing it and in providing the trains. However, they are always regulated by the government to ensure that the public is not charged too much for the services.
- ***Railway Service Providers***: These include the maintenance companies, workers. contractors, catering service providers, railway station shop owners and information providers in railway stations who facilitate smooth passenger railway interaction.
- ***Third parties***: This includes vehicles and pedestrians at level crossings, bridges, those who could trespass or vandalize railway property and those involved in development adjacent to railways such as in construction or drainage work. It also includes locals living near the railways who always play an important role in informing the railways of any issues which could lead to accidents [5].

2.4 Environment

The final aspect that influences the SoI is the environment. This includes the regulations which are applied on various subsystems and aspects of the train, the physical external environment which plays a major role in accidents which influences the design of railways as a whole and the competing systems such as metros, trams and other transportation options. This can also include other trains as they are an external factor as well.

2.5 Interaction

Since the system, human and environment have been identified, interaction among them is identified. This can assist in identifying the safety regulations required, hazards which could occur and the methods of integrating safety into the human system interaction. This is done using a safety cube as shown in Table 1 and Table 2.

Table 1: Elements of safety cube for safe integration of humans and railway systems

	Human	**System**	**Environment**
Human	Passengers, train operators, railway service providers, railway company and the government	Quality, comfortability, entry-exit procedure, driver input, misbehavior on equipment in trains	Travel frequency, misbehavior on tracks or stations
System	Comfortable, affordable, safe, and punctual transport	Railways(and the subsystems included in it)	Visibility during weather conditions, obstruction on tracks
Environment	Onboard entertainment/information system, catering services, ticket purchasing service, climate requirements	Detectability of obstacles, weather conditions, spare parts supply, communication updates	Railways, control center, stations, weather, policies, regulations, energy supply

Table 2: Safe integration with focus on system (System safety cube)

	System requirements, functions, and behavior	**Physical system (system-SoS/environment relation)**	**Use/misuse scenarios (human-system relation)**
Environment and super systems	Railway policy and regulations in the Netherlands and Europe, control functions,	Railways, stations, crossings, environmental conditions, energy supply	Misbehavior from other passengers/trains/external persons on tracks or platforms, malfunctioning power supply

	environmental regulations and requirements		
System	Ergonomically safe, complies with safety standards, meets desired performance	A multi-wagon vehicle to transport humans on railways, powered by electricity and steered by a driver or a semi-automated system	Train uses unassigned tracks, boarding when the train is moving, departing at wrong time
Sub-systems	Components need to comply with national and international standards	Coaches with bases and software. Software failure, air conditioning failure, doors malfunctioning, seats which could harm posture	Passenger/object gets stuck in between doors, breakage of equipment/windows, misusing emergency break, passenger/object falls between the train and platform, damaging onboard interface systems, damaging bathroom equipment

2.6 Experience and Expectations

This safety cube enables easy integration of safety into the system [6] From this, a table can be created which helps learn from the experiences of the past and improve safety in the future for better expectations using the present as the basis. Here, the design and safety integration of SoI is presented in Table 3[3].

Table 3: Physical system, its use and functions across the timeline

	Past	***Present (in use/life time)***	***Future***
Structure/ failure in structure			
Environment or supersystems for SoI	Very few platform barriers. No actively secured crossings. Weather conditions played a big influence on performance. No external electrical power supply used.	No platform barriers Many of the crossings are actively secured. Weather has some influence on performance. Wired electrical power supply.	All station platforms have safety barriers. All crossings actively secured. Weather conditions become more severe due to climate change. Wireless electrical power supply.
SoI	Trains were in GoA0 or level of automation. Software integration was low	Trains are in GoA1 and GoA2 regarding automation.Software integration is being used	Trains are in GoA3 or GoA4 regarding automation. Most of the systems are automated and will be integrated.
Subsystems or components of SoI	Communication systems were hardly developed and used. No digital data was used.	A vast amount of communication systems is present in the SoI, digital data is stored and used.	All subsystems are connected to each other and interact through the Internet of things(IoT) or another suitable interface.
Use/ misuse			
Environment or supersystems for SoI	Vague or no regulations and protocols for railway transport. They were not strictly defined.	Strict defined regulations and policies regarding safety, environment, humans and integrity regarding railway transport.	Advancement of the (enforcement of the) regulations concerning railway transportation.
SoI	Most of the systems are accessible by unauthorized people.	Almost no systems are accessible by unauthorized people.	All systems and software are only accessible by authorized personnel.
Subsystems or components of SoI	No onboard travel information systems. Doors can be opened manually.	Onboard and online travel information systems are present. Doors are opened by driver.	Onboard and online travel information systems contain more precise, up to date and detailed information. Doors are automatically opened.

(Mal)Functions			
Environment or supersystems for SoI	The environment is competing with the functioning of the SoI.	The environment is collaborating and competing with the functioning of the SoI.	Advancement of the environment towards collaborating with the SoI.
SoI	All functioning of the SoI is manually controlled.	Most of the functions are automatically controlled.	All functions are automatically controlled.
Subsystems or components of SoI	Driver needs to visually check the tracks and signals.	Driver needs to visually check the tracks. Signals are digitized.	All sensoring of systems and environment is digitized. Human interference is eliminated.

2.7 History of Accidents

Knowing the human-system specific accidents which have occurred in the past will help in recognizing the real causes of accidents and enables us to develop the required safety measures [7].
Statistics show that in the Netherlands [8]:

- Between February 1, 2018 and January 31, 2020, Rijden de Treinen has reported 51 disruptions caused due to police action.
- Between February 1, 2018 and January 31, 2020, Rijden de Treinen has reported 374 disruptions caused due to an emergency call. This is an average of 1 disruption per day.
- Between February 1, 2018 and January 31, 2020, Rijden de Treinen has reported 586 disruptions caused due to a person hit by a train. This is an average of 1 disruption per day.
- March 20, 2003, Roermond -Due to a heart attack of the driver, a train crashed into another train, where one person was killed and 38 injured.
- April 21, 2012, Amsterdam -A driver missed a stop signal and the train crashed into another train. One person died and 136 got injured.
- 16 February 2016, Bavaria - Human error by a train controller was to blame for a crash in Bavaria, Germany, that killed 11 people and dozens more were injured when two commuter trains collided on a single-track stretch of railway [9]

Also, a few statistics are taken into account from the other countries along with a basic analysis is explained briefly in a tabular manner in Appendix 1 [10]:
When it is observed thoroughly from the table, apart from the Casselton, USA and West Virginia Train Derailment all other accidents are caused due to human error. Preventing these human errors is essential for safety in railways as humans can always affect hazards.

3. Safety Objectives

This chapter will contain information regarding the safety critical functions which are linked to the subsystems identified in the previous chapter. Following this, the level of safety for each of them is identified and later on the required regulations and safety requirements are discussed.
From the safety cube it is observed that when it comes to human-system interaction:

- Passengers expect from the system is comfortable travelling experience, affordable tickets, safe equipment, seats, handles, ventilation and lighting equipment, punctuality from the train and a good information providing interface to interact within the train. As trains of the future are automated, humans will have to interact directly with the train instead of a train operator when it comes to entering/exiting, internal climate control etc.
- However currently, train drivers are common and their interaction with the train is of utmost importance. The drivers should be in good mental and physical health while working and should have thorough knowledge about their tasks

and must be given training on how to handle trains during emergencies. All this defines how a train operator interacts with it.

- Also, maintenance workers interact with the railways especially when fixing the tracks and while conducting timely maintenance of trains. They must have ease of access to the parts which require maintenance and this happens only when the train is designed to give secure and easy access to its parts which could fail the most.
- Third party: They are not involved directly in the railways. What they expect is to be given protection from the hazards railways could cause and are expected to be responsible towards protecting railway infrastructure.

3.1 Safety critical functions and Level of safety

In the earlier chapter, the components were listed out. Based on this, the functions are identified. These functions are common for all trains in use currently and along with this, the level of safety will be assigned to them. The safety level assigned to the system throughout its lifecycle is assumed to be assigned as "catastrophic" for railway operations. This basically means that accidents and risks related to this system can easily result in the death or disability to humans and a huge monetary loss to railways. The subsystems defined in the system definition gives a clear overview of how each of them perform the functions mentioned above.

Based on these subsystems, we can give each of them a level of safety.
The level of safety are as follows:

1= Must be avoided in all circumstances
2= Changes in design must be implemented
3= Technical measures can be taken
4= Information must be provided
5= Risks can be accepted due to low severity

Along with the functions which have to be ensured in the railways, the ISO12100 safety standards are used which specify the definitions, principles and methodology to achieve safety during the designing of machinery. It also specifies risk assessment and reduction during its lifecycle to enable designers in reaching their goals.
This standard is the basis for a set of standards which have the following structure [11]:

Type A - Basic safety standards which give basic concepts, principles for design and general aspects that can be applied to all machinery.

Type B - Generic safety standards which deal one safety aspect or one type that can be used across a wide range of machinery.

Type C - Machine safety standards which deal with detailed security requirements for a particular machine or group of machine standards.

Here, the level of safety which has to be assigned to each of the subsystems and the mention of functions below which they can be categorized is also given. The risks are mentioned and the levels of safety are also assigned. These standards are basic and are assumed for the Type A level of safety regulations as the focus is on creating safety regulations for the overall system and its subsystems.
The functions of the subsystems are given below with their respective level of safety [3].

i. ***Safety systems*** This comes under passenger safety and any compromise on safety over here deals with the risk of facing injuries or death. Here, it must be tried to remove any chances of risks here and thus it has a safety level of 1.
ii. ***Trackside control & signaling*** This comes under route control. Wrong signals here can lead to the train colliding with other objects or can get derailed which is deadly for the passengers and machinery. Also, external bystanders could be affected severely due to this. Here, it must be tried to remove any chances of risks here and thus it has a safety level of 1.

iii. ***Onboard control & signaling*** This comes under communications and route controls. These are issues which deal with the operator being able to understand the signals coming, errors here are not deadly. This can be solved by taking technical measures to handle cases when electronic systems fail. Standby mechanical systems can be placed to replace them temporarily. It comes under safety level 3.

iv. ***Seating facilities*** This comes under comfort. This is important for passenger satisfaction, given that the risks due to sudden breaks are not dangerous when passengers are sitting, however it is a risk if they are standing and thus it is an accepted risk which is solved by giving proper safety information to the passengers and comes under safety level 4.

v. ***Climate control*** This comes under ventilation and feedback to operator. These are necessary for a comfortable journey and for the overall health of the passengers. Improper circulation of air can cause respiratory issues especially if dust levels are high inside. This can cause repetitive illness to frequent travelers. This is something which must be dealt with during designing the coaches as they need to determine the vents, grilles, path of travel of supply and exhaust and fresh air during preliminary design and thus is given a safety level of 2 as changes in designs is necessary here.

vi. ***Communication system*** This comes under communications. It deals with the most important tools through which the autonomous train is connected to the control center outside and the internal internet provision. This is extremely important for the train to be intimidated of upcoming obstacles and other external hurdles. Thus the issues need to be removed and it comes under safety level 1.

vii. ***Power supply*** This comes under energy security. This is the most essential as the lines above supply the train with electricity. Any issues with this could lead to a sudden halt. If there is an issue with insulation, then human life is risked. To avoid all these harmful issues, this is assigned a safety level of 1 and must be eliminated.

viii. ***Physical*** This performs the primary function of protecting the passenger during transportation. Risks over here have to be eliminated in the design phase itself since changing it later can cause delays in production, delivery and other related issues. If tracks are not in a good condition it could lead to derailment and death and destruction of nearby environment as well and also a huge monetary loss for the company and humans. Thus the safety level given is 1.

3.2 Required regulations and Safety requirements

The regulations which can be used here for ensuring safety standards are now mentioned [12]:

Safety systems

i. IEC 60050-821 gives the general terminology relating to signaling and security apparatus for railways, as well as general terms pertaining to specific applications and associated technologies.

ii. NEN-EN 50126-2:2017 deals with the specification and demonstration of Reliability, Availability, Maintainability and Safety independent of actual technology but mentions how to use the systems engineering approach to assess risks, specify, design and implement measures of safety.

iii. NEN-EN 45545-2:2013+A1:2015 specifies the reaction to fire performance requirements for materials and products used on railway vehicles. For each hazard level, this part specifies the test methods, test conditions and reaction to fire performance requirements.

iv. NEN-EN 17065 specifications test methods and acceptance criteria for a brake system used in passenger coaches including driving trailers for use in general operation. This document is applicable to all new passenger coaches including driving trailers, which are designed for general operation in the European conventional rail system network in accordance with EN 14198.

v. NEN-EN 16334 specifies the characteristics of the Passenger Alarm System. The aim of the Passenger Alarm System is to: a) permit passengers in a case or emergency situations to inform the driver; b) permit the driver to keep the train moving or to stop the train at a safe location; c) stop the train automatically: 1) at a platform, 2) if there is no acknowledgment by the driver.

Trackside control and signaling

i. NPR-CLC/TR 50507:2007 deals with the interference limits in existing track circuits in European railways. Also it provides an overview, a reference and a source of information for other specifications and specifications that are presently in preparation.
ii. NEN-EN 50238-1:2019 describes a process to demonstrate compatibility between Rolling Stock (RST) and Train Detection Systems (TDS). It describes the characterization of train detection systems, rolling stock and traction power supply systems.
iii. CEN/TR 17315:2019 regulates the calculations for the estimation of stopping distance for specific Wheel Slide Protection testing. This has to be uniform for all systems to predict braking, track changes especially for an autonomous train.

Onboard control and signaling

i. NEN-EN-IEC 61375-3-3:2012 specifies the data communication bus inside that are based on CANopen. CANopen networks are utilized to network subsystems which consists of systems such as brake control systems, diesel engine control systems and interior or exterior lighting control systems.

Seating facilities

i. NEN-EN 12299:2009 is a standard which specifies methods for quantifying the effects of vehicle body motions on ride comfort for passengers and vehicle assessment with respect to ride comfort. The effects considered are discomfort, associated with relatively low levels of acceleration and roll velocity.

Climate control

i. NTA 9065:2012 deals with the air quality and odor measurement and describes the standard procedure in the Netherlands for carrying out odor investigation, where possible as an obligation, otherwise as a recommendation.
ii. NTA 9055:2012 draws up a list of requirements for using an electronic nose (e-nose) to detect changes in the composition of the ambient air. The e-nose is used for emission, pollution monitoring of odor emissions. This e-nose maps the effects on surroundings of occasional emissions.

Communication system

i. NEN-EN 50129:2018 deals with communication, signaling and processing systems and with the safety related electronic systems used for signaling.
ii. NEN-EN 50159:2010 is a European Standard, applicable to safety-related electronic systems used for digital communication purposes or a transmission system which was not necessarily designed for safety-related applications. This standard gives the basic requirements needed to achieve safety-related communication between safety-related equipment connected to the transmission system.
iii. NEN-EN-IEC 62580-1 specifies the general architecture of the On-board Multimedia and Telematics Subsystem, which includes four categories of multimedia and telematics subsystems identified as: a) Video surveillance / CCTV b) Driver and crew orientated services c) Passenger orientated services d) Train operator and maintainer orientated services

Power supply

i. NPR-CLC/TR 50488:2007 is applicable to all work activities on or near the overhead contact line [IEC 60050-811, definition 811-33-02] of railway installations with supply voltage values. This deals with electric hazards only.
ii. NPR-CLC/TS 50534:2010 defines characteristics and interfaces for electric onboard power supply systems. It applies to locomotive hauled passenger trains and electric multiple units with distributed power as well as trains with concentrated power for main-line application.
iii. NEN-EN 50463-5 specifies the conformity assessment arrangements for newly manufactured Energy management system installed on a traction unit. This includes the integration conformity assessment and installation conformity assessment.

Physical

i. NEN-EN 13450:2003+C1:2006 specifies the properties of aggregates obtained by processing natural of manufactured materials or recycled crushed unbound aggregates for use in construction of railway track.
ii. NEN-EN 15595:2018 specifies the criteria for system acceptance and type approval of a wheel slide protection (WSP) system along with criteria for implementation to specific vehicle applications and specific operating conditions, as well as requirements for wheel rotation monitoring (WRM).
iii. NEN-EN 14067-3:2003 describes physical phenomena of railway-specific aerodynamics and gives recommendations for the documentation of tests.

4. Hazard Identification

Hazard analysis involves identifying hazards which occur due to human-system interaction and then analyzing them, ranking accidents according to their severity and finally coming up with controls and follow up action for the hazards. In this report, hazard analysis is conducted by listing them down, scoring them on the basis of severity and frequency to eventually obtain a risk assessment matrix. Hazard controls are applied based on the level of seriousness of the hazards. This is a part of Preliminary Hazard Analysis(PHA) which is a semi quantitative analysis method for hazards [13]. It is one the many useful techniques to analyze safety as shown in Figure 3 and is employed along with other techniques to get a complete view of safety design and analysis.
Hazards identified here are based on the understanding developed in the safety cube, system of interest (SoI) and on the understanding of how the system and subsystems interact and affect humans and vice versa. The history of accidents is also a good source of identifying hazards. The main focus has been on human and system related hazards which forms the basis of the report.

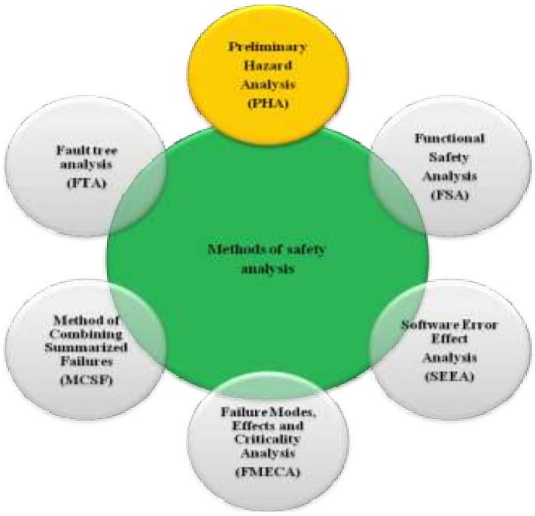

Figure 3: Main Safety Analysis Method [14]

4.1 Hazards Ranking

The hazards are identified in Table 6 and given a code along with a score for severity and occurrence. The details of the severity and occurrence score is given below in Table 4 and 5.

Table 4: Frequency score

Frequency of occurrence	Score
Frequent	5
Reasonably Possible	4
Occasional	3
Remote	2
Extremely Unlikely	1

Table 5: Severity score

Severity	Score
Catastrophic	5
Critical	4
Major	3
Minor	2
No significant effect	1

The score/rank is given based on the frequency of news reportings in various regions, experience and severity of the hazard on humans.

Table 6: List of hazards with score for occurrence and severity.

Code	Hazard Identified	Frequency of occurrence score	Severity score
A	Train driver falls ill during duty.	3	5
B	Error by track controller while switching gears.	3	5
C	Signal passed at danger by driver	3	4
D	People on tracks when the train is in motion	2	4
E	Negligence by humans on railway crossings	3	5
F	Unruly behavior by train driver	2	5
G	Lack of focus on track by train driver	3	5
H	Improper maintenance resulting in faulty brake	1	3
I	Improper maintenance resulting in faulty sensors	2	3
J	No advanced warning about possible detours/disasters by railway officials to driver	2	3
K	Dislodged fishplate on track due to improper maintenance	2	3
L	Over speeding by driver	3	2
M	Destroying railway infrastructure by humans	2	3
N	Unscheduled maintenance on tracks leading to injury to workers	1	1
O	Inappropriate separation between un-insulated live conductors and the public	2	5
P	Improper separation of railways from nearby neighborhood	1	2
Q	Flying debris from moving train and objects falling from trains	1	1
R	Unsecured Objects at Height train placed by	2	1

	passengers		
S	Cyber security issues when there is an attempt to take over the train's control by hackers	1	1
T	Humans onboard the train who could harm other passengers physically	3	4
U	Humans attempting suicide on railway tracks	4	5
V	Objects thrown intentionally/unintentionally on trains by humans	1	1
W	Vandalizing the insides of a train compartment	1	1
X	Passenger falls sick inside the train	4	3

4.2 Hazard Analysis

Based on the scores given above, the hazards are assigned below to respective sections in Table 7. The risks are categorized in the Risk Assessment Matrix in the boxes with Red: High risk, Orange: Serious risk, Yellow: Medium risk and Green: Low risk. Accordingly, the first priority goes to high and serious risks that needs to be controlled and eliminated urgently. Afterwards, the medium and low-risks can be controlled based on the cost-benefit of the system safety control measures.

Table 7: Risk Assessment Matrix

Severity/Frequency	**Extremely unlikely (1)**	**Remote (2)**	**Occasional (3)**	**Reasonably possible (4)**	**Frequent (5)**
Catastrophic(5)		**F,G,O**	**A,B.E**	**U**	
Critical (4)		**D**	**C,T**		
Major (3)	**H**	**I,J,K,M**		**X**	
Minor (2)	**P**		**L**		
No significant Effect (1)	**N,Q,S,V,W**	**R**			

From the above table, the risks with a higher level of priority are chosen and hazard control measures will be taken for them. Along with that, Fault tree analysis is created for a few major risks such as:

i. Humans attempting suicide on railway tracks.
ii. Train driver falls ill during duty
iii. Negligence by humans on railway crossings

These are shown in Appendix 2. FTA explain in a top down manner the reasons for "why" undesired hazards occur in our system. From this, the crucial and primary reasons for the hazards are understood and thus the root cause of the hazard can be targeted and controlled or eliminated.

Apart from this, an event tree diagram which is another method of analyzing the consequences of hazards is shown in Appendix 2 as well for:

- Negligence by humans on railway crossings

5. Hazard Controls

From the Table 6, we observe hazards of various levels of risk. It is always desired that the risks are reduced and the reliability of the system increased. The hazards with lower risk levels are not going to be controlled to save costs and avoid unnecessary redesign of the system. Thus the hazards which need to be controlled include A, B, C, E, F, G, O, T, U and X. Control of a hazard needs to be done in a planned order to reduce the risk as much as possible, using the ISO 12100 [15]. Initially, redesign of the system must be considered. This means redesigning the system such that the hazard is no longer present or the risk is reduced to an acceptable level. If that is not possible, safety devices must be used when operating the system. This will reduce the probability of the hazard's occurrence. If that is insufficient, warning devices should be placed around the areas where the hazard persists. And finally if none of the above can be implemented, special procedures and training of the operators can also be used to reduce the risk which also includes information campaigns.

5.1 Control Measures for each hazard

It must be noted that creating more automation in railway systems, especially when it comes to train drivers, opening and closing of doors etc, then risks are reduced. However here we take in the current conditions in which the train is still driven by the driver. All these controls are sent to a design review team as well which approves the designs.

A. Train driver falls ill during duty

Here, the control measure includes conducting regular health checkup for train drivers to check for chances of heart attacks which if it happens during driving can risk the passenger's life as well. Also, the drivers must be given time off if they are genuinely affected by mental issues. There must be a safety button in the driver's control board on the train which needs to be activated periodically to ensure that the driver is alive failing which the train halts slowly and completely as it could mean that the driver has fainted or is dead.

B. Error by track controller while switching gears

If the track controller makes mistakes while switching gears to change tracks, there is a high chance that 2 different trains could be coming towards each other from different directions. This could happen if the controller does not understand the data which he is receiving from outside in his computer due to a cluttered interface. The solution here is to use a clean software interface to provide the controller with real time data of trains and their routes so that he can change the tracks smoothly. He must also be given proper training before using the interface.

C. Signal passed at danger by driver

Installing automatic train protection(ATP) which automatically regulates train speed and can detect danger points and thus apply brakes or slow down when necessary must be installed or else, a warning system to remind the driver must be installed to warn the driver of an incoming signal and this will alert him to apply brakes or slow down. Thus this issue is solved using both redesign techniques and installing warning devices

E. Negligence by humans on railway crossings

This negligence happens if there is a lack of proper signals and barriers on railway level crossings. In such a situation, people could get on the track when the train is arriving which could be deadly for them. The solution here is to install proper barriers and alarm systems on level crossings to ensure that humans do not neglect the warning signs.

F. Unruly behavior by train driver

The control measure here includes instilling safety culture and positive attitude in the drivers. This is a form of training. If there is an incident, the safest method of eliminating another situation would be to terminate such unruly drivers.

G. Lack of focus on track by train driver

Lack of focus on the track by the train driver can result in many other hazards as well which include signal passed at danger, over-speeding, collision with other trains, animals, humans etc. The easiest method of controlling this hazard is to install ATPs which will warn the driver of over-speeding, sensors to detect obstacles and initiate brakes if necessary and equipment fitted to trains and on the track that reduces the consequences of a train passing a signal at danger, by automatically applying the train's brakes should be installed as a design change. Finally, the driver must be allowed to take sufficient rest between each shift so that he stays focused while working. Simulators can also be used to train drivers periodically to avoid such hazards.

O. Inappropriate separation between un-insulated live conductors and the public

Un insulated live conductors could always lead to which are the electric wires on top of the trains must be kept inaccessible to humans especially in remote railway tracks. It should be quickly fixed if they are damaged or fall down. If maintenance workers or other people come in contact with such wires, then they could die due to high voltage electrocution. This is done by designing the wires at a safe height and ensuring that proper warning is given to humans if there is a breakdown.

T. Humans onboard the train who could harm other passengers physically

There is always a chance that some humans with negative attitude might misbehave and harm other passengers. If there are no control measures, then there is a high chance that innocent passengers could face severe damage or death. This is prevented through public outreach, guiding passengers on what is acceptable behavior, providing an easily accessible helpline and having railway police monitor coaches to check for deviant passengers who could harm others.

U. Humans attempting suicide on railway tracks

Suicides on railway tracks is a complex issue which has to be solved by different methods. Deploying mitigation measures, such as fencing to prevent access to the tracks at high-risk locations is one method of redesigning the system (railway tracks) at that location. Raising awareness, installing safety devices such as blue lights [16], deploying anti trespass guards near suicide prone areas and approaching people who could be prone to depression and suicide for the purpose of providing psychological help and also by introducing smart motion-detection cameras to alert of unusual movements both in stations and at level crossings [17].

X. Passenger falls sick inside the train

In situations when a passenger is severely sick or experiences sudden pains, it is best to have at least one trained medical professional of the rank of a nurse or higher in each train to keep the sick passengers safe until they can be moved out at the next station to a nearby hospital.

5.2 Cost benefit analysis

In this section, cost benefit analysis is discussed. Every control measure which is adopted has to be evaluated to justify whether the money spent on it is worth reducing the hazard. Thus the design engineer must take this into account when designing or redesigning a system and its interaction with humans.

If the risks in terms of human life is involved and if the damage to the railway system is high, then the price spent on enforcing control measures are always justified. Always, a separate amount from the budget is assigned for this which is used to implement the necessary solutions. It would be wise to assign this budget for the hazards for which control measures have been mentioned in the above section. If there is any remaining money, then that can be assigned to fix the hazards which are marked in the yellow section of the risk assessment matrix.

6. Monitoring the system

The system always has hazards even after the control of hazards. In order to monitor those risks, safety indicators need to be identified which help to create a safe system. Along with this, the safety culture around the system needs to be addressed in order to reduce the human factor in the hazards.

6.1 Safety indicators

There are two types of safety indicators, leading and lagging. Leading indicators are indicating future actions that should be taken when deviations occur from safety expectations. Lagging indicators indicate changes in performance factors due to taken safety-related actions. Leading indicators tell how well the prevention of incidents in going, while lagging indicators are showing the current level of safety [18].
The leading safety indicators in this system are the number of near-misses, effectively completed trainings and the number of maintenance programs. The safety program of the owner of the SoI is also an indicator, by the number of safety meetings or trainings. These indicate whether the safety of the system is addressed fully or whether further action is required.
The lagging indicators for the SoI are the number of times the driver has missed signals(SPADs) or failures by the ATP systems, concerns from passengers regarding the safety of the train. This indicates the state of safety in the SoI.

6.2 Safety culture

Even though there are proper safety standards in place, humans are unpredictable and thus when they interact with the system, to reduce the chances of human induced hazards, a proper safety culture has to be set in place which can train employees to cultivate a proper safety culture. This is developed by going through different levels which can be demonstrated in the form of a Safety maturity model [15]:

- ***Pathological*** This is when the employee does not trust his employers, is not motivated, careless and does not follow safety standards. This is illegal to be precise and undesirable for any company or customers.
- ***Reactive*** Here the employees respond to risks only when they occur and there are no pre planned safety modules in place to deal with them since the leadership might not be interested in spending money on such tasks.
- ***Standardized*** Here, regular safety tests are set in place and safety management system is set up to monitor basic hazards.
- ***Integrated*** Here, the hazards are monitored pro-actively, the leadership is involved actively in monitoring hazards, there is a safety management system in place and the entire staff is motivated to ensure safety.
- ***Optimized*** There is constant monitoring of safety standards and an active support from the managers. Safety here is strongly integrated into the company's corporate strategy and they use this as a business differentiator.

It is understood that for proper human-railway system interactions to happen, there must be a well-established set of practices which are to be followed by the company and constant feedback and improvement must be present between them and customers. The managers must also be involved directly to ensure that safety standards are enforced and control measures are taken seriously. Railways is an intensive industry as far as manpower, schedules and investments are concerned. This is why the safety culture which must be operated here is "*Optimized*" level.

7. Prove Sufficient Safety

Goal structuring notation is used to prove that the arguments and logical reasoning made in the above cases makes the human-railway system interaction sufficiently safe for practical application.
The Goal Structuring Notation (GSN) is a practice commonly used for developing and presenting the safety argument, forming the framework of a safety case, in a rigorous, hierarchical and easily-understood manner [19]. It facilitates the construction of complex safety cases by showing clearly the logical relationships between the Goals, Sub-goals, strategies,

rationales, contexts and evidence using graphical symbols. The top-level safety goal is that the system is ‘safe’. This is progressively broken down until sub-goals are reached for which convincing evidence can be provided [20].
The GSN is shown below in Figure 4 and also portrayed in Appendix 3 in an enlarged form. It is self-explanatory and shows why the human- system interaction for railways in this case is sufficiently safe by showing how different aspects of this report come together to cover the issue regarding safety completely.
It starts with stating the real goal of the report in G1 as human system interaction for railways is safe. The contexts used to define that is given in C1 and C2. After that, the various strategies used to prove this goal are mentioned in S1-S6. Following this, the sub-goals which are achieved from the strategies are mentioned in G2-G9. Later on, the solutions obtained from each sub-goal is stated from S1-S10 and these are either conclusions arrived at or a layout within the report which explains the solution clearly. Finally, the sub-contexts are used to reference to the location of the solutions to understand in what context the solutions are used in.

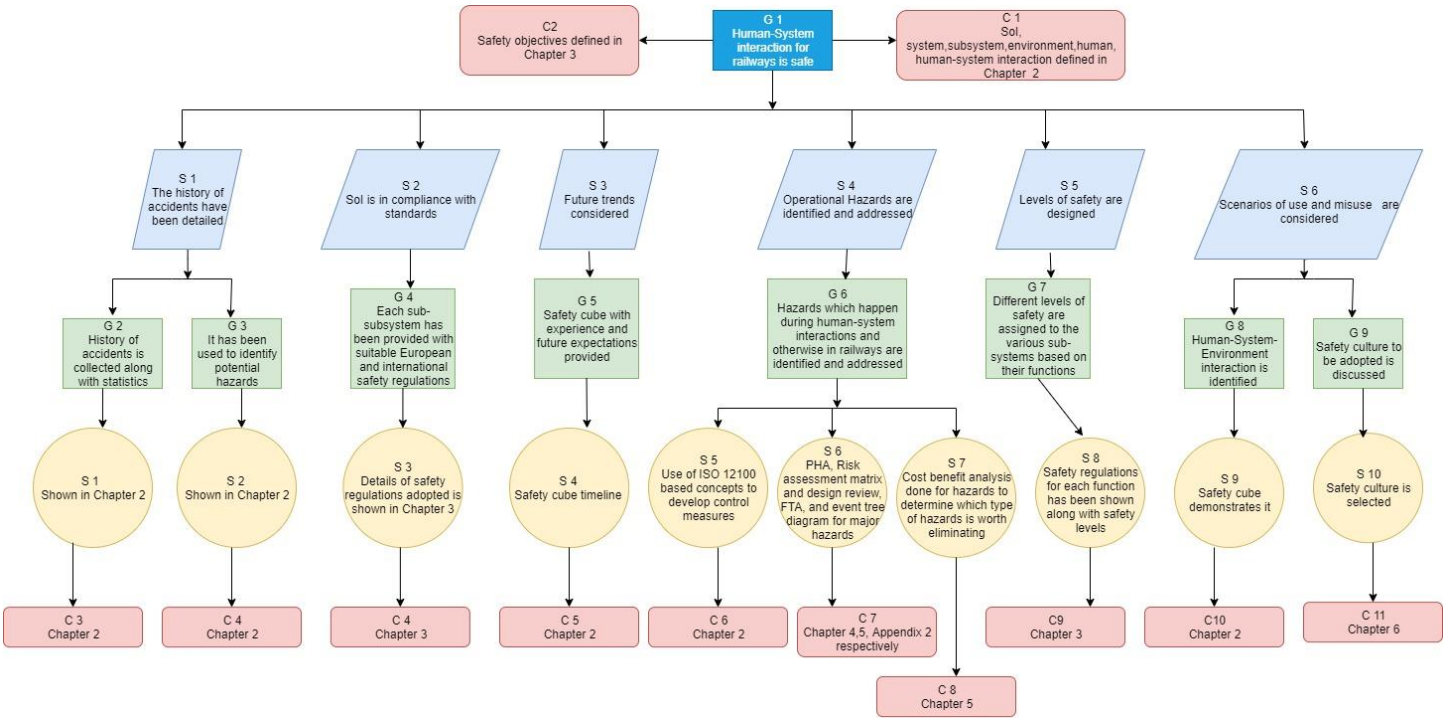

Figure 4: Goal Structure Notation for the case

8. Reflection

The course “Safety by Design” has been a resourceful learning experience and has increased knowledge on the scope and consequences of safety challenges with real life examples. It has created an interest for analyzing hazards in an organized manner and giving meaningful solutions and has introduced the idea of accepting a system as safe only if there is hard evidence rather than accepting safety on face value due to the fame of the brand etc. The safety cube has been useful in understanding system, human, environment and their interactions. Using the event tree analysis, PHA, FTA and most importantly the risk assessment matrix has shown how hazards can be classified and dealt with accordingly. The concepts of conducting a cost benefit analysis and having good safety culture in the system has been interesting and useful. Working on a real system which could be analyzed for hazards in person would always be something exciting and would make the course even more effective. The excursion to the UT Workshop-1 was one such event. In conclusion it must be noted that this course has provided me with tools to think in a structured, design oriented and scientific manner when it comes to developing safety measures for systems, products and their interaction with humans and the environment. It will also be very helpful for my further courses in the field of design engineering when it comes to hazard analysis and implementation of safety on mechanical devices or structures.

9. Conclusion

Railways is one of the most widely used public transport globally. Along with that, it provides employment to humans of varying levels of skill from managers to drivers, maintenance workers, etc. Human interaction here with the railway system becomes a very important topic of study for safety and hazard analysis. In this report, the SoI, subsystems were identified and safety regulations were provided along with a mention of accidents. Following this, hazards which occur when humans interact with the railway systems was studied and control measures were provided. Following this, cost benefit analysis is discussed as a factor in implementing control measures. A need to implement a proper safety culture is spoken about and finally safety is proven to be sufficient for this report using a GSN. It is ultimately understood that ensuring safety is not just the task of an individual stakeholder but something which must be implemented and followed by all humans who are involved in the use of the railway system.

References

[1] https://www.computerweekly.com/news/252439066/Dutch-railway-operator-to-experiment-with-self-driving-trains

[2] http://www.otif.org/fileadmin/user_upload/otif_verlinkte_files/06_tech_zulass/05_Reglementation_en_vigueur/A_94-01B_1_2012_e__UTP_GEN-B_-_Subsystems_-_IN_FORCE_.pdf

[3] Autonomous Operations Group 1Midterm Report -Laura Hutten, Shrikanth Venkataramana, Anuj Chalotra

[4] https://julkaisut.vayla.fi/pdf8/lts_2017-42eng_ertms_deployment_web.pdf

[5] https://timesofindia.indiatimes.com/india/Villager-alerts-rly-staff-of-dislodged-plates-from-tracks-averts-accident/articleshow/52014922.cms

[6] Rajabalinejad, M. (2018). Incorporation of Safety into Design by Safety Cube. Industrial and Manufacturing Engineering, 12(3), 476-480.

[7] https://nl.wikipedia.org/wiki/Chronologisch_overzicht_van_ernstige_spoorwegongevallen_in_Nederland

[8] https://www.rijdendetreinen.nl/en/statistics/causes/

[9] https://www.bbc.com/news/world-europe-35585302

[10] https://www.birmingham.ac.uk/Documents/college-eps/railway/RSEI-event/SCHMID-Felix-Human-Factors-Systems-and-Safety.pdf

[11] ISO 12100-2 Safety of machinery-basic concepts, general principles for design- technical principles

[12] NEN Connect, https://connect.nen.nl/Home/Detail

[13] https://ab-div-bdi-bl-blm.web.cern.ch/ab-div-bdi-bl-blm/Literature/fmcea/pha.pdf

[14] HADJ-MABROUK, Habib. Preliminary hazard analysis (PHA): new hybrid approach to railway risk analysis. Int Refereed J Eng Sci, 2017, 6.2: 51-58.

[15] M. Rajabalinejad, Product, machine and system safety, In Course Safety by Design

[16] https://www.bbc.com/future/article/20190122-can-blue-lights-prevent-suicide-at-train-stations

[17] https://www.railway-technology.com/features/featurepreventing-suicide-at-railway-stations-4627355/

[18] M. Middlesworth, A Short Guide to Leading and Lagging Indicators of Safety Performance, ErgoPlus, https://ergo-plus.com/leading-lagging-indicators-safety-preformance/

[19] https://www.icao.int/ESAF/Documents/RVSM/AFI_RVSM_PISC_Core_Document_FEB2008.pdf

[20] https://pdfs.semanticscholar.org/7223/b9d4086f1d76570628afaadf72625df01a8f.pdf

Appendix 1

Table 8: List of accidents showing human factors involved

Accident Location	Change not understood?	Immediate Cause(s)	Contributory Cause(s)	Management Failure(s)
Neuhausen, CH	Better Train Performance	SPAD (1.2 km/h)	No Speed Supervision	We are the best in the World
Lac Mégantic, CA	New Flows of New Fuels	Train Not Secured	Poorly Maintained Locos	Cost cutting and negligence
Brétigny-sur-Orge	Focus on LGV Higher Speeds	Dislodged Fishplate	Inadequate Supervision	Lack of interest
Santiago de Comp	ATP off, no train stop	Driver error Over speed	Hasty start of new services	Reliance on human beings
Granges-Marnand	New services, peak time only	SPAD (50 km/h)	No ATP, train stop site wrong	Minor routes not enhanced
New York, USA	No vigilance device in cab	Micro sleep Over speed	No ATP, no speed traps	Politically focused
Casselton, USA	Huge growth in oil flows	Poor track maintenance	New type of fuel oil, wagons	Undercutting of competition
Bintaro LC	Overall Traffic Growth	Truck on Level Crossing	No CCTV LC Supervision	People are unimportant
Collision at Rafz nr. Zürich, CH	Train Power Increases	SPAD by Trainee Driver	Difference in Timetable	We are still best in World
West Virginia Train Derailment	Huge growth in oil flows	Poor track maintenance	Out of date wagons in use	Undercutting of competition

Halifax Collision	Growing Road Vehicle size	Truck on Level Crossing 20’	No CCTV LC Supervision	Instructions for police incorrect
Philadelphia High Speed Derailment	Complexity of Driving Task	Driver Mistake	PTC not yet Operational	Budget cuts & radio spectrum
Eckwersheim, Train Derailment	Increased speed of Tests	Driver Mistake	ATP not Operational	Complacency, we are the best.

Appendix 2

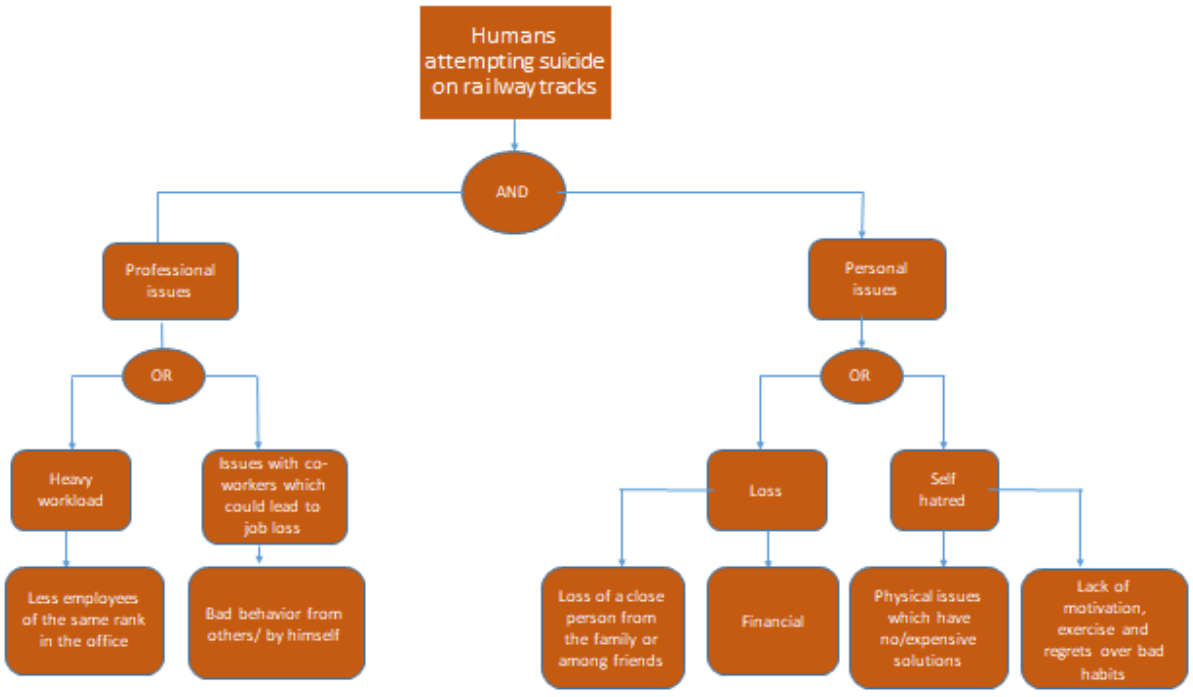

Figure 5: Fault Tree Analysis for humans attempting suicide on railway track

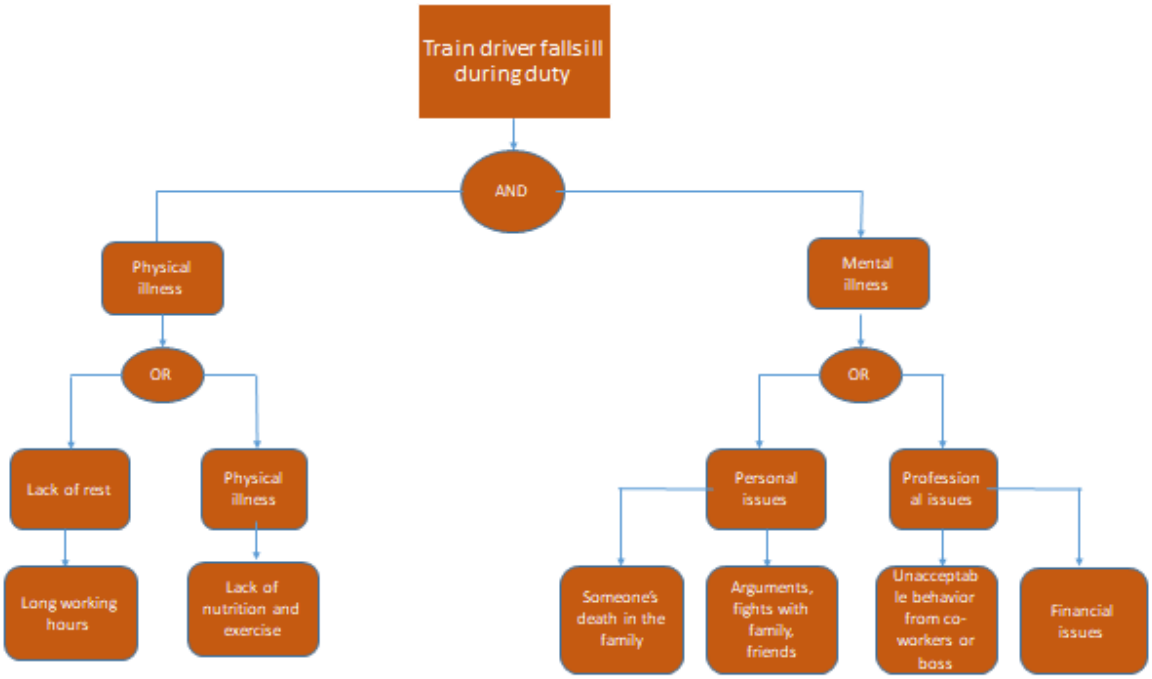

Figure 6: Fault Tree Analysis for train driver falling ill during duty

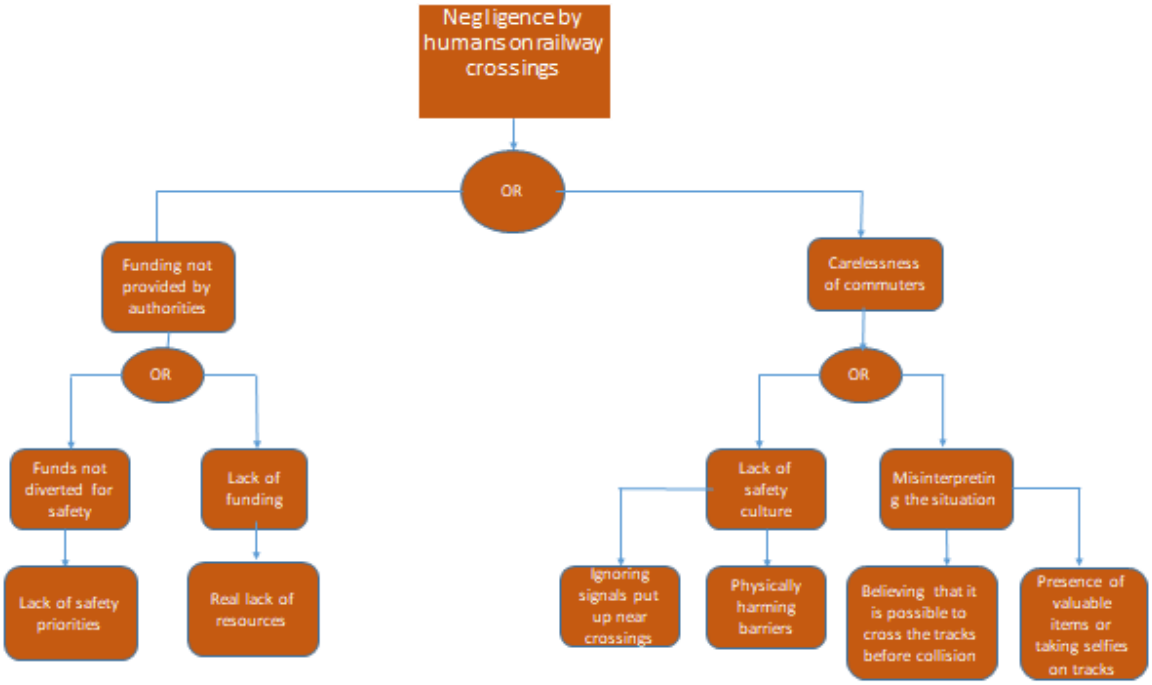

Figure 7: Fault Tree Analysis for negligence by humans on railway crossings

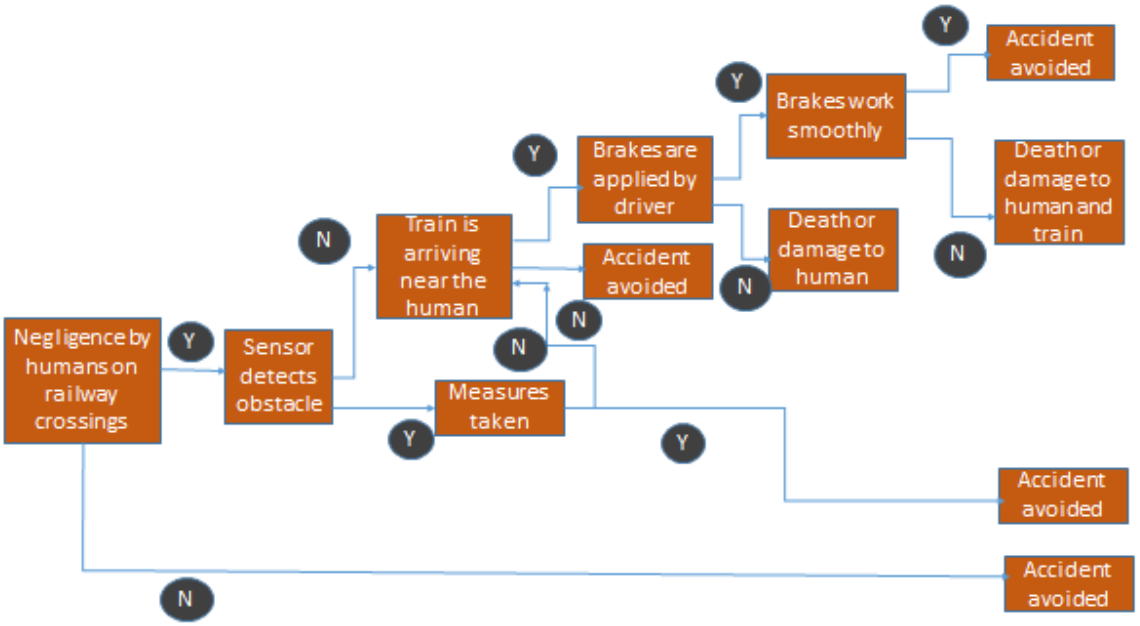

Figure 8: Event Tree Analysis for negligence by humans on railway crossings

Note: Y=Yes,N=No

Appendix 3

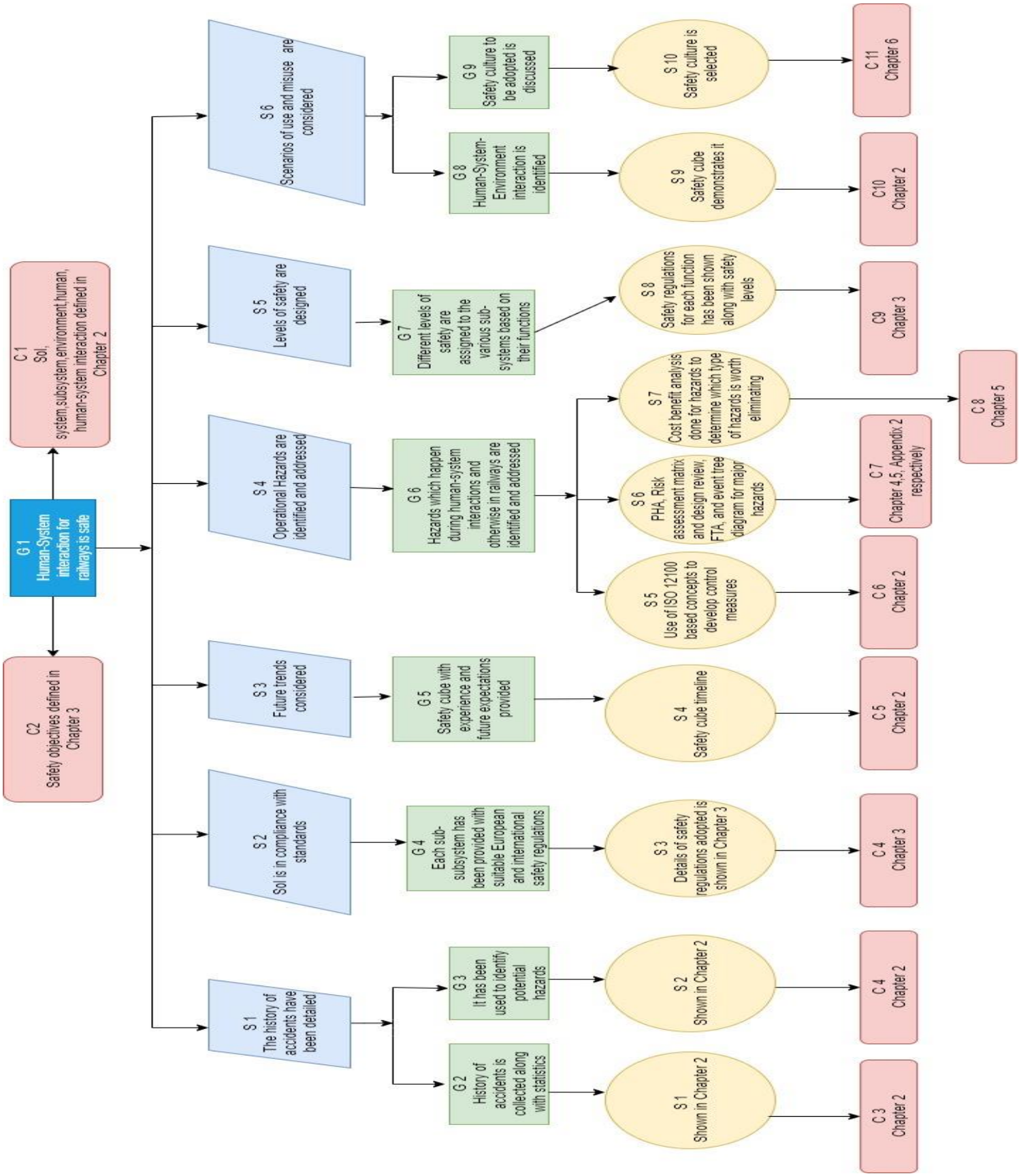

Figure 9: Goal Structure Notation for human railway system interaction safety report