Digital Twin and Railway System Safety

Safety by Design

Project group 7
S2429454 - Benjamin Parbst
S2041197 - Emiel Dolmans
S2429470 - Thomas Finch Rasmussen

Table of Content

1. Introduction

This report is a group assignment for the Safety by Design course by df. M. Rajabeli Nejad at the University of Twente. The main objective is to apply the group's knowledge of the system safety process and provide design proposals for improving safety in the dutch railway system, with the use of a Digital Twin.

The train is a relatively sustainable transport mode and will therefore play a major role in the future. The EU recognizes the importance of the rail network and aims to achieve a single European rail area operating openly across the whole of Europe under agreed (non-)technical demands. One of the major aspects of the rail network is safety. The EU targets to halve the number of casualties by 2020 and achieve almost no fatalities by 2050. New technologies can play a major role in the safety objectives for the rail network. Digital twins is such a new technology which has become one of the most talked about topics because of their promise to leverage innovation to improve design, visually enhance collaboration, and increase asset reliability and performance. This report will look into the positive changes the Digital Twin technology can provide for the safety of railway systems.

2. Method

To achieve a better understanding of the system and the safety challenges, the following steps will be undertaken.

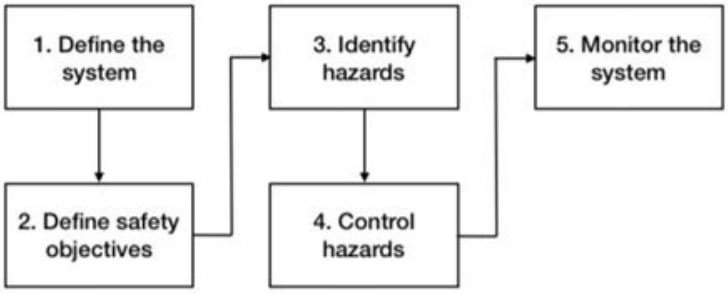

Figure 1, The steps for system safety analysis

The first step will consist of defining the scope of the System of Interest (SoI). For this, there are three important elements; system components, humans and the environment. The stakeholders that have an interest in our system are identified. Besides, there are a lot of things that influence the system. The physical environment, regulations and collaborating/ competing systems interact and influence our system. To have a better understanding of the system, these will be identified. The second step will consist of the definition of the safety objectives and identification of regulations/standards that needs to be addressed. The third step looks at the history of accidents and identifies hazards. The identified hazards will be analysed based on hazard severity/ probability and the risk is evaluated. In the fourth step, the hazards are controlled by new designs. The final step consists of the monitoring of the system. Safety indicators will be identified to check the impact of our design measures.

3. Defining System of Interest

It is important to define the System of Interest (SoI). To define the system correctly, three elements are important, namely system components, humans and the environment. To have a better understanding of the system, these will be identified. However, first it must be made clear what the writers mean with the term Digital Twin. Therefore, this will be discussed first.

3.1 Digital Twin

To understand the system however, we have to understand the concept of a Digital Twin. A Digital Twin, like a virtual prototype, is a dynamic digital representation of a physical system. However, unlike a virtual prototype, a Digital Twin is a virtual instance of a physical system (twin) that is continually updated with the latter's performance, maintenance, and health status data throughout the physical system's life cycle [2].

A Digital Twin, by definition, requires a physical twin for data acquisition and context-driven interaction. The virtual system model in the Digital Twin can change in real-time as the state of the physical system changes (during operation). Today, a Digital Twin consists of connected products, typically utilizing the Internet of Things (IoT), and a digital thread. The digital thread provides connectivity throughout the system's lifecycle and collects data from the physical twin to update the models in the Digital Twin [2]. Figure 1 presents the Digital Twin concept.

Figure 2, Digital twin concept [2]

As shown in this figure, the Digital Twin links the virtual and physical environments. The physical environment includes the physical system, onboard and external sensors, communication interfaces, and possibly other vehicles operating in an open environment with access to GPS data. Both operational and maintenance data associated with the physical system are supplied to the virtual environment to update the virtual model in the Digital Twin. Thus, the Digital Twin becomes a precise and up-to-date representation of a physical system that also reflects the operational context of the physical twin.

Functions of Digital Twin

The Digital Twin can be used for the following:

a) It is a specific instance that reflects the structure, performance, health status, and characteristics such as distance covered, malfunctions experienced, and maintenance and repair history of the physical twin.
b) It helps determine when to schedule preventive maintenance based on knowledge of the system's maintenance history and observed system behavior.
c) It helps in understanding how the physical twin is performing in the real world, and how it can be expected to perform with timely maintenance in the future.
d) It allows developers to observe system performance to understand e.g. how modifications are performing, and to get a better understanding of the operational environment.
e) It promotes traceability between life cycle phases through connectivity provided by the digital thread.
f) It facilitates refinement of assumptions with predictive analytics-data collected from the physical system and incorporated in the Digital Twin can be analyzed along with other information sources to make predictions about future system performance.
g) It enables maintainers to troubleshoot malfunctioning remote equipment and perform remote maintenance.
h) It combines data from the IoT with data from the physical system to, for example, optimize service and manufacturing processes and identify needed design improvements (e.g., improved logistics support, improved performance)
i) It reflects the age of the physical system by incorporating operational and maintenance data from the physical system into its models and simulations.

So in short, by integrating the virtual and physical worlds, the Digital Twin enables real-time monitoring of systems, processes and timely analysis of data to head off problems before they arise, schedule preventive maintenance to reduce/prevent downtimes, uncover new business opportunities, and plan for future upgrades and new developments [2]. NASA and USAF (United States Air Force) researchers describe a Digital Twin as an integrated multi-physics, multiscale, probabilistic simulation of an as-built vehicle or system that uses the best available physical models, sensor updates, fleet history, etc., to mirror the life of its corresponding flying twin [3].

3.2 Digital twin of railway system

The Digital Twin can be used in the railway system. This part describes how the virtual twin interact with the railway system (components of the system). In the figure below, the system of the Digital Twin is visualized with its subsystems and components. The virtual representation consists of a model and the input from the sensors on the real asset (sensor readings). The data collected will result in an up-to-date representation of the physical system. The railway system consists of several subsystems, shown in yellow. These subsystems each consists of multiple components (green). Each component has sensors and actuators (blue). The sensors act as the eyes and ears of the component, and detect changes in the environment around them, providing information for a processor, MCU or other system to react to. The actuators provide a mechanical response according to the input provided by the sensors and (usually) processed by other electronics.

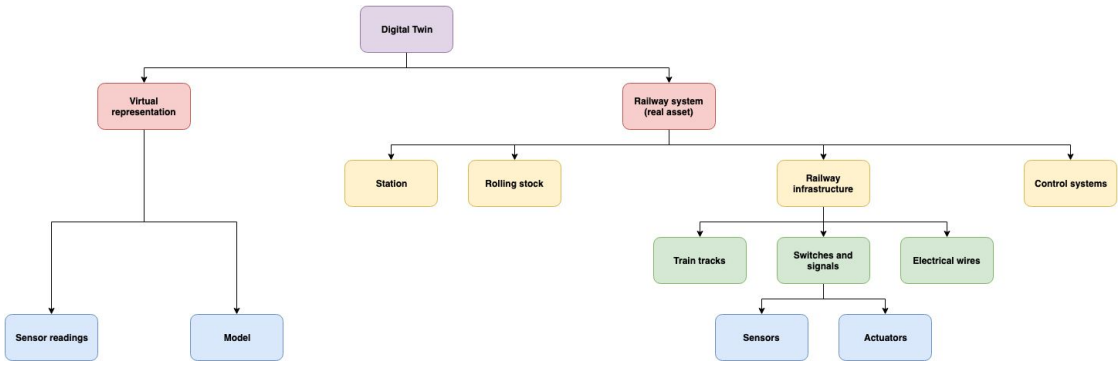

Figure 3, system of the Digital Twin

Digital twins can have a big impact on railways. However, because of the huge size and complexity of the railway system, as shown in the figure above, it will be almost impossible to fully twin the whole system. Most likely, there will be many Digital Twins for the railway, modelling different components and processes. In the future, unique virtual representations of each unique component of the rail system might be connected dynamically with its specific real-world counterpart, but also with one another building a decentralized system of systems. However, the first step remains to model different components of the railway system. This will result in:

- Continuous knowledge generation
- Monitor & optimize the performance virtually at any given time of the unique component: from requirements to disposal
- Minimize uncertainties by state of health monitoring and prediction for the unique component in full-system context
- Resolve issues (fault isolation) while minimizing time and capital invested
- Generate insights, user-requirements for new products & services
- Optimized component design based on knowledge from production & operations

The system is also influenced by human and environmental elements. The following stakeholders interact with our Digital Twin:

- Prorail, which is the infrastructure owner.
- The NS (dutch railways), which is the train operator.
- The company which creates the Digital Twin system. In Denmark, Engineering company Fugro has been awarded a four-year contract to create a Digital Twin of Denmark's rail network. In Singapore, to Siemens has been set to the task of creating a Digital Twin.

These stakeholders will work together to create a safe system. This is eventually also to the benefit of the users. The interaction with the environment can also be influenced by Digital Twin technology. The following aspects are considered under the term environment:

- Weather system
- Obstacles on or near the train tracks
- Regulations and train traffic rules
- Power outage

4. Defining Safety Objectives

In this section, safety scope and objectives in pursuing a higher level of safety with the implementation of a Digital Twin will be described. With focus on the safety of the Dutch railway system, both relevant national and international regulations will be investigated. When investigating these, relevant norms and standards are identified and finally safety critical functions of the system of interest are listed and discussed.

4.1 Safety Scope

The Digital Twin (DT) is a powerful tool that will be able to help improve both efficiency, scheduling, performance and other aspects of the railway system. However, in this report the only focus is safety. How can the DT help improve safety? What safety objectives are most important and why. The system of interest described in section three, points in the direction of the safety scope specified in this section.

The railway system consists of many smaller systems and components. The scope of this report will consider the outer mechanical and electrical components as mentioned in section 3. The analysis will consider components like the tracks, the train and other components within the railway system, for which the Digital Twin can be used to improve safety and minimize accidents. Mechanical malfunctions happening inside the train e.g. air conditioning or other components, that will not result in safety issues for the environment around the train like people or vehicles crossing the tracks, will not be taken into consideration. The purpose of this will be to focus on reducing the number of incidents caused by, either human or environmental interaction. Examples can be people misusing the system or unexpected behavior by the trainsystem's surroundings, causing potential safety issues.

4.2 Safety Goal and Objectives

The difference between goals and objectives is that the objectives are created in order to measure performance in certain areas and allows the organisation to account for the goal. They are the means of achieving the goal. Following primary goal is defined:

- Improving overall safety for train systems with the use of a Digital Twin.

Following safety objectives are defined in order to achieve this goal:

- Predict accidents beforehand and act accordingly automatically
- Decrease the number of yearly hazards
- Decrease the severity of hazards

4.3 National and International Regulations

The relevant regulation, both nationally and internationally, needs to be obeyed in order to achieve license to operate. The regulations of interest is listed below:

1. EU Directive 2016/798 - Railway Safety[4]
2. EU Directive 2016/797 - Interoperability of the rail system within the European Union[5]

3. EU Regulation 1158/2010 - A common safety method for assessing conformity with the requirements for obtaining railway safety certificates[6]
4. EU Regulation 445/2011 - System of certification of entities in charge of maintenance for freight wagons and amending Regulation (EC) No 653/2007[7].
5. EU Regulation 653/2007 - Use of common European format for safety certificates and application documents in accordance with Article 10 of Directive 2004/49/EC of the European Parliament and of the Council and on the validity of safety certificates delivered under Directive 2001/14/EC[8].
6. EU Regulation 402/2013 - Common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009[9].
7. NEN-EN-ISO 9001 - Quality management systems - requirements[10].
8. NEN-ISO 55000 - Asset management - Overview, principles and terminology[11].
9. NEN-EN 50126-2 - (Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety)

One of the most relevant regulations is number 9. It describes what kind of perspectives and scenarios that should be considered when developing safety measures.
The specification of safety requirements shall consider the following:

- safety-related functions
- safety-related assumptions such as effectiveness (probability of failure on demand, per hour, etc.) of mitigation barriers (e.g. protection systems, redundancies)
- tolerable hazard rates (THR) or TFFR for quantitative requirements, if defined during the explicit risk estimation, considering:
    - definition of safe states
    - definition of the maximum permitted time to enter a safe state
    - failure detection measures or facilities or devices
- requirements resulting from the hazard analysis performed at upper level
- adaptation to interfaces
- organisational rules
- maintenance rules
- environmental conditions
- legal safety requirements

4.4 Norms and Standards

The relevant norms, standards and regulations for the Digital twin is these of which the system can interfere with and that affect the system of interest. The relevant ones are described in the ruleset and directives below:

1. EU Directive 2016/798 - Railway Safety[12]
2. EU Directive 2016/797 - Interoperability of the rail system within the European Union[13]
3. Railway Traffic Regulation (NL) Regeling Spoorverkeer[14]

4.5 Safety Critical Functions of the SoI

Safety regulations for approval on the European railway system

The Digital Twin may affect the trains controls in emergency situations. This means that it has to be ensured that it does not violate the EU safety regulation on railway safety (EU Directive 2016/798). Violation of this regulation includes exclusion of the European railway network so it is a top priority to obey this standard. There are different roles with different responsibilities in terms of development and management of railway safety. The relevant roles in the case of NS is the state because it is a state owned company. The safety requirements which are especially relevant for this role in the case of Digital Twin technology are listed below:

- Ensure that measures to develop and improve railway safety take account of the need for a system-based approach
- Ensure that all applicable legislation is enforced in an open and non-discriminatory manner, fostering the development of a single European rail transport system

Approval of the Digital Twin on the European railway system

In order to obtain approval of operation on the European railway system, EU Directive 2016/797 states the following requirements must be included in the railway system:

(a) Specially built high-speed lines equipped for speeds generally equal to or greater than 250 km/h;
(b) Specially upgraded high-speed lines equipped for speeds of the order of 200 km/h;
(c) Specially upgraded high-speed lines which have special features as a result of topographical, relief or town-planning constraints, on which the speed must be adapted in each case. This category includes interconnecting lines between high-speed and conventional networks, lines through stations, access to terminals, depots, etc. travelled at conventional speed by high-speed rolling stock;
(d) Conventional lines intended for passenger services;
(e) Conventional lines intended for mixed traffic (passengers and freight);
(f) Conventional lines intended for freight services;
(g) Passenger hubs;
(h) Freight hubs, including intermodal terminals;
(i) Lines connecting the above mentioned elements.

From the safety requirements above, we can see that the Digital Twin must be implemented in such a way that it does not interfere or violate these requirements. Furthermore these has taken into account when implementing the Digital Twin, such that it recognizes its environment and simulate the real requirements. In addition it should take the rail traffic regulations into account as well upon implementation so the system knows the rules of train traffic [15].

5. Identifying Hazards

A hazard analysis (PHA) will be performed [16, ch.2], thus controlling the hazards will have its own section (6). In this section, accident statistics concerning the Netherlands are analysed in order to identify hazards relevant for the scope of this report. The hazards will be categories in order to get a better overview and being able to focus on the most frequent ones and their severity. This approach will clarify which hazards to focus the most, and prepare for the last steps in the hazard analysis about how these can be controlled.

5.1 History of Accidents

Valid statistics of accidents are found the homepage of Eurostat. I website that holds different sort of statistics for the European Union. From the zip file available, with full table information, everything but statistics regarding the Netherlands is removed.

Accident/Year	2015	2014	2013	2012	2011	2010	2009	2008	2007	2006	2005	2004
Collision	2	2	2	2	4	5	2	2	4	4	2	2
Derail	1	0	1	0	3	3	2	1	0	2	5	1
Level crossing	29	18	25	20	14	9	13	21	26	12	26	25
Other	0	1	1	3	2	1	0	1	0	0	0	0
Rolling stock, fire	1	0	1	0	1	1	0	0	0	1	1	0
Rolling stock, moving	4	6	9	3	0	5	4	1	3	9	14	9
Total accidents in NL	37	27	39	28	24	24	21	26	33	28	48	37

Table 5.1: A view of the number of different types of accidents in the Netherlands [17].

The history of railway accidents in the Netherlands over the last decade, shown in table 5.1, clearly shows a clear pattern in the distribution of accidents. The number of collisions have stayed almost on a low constant level throughout the period. The number of derails have been decreasing over the years and are too, at a low level. However, the number of level crossing accidents are very high compared to the other types of accidents. The number was decreased in 2009 and 2010, but has increased to the same level as the previous years. This evolution shows that, either the focus has not been on this kind of accident, or the initiatives supposed to prevent them from happening has been ineffective. The number of other accidents along with rolling stock accidents have stayed stable at a low level. Accidents while rolling stock is in movement have gone up and own over the years.

Table 5.1 gave a good overview of what accidents that happen on the dutch railways. It helps identifying what type of accidents the Digital Twin should help decrease and thereby improve safety in environments where these occur. To improve the understanding of these accidents, statistics regarding which types that causes the most and worst casualties is analysed.

Accident, Severity / Year	2015	2014	2013	2012	2011	2010	2009	2008	2007	2006	2005	2004
Collision, injured	0	0	0	28	0	0	1	0	1	0	0	8
Collision, killed	0	0	0	1	0	0	1	0	0	0	0	0
Derail, injured	0	0	0	0	0	0	0	0	0	0	0	0
Derail, killed	0	0	0	0	0	0	0	0	0	0	0	0
Lvl Crossing, injured	2	5	1	9	3	1	4	6	7	2	12	11
Lvl Crossing, killed	12	9	8	13	9	8	13	18	19	12	18	17
Other, injured	0	1	1	4	4	0	0	0	0	0	0	0
Other, killed	0	0	0	2	1	1	0	1	0	0	0	0
Rolling stock fire, injured	0	0	0	0	0	0	0	0	0	0	0	0
Rolling stock fire, killed	0	0	0	0	0	0	0	0	0	0	0	0
Rolling stock moving, injured	3	4	9	7	0	8	6	0	2	4	7	2
Rolling stock moving, killed	0	0	0	0	0	1	0	1	1	5	7	7

Table 5.2: A view of accident types and the number of injured or killed in the Netherlands [17].

Table 5.2. Shows the distribution of how many that were either injured or killed by certain accidents. This distribution will later be used when hazards are identified and controlled as a guidance towards which accidents that is seen as the most important one and where safety should be increased. Looking at the severity distribution between the different types of accidents, it stands out the each collision can potentially have a huge amount of casualties. Luckily the number of deaths caused by collision is very low over the years. Further details from the full table in appendix A tells that the casualties are among staff and passengers. Unfortunately a lot of both injuries and deaths are caused by level crossing. Details from the full table informs that the primary casualties here are other people than passengers and staff, meaning people on foot, by bike etc. using the level crossing. The detailed table, referred to earlier, also tells that the casualties from rolling stock in movement are mainly passengers, but also staff.

5.2 Identification of Hazards

In identifying the hazards the System Safety Process (SSP) is followed into the third step[16, ch.5]. Based on the definition of the system of interest in section 3 and the objectives, describing the focus and boundary of this report, the hazards leading to the accidents, mentioned in previous section, can now be identified.

Potential hazards are identified and formulated through a brainstorm, review of accident history statistics from previous section and another source [18]. The challenge is to find these hazards by understanding the system in details and viewing the occurrence of the known accidents from different perspectives. The correct approach is not just to look at the statistics and then come up with incomplete and inaccurate proposals to prevent the accidents from happening. The accidents can occur for many reasons, and these are the ones the designer should focus on. The analysis is done for each accident in order to cover all of them in the best and most complete way, with also having the system definition and it's interacting between the human, system and environment interaction in mind.

The analysis resulted in the following hazards, listed respectively for each accident:

Collision:

1. Train driver misses red light due to:
   a. Heart attack
   b. Heavy fog
   c. Broken wheel on the train
2. Technical errors in the signalling system
3. Theft of copper wire leading to switches and signals not working.
4. Technical error in a switch
5. Transitioning between areas using different signal systems
6. Trees lying on the track
7. Miscommunication from maintenance vehicles

Derail:

8. Excessive speed of train in turns
9. Broken wheel
10. Broken rail
11. Slippery tracks
12. Poor track geometry
13. Wear and fatigue in the wheel-rail interface
14. Vehicle suspension faults

Level crossing:

15. Traffic jam results in vehicle being stuck between barriers.
16. Unguarded crossing, people who is not paying attention or gets distracted
17. Malfunction in the light and barrier system
18. Second train unexpectedly approaching
19. Violations by road users, ignoring the warning of lights and barriers at the crossing

Fire in rolling stock:

20. Electricity malfunction
21. Dangerous goods get ignited

Moving rolling stock:

22. Goods not attached correctly
23. Doors malfunction and opens while the train is moving

Other:

24. Suicide

See appendix A1 for full table with categories.

From this wide collection of hazards, a complete hazard tree for each accident is produced in order to provide a good overview of the hazards and how they result in provoking an accident. The hazard trees can be seen in appendix A2.

5.3 Hazard Evaluation

The hazard evaluation will include describing the severity categories for this project and assigning mentioned hazards to a category. Each hazard will also be assigned a probability value, which, along with the severity categories, results in a hazard risk assessment matrix. This will provide further knowledge about each hazard and whether or not they are the most important ones to control.

Defining Severity Categories

Description	Category	Definition
Catastrophic	1	Death, total disabilities
Critical	2	Partial disabilities, hospitalization of people, injuries inhibiting people for a

		longer period.
Marginal	3	Injuries resulting in inhibiting people for a short period
Negligible	4	Minor injuries that only inhibit people a day or two.

The definitions above are inspired by those in the used material [16, ch.5]. Due to the fact that this analysis focus on the hazards causing damage and harm to people, as explained in the beginning of section four, the definitions does not include information about how the system is affected.

Risk Assessment

Usually, as per the information in recent source referred to, the idea is to assign each hazard into a box within the risk assessment matrix, based on probability of occurrence and severity. Optimally, the probability is calculated based on statistics that implied how often a certain hazard occurs and the level of severity based on what these hazards may result in. However, it is not that easy.

Statistics of hazards leading to the different accidents mentioned earlier in section four are not available. This means that it is hard to determine which hazards leading to the same accidents are the most severe ones. Therefore, they must be treated as equally severe. Furthermore statistics that implies how often these hazards occur is difficult to obtain. Due to this, the assessment is done from a subjective point of view where solutions will differ, depending on the people doing the analysis. However, the purpose of the risk assessment matrix is still fulfilled, namely giving a good overview of which hazards that are the most important ones to focus on preventing, to improve safety. When reading table 5.3, please note that the numbers used for each hazard are the ones assigned to each one in section 5.2.

	Catastrophic	Critical	Minor	Negligible
Frequent				
Probable	15,19,16			
Occasional	18	22,23		1b,11
Remote	17	4,5,6, 7	2	
Improbable		3	1a,1c	8,9,10,12,13,14,20,21
Eliminated				

Table 5.3: Risk assessment matrix

Risk Evaluation

Based on the history of accidents from section 5.1 and a subjective approach to the assessment of each hazard, the risk assessment matrix is complete. The colours illustrate the risk decision criteria. The hazards in the red cells provides the largest incentive for control of the high risk, from which the risk lowers the further down in the right corner you go. The matrix clearly implies

that the hazards leading to the cross level accidents are the most frequent and severe ones. However this does not mean that the hazards in the orange area, leading to accidents for rolling stock in motion, should be ignored. They are at a high risk as well, just not as much as the ones in the red area. Even the hazards in the yellow area should be managed as they are still undesirable. The hazards in the green area are acceptable without further review.

Since the purpose of this analysis is to identify and control the hazards with the highest risk, it is decided to continue the process with the hazards causing the level crossing accidents. For future purposes, the hazards in the orange and yellow risk area should be addressed. So far, the hazard analysis gave a good overview of the hazards leading to different accidents were identified, analyzed and their risk impact evaluated.

6. Controlling Hazards

The dream scenario is to eliminate all hazards, but the reality is often quite different. Even though designers come up with great ideas, one must face the fact that not every hazard can be avoided completely. Some can be avoided, some can be controlled and some cannot. Based on the results from the previous section, designs that can reduce or eliminate the hazards will be developed and discussed in this section.

Before getting into the design proposals, a short introduction to sensors and actuators is given. Sensors are considered anything that the Digital Twin can use to observe the real world environment. Examples are: cameras, microphones, lasers, etc. Actuators are considered anything that the Digital Twin can use to interact with the real-world environment. Examples are: monitors, speakers and the train control system.

6.1 Design Proposals

In table 5.3, the hazards are categorized in severity and frequency in a risk assessment matrix. As mentioned, the focus will be on the most severe hazards with the highest frequencies. The addressed hazards are mainly caused by the human factor and the proposed solution addresses this with automations and safe fails in the event of an error in judgment or lack of attention from people in the environment of the train. The hazards in focus is listed below:

1. Traffic jam results in car being stuck at level crossing
2. Unguarded crossing, where people do not pay attention/are distracted and move onto the train track
3. Malfunction in the light and barrier system
4. Second train unexpectedly approaching the crossing
5. Violations by road users ignoring the warning of approaching trains

Traffic jam results in car being stuck at level crossing.
Based on the distance between the train (GPS signal) and the level crossing, the train driver gets notified that a sensor has captured movement on the crossing and after a certain time, if the driver does not act, the train should do an emergency brake. The goal of this solution is to

reduce the severity of accidents like this. Due to the involvement of the human factor, It is not possible to eliminate this issue but with an automated emergency brake system, the human reaction time and observance ability is taken out of the equation which should either make avoid impact or massively reduce the speed of the train before impact with a car that is stuck in a crossing.

Unguarded crossing, where people do not pay attention/are distracted and move onto the train track

This hazard is categorized into two types, concerning pedestrians and vehicles. To wake up unattentionate pedestrians, speakers at the crossing will alarm when a train is coming based on the distance from the crossing. In regards to vehicles, the train will capture movement with a sensor on the train that spots a vehicle on an unguarded crossing from a distance and trigger an emergency braking procedure if appropriate. This solution is not meant to eliminate the hazard but to control it and greatly reduce accidents by preventing them to happen by alarming unaware civilians.

Malfunction in the light and barrier system

External sensors show if the barriers are down by observing the light and barriers at crossings. In the event that a train is coming and the barriers or light is not in the desired state, the Digital Twin will observe this and brake the train to avoid any potential accidents. The braking will take place when the trains distance to the crossing is a break-length. The goal of this solution is to eliminate the hazard and this is more easily possible because it is not based on the human factor but technical factors which are more predictable than human behavior.

Second train unexpectedly approaching the crossing

When two trains drive by an intersection within a few seconds, It can introduce dangerous situations where pedestrians or vehicles think there everything is safe when the first train has driven by. This is especially a danger at unguarded crossings, and the solution in this case is (like with the unattentionate people at unguarded crossings) speakers that notify pedestrians when two trains are driving by and automated emergency braking procedure in the event of vehicles on the crossing when the train is close to the crossing. When this happens at a guarded crossing, the solution is the same but the sensor is at the crossing instead of the train. This is to increase safety at the crossings. This will not eliminate the problem because it is based on an unpredictable human factor but is meant to greatly reduce the accidents by alarming and notifying civilians about the environment they are in.

Violations by road users ignoring the warning of approaching trains

This hazard is too expensive to prevent because it is based on a very unpredictable human factor. People ignoring rules crossing the railway when they are not supposed and even suiciding cannot be prevented because it would mean making safeguards around all thinkable perspectives and scenarios of the railway system, which is astronomically expensive to prevent. The solution to this problem is to change the culture instead.

7. Monitoring the System

In order to monitor the safety of the system, indicators needs to be put in place to be the base of this. Due to the fact that the systems hazards is highly based on the human factor, the safety indicators that is considered with this project are:

- The amount of incidents every year caused by human factors in % with regards to the incidents of focus in this report.
- The severity of these incidents every year categorized as catastrophic, critical, minor and negligible.

The implementation of the design choices proposed in this paper will lead to a decrease in these two indicators. It is difficult to say by how much, but that could be documented by looking at new statistics after the implementation of the Digital Twin. These kinds of lagging indicators are good to measure change in safety performance over a period, but it is also suggested that the SoI uses leading indicators. Leading indicators consist of safety initiatives that proactively prevent accidents before they happen. Some leading indicators could be:

- Safety training of personnel
- Training of personnel in using the Digital Twins' many possibilities including:
    - Traffic behaviour analysis
    - Wear and maintenance analysis
    - Runtime-monitoring of tracks and train

The DT provides the safety initiatives that are necessary for using leading indicators. This will improve railway safety overall as the runtime-monitoring tools offered by the DT provides an easy, predictable and optimized way of reducing risks and minimize potential accidents from happening. This is possible due to the precise reflection of reality the DT is and the IoT devices integrated with it, that provides the data as foundation for this runtime monitoring.

The Digital Twin really does provide a ton of possibilities for companies like Protail and NS. In this report the focus has been on safety in the matter of hazard elimination or reduction. However the DT can also be used to reduce cost, performance or improving designs for the railway system. The report thereby implies that new and innovative technology can help improve safety in a very traditional and safe-sensitive industry as the railway system.

8. References

[1] : Picture for front page
https://www.google.com/url?sa=i&source=images&cd=&ved=2ahUKEwiqpPz3k6TmAhUSL1AKHWoVAO0QjRx6BAgBEAQ&url=https%3A%2F%2Fwww.pinterest.com%2Fpin%2F805792558310590507%2F&psig=AOvVaw1hlhSEzSfeMLfOpLNo9y3e&ust=1575828830574373

[2]: Madni, A. M., Madni, C. C., & Lucero, S. D. (2018). Leveraging Digital Twin Technology in Model-Based Systems Engineering.

[3]: Glaessgen, E. H., & Stargel, D. S. (2012). The Digital Twin Paradigm for Future NASA and U.S. Air Force Vehicles.

[4]: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0798&from=EN

[5]: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1519999459620&uri=CELEX:32016L0797

[6]: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010R1158

[7]:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2011.122.01.0022.01.ENG&toc=OJ%3AL%3A2011%3A122%3ATOC

[8]: https://ec.europa.eu/transport/sites/transport/files/celex_32007r0653_en_txt_0.pdf

[9]:
https://connect.nen.nl/standard/openpdf/?artfile=211646&RNR=211646&token=81c981fa-63d8-4010-851b-7d69be2cde3c&type=pdf#pagemode=bookmarks

[10]: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32013R0402

[11]:
https://connect.nen.nl/standard/openpdf/?artfile=558714&RNR=193610&token=0bd60240-4d85-4ff8-820d-f2a79f5294b4&type=pdf#pagemode=bookmarks

[12]: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0798&from=EN

[13]: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0797&from=EN

[14]: https://wetten.overheid.nl/BWBR0017707/2019-10-01

[15]: https://wetten.overheid.nl/BWBR0017707/2019-10-01

[16]: System safety and risk assessment, a practical approach. 2nd edition, 2014

[17]: https://ec.europa.eu/eurostat/web/transport/data/database
go to transport -> railway transport -> railway transport accidents history. Download zip for full table.

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

Appendix

A1 Table: Accidents and their hazards

Indicator	**Hazards (reasons why)**	**Human/system/environment**
Collision of train with rail vehicle	Missing of red sign due to heart attack	human
	Missing of red sign due to heavy fog	environment
	Missing of red sign due to broken wheel	system
	Missing of red sign due to failure of brakes	system
	technical errors in the signalling system.	system
	Stealing of copper wire> switches and signals do not work	environment
	Isolation error in a switch (malfunction of switch) results in trains on the same track	system
	transitioning between areas using different signalling systems	Environment (different regulations per countries)
collision of train with obstacle within the clearance gauge	Trees which fall on the track	environment
	collision with maintenance cherry picker	environment/human
derailment of train	too high of a speed in the turns during maintenance > speed should have been adjusted	human
	Broken wheel	system
	Broken rail	system
	Slippery tracks due to weather conditions	environment

	poor track geometry	system
	wear and fatigue in the wheel-rail interface	system
	vehicle suspension faults.	system
	excessive speed	human
level crossing accident	traffic jam results in car being stuck at level crossing.	environment
	unguarded crossing, where people don't pay attention/are distracted and move onto the train track	human
	Malfunction in the light and barrier system	system
	Second train unexpectedly approaching the crossing.	human
	violations by road users ignoring the warning of approaching trains.	human
fire in rolling stock	Electricity malfunction	system
	Dangerous goods gets ignited	environment
accident to persons involving rolling stock in motion	Goods are not attached correctly within the required measures.	human
	Doors malfunctioning and opens while the train is in motion.	system
	People near the tracks unaware of a train coming	human
Other	suicides	human
	carriage of dangerous goods such as chemicals, petrol, liquefied gasses and nuclear waste.	environment

A2: Hazard Trees

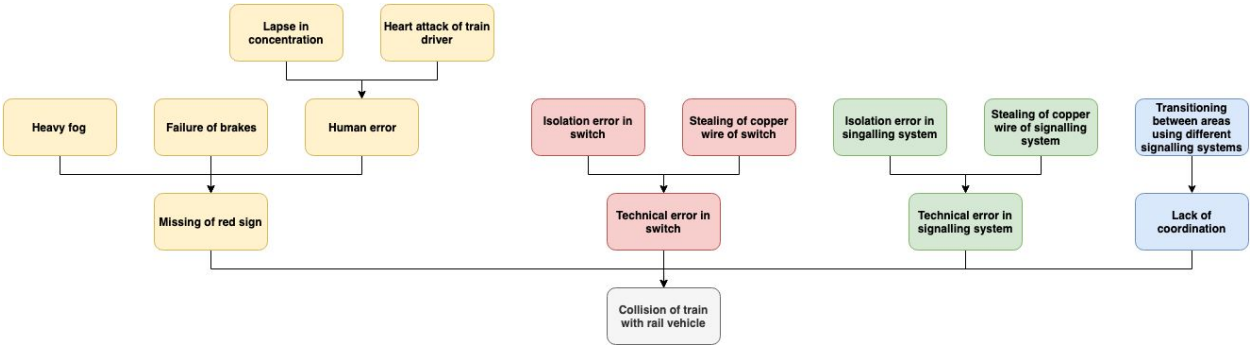

Figure 5.1: Hazard tree, Collision

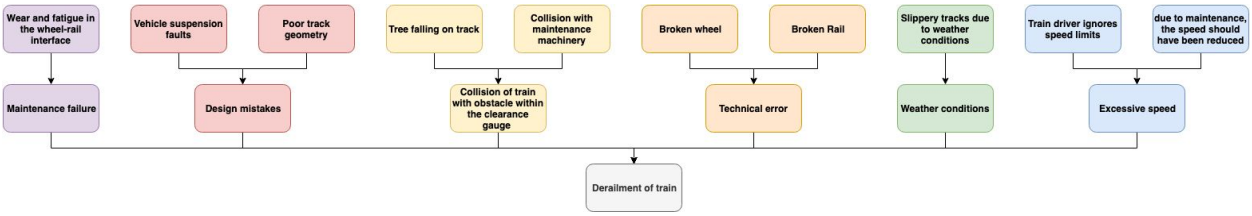

Figure 5.2: Hazard tree, Derail

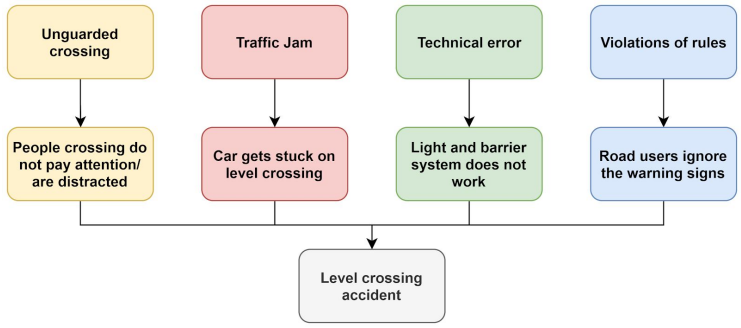

Figure 5.3: Hazard tree, Level crossing

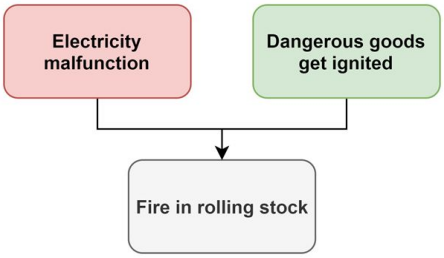

Figure 5.4 Hazard tree, Rolling stock in fire

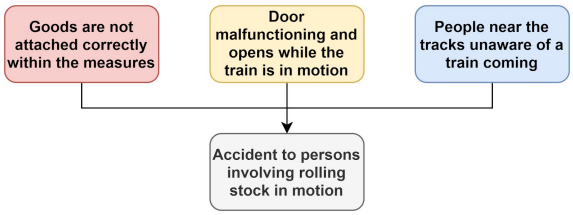

Figure 5.5 Hazard tree, Rolling stock in movement