

# Identification and cause isolation of Dutch rail dispatching system failure notifications

B. Leistra

January 19, 2017







*“Voorkom storingen door beter onderhoud en als ze er zijn,  
zorg dan als de sodemieter dat ze opgelost worden.”*

Pier Eringa - CEO ProRail  
(Algemeen Dagblad, October 18, 2016)

In memory of



*Laurens Leendert Cornelis van Strien*

\* 18 juni 1989, Eindhoven

† 13 oktober 2012, Rotterdam



*Julius Krijn van Gilst*

\* 31 januari 1989, Haren

† 16 september 2014, Los Angeles





**WACHT** tot het rode licht gedoofd is  
er kan nog een trein komen



# Identification and cause isolation of Dutch rail dispatching system failure notifications

by

B. Leistra

in partial fulfilment of the requirements for the degree of

**Master of Science**  
in Civil Engineering,  
Transport & Planning  
with Rail Annotation

at the Delft University of Technology  
Academic Year 2016-2017, Quarter 2

to be defended privately on Thursday, January 19, 2017 at 03:00 PM,  
and presented publicly on Thursday, January 19, 2017 at 04:00 PM.

Status: Final  
Date: January 19, 2017  
Student number: 1511831  
Email: leistra@gmail.com  
Project duration: July 4, 2016 – January 19, 2017

Thesis committee:	Prof. dr. ir. B. van Arem,	Chair, TU Delft, Civil Engineering T&P
	Dr. R.M.P. Goverde,	TU Delft Civil Engineering T&P
	Ir. P. Wiggendaad,	TU Delft Civil Engineering T&P
	Dr. D. Kurowicka,	TU Delft, Applied Mathematics
	Ir. W. T. Op de Woert,	ProRail

*This thesis is confidential and cannot be made public until January 31, 2021.*

After which, an electronic version of this thesis is available at  
<http://repository.tudelft.nl/>.







# Acknowledgements

This thesis is the result of my graduation research, concerning disruption management, on the Dutch railway network by ProRail and concludes my Master's studies in transport and planning with a rail annotation at the faculty of Civil Engineering and Geosciences at the Delft University of Technology. From July, 2016, until January, 2017, I worked on this thesis as an intern of the *meldkamer spoor* at the department of Asset Management within the Operational Control Centre Rail (OCCR) in Utrecht on behalf of ProRail.

Since the start of my Master's degree, I have been determined in my ambition to finish the two-year program within a year and a half and to be the first to graduate with a rail annotation to my degree. The keystone to that goal was to finish my graduation research within 28 weeks. You are reading this thesis, and that confirms I have achieved my goal. I am very glad to been able to stick to my plan, but without the assistance of my assessment committee, this accomplishment would not have been possible. First and foremost, I thank my daily supervisors, Rob Goverde and Walter op de Woert for their intensive support and detailed feedback on my work. Additional gratitude goes to Prof. Bart van Arem and Dorota Kurowicka for feedback in their respective areas of expertise and for their trust in my work.

Aside from those among my assessment committee, I want to say thanks to my direct colleagues at the OCCR and ProRail. Everyone at the OCCR was always interested in my work, and they included me in several other task so that I could experience what ProRail AM is responsible for. I had many conversations, so thanks to everyone I talked to and who answered my questions regarding my research subject. Special thanks to Walter, again, for linking me with all the interesting people of ProRail who were most relevant to my studies.

I want to thank my fellow students, with whom I worked closely during my time in Delft. I want say thanks to my family and friends as well, for supporting me during my research. Much has happened since the start of my studies, both ups and two very deep downs. My deep gratitude goes to my parents, their partners, my brother Paul, my grandparents and all my friends. Their interest, support and love were essential to me.

Finally, I want say thanks to my girlfriend Anne, whose unconditional and everlasting interest, support and love amazes me every day. Without her, I would never have had this goal, and I certainly would never have achieved it. I love you.

Enjoy reading!

*B. Leistra*  
*Den Haag, January 2017*







# EXECUTIVE SUMMARY

**Abstract** - This research assesses if, and how, the disruption-management process of the Dutch rail infrastructure manager ProRail could be improved with better use of additional information. Through mapping the system elements in a fault tree (FT), the causes of a failure notification can be visualised. After identifying other effects for all failing elements, the side effects of the main failure notification can be mapped. The side effects are reformulated in identifying questions for an event tree (ET). When, in the case of a failure, the ET is followed, the cause of the failure can be better identified and isolated. The methodology was tested for a general multidisciplinary 'power supply disturbed' notification. This study shows that the approach can contribute to more effective disruption management. In current practice, the specific cause, location and mechanic discipline are unknown beforehand. The approach presented here can contribute to clarifying those unknowns by using side effect of PRL failure notifications.

## Introduction

ProRail is the Dutch rail infrastructure manager (IM) and is therefore responsible for the tasks as shown in Figure 1.

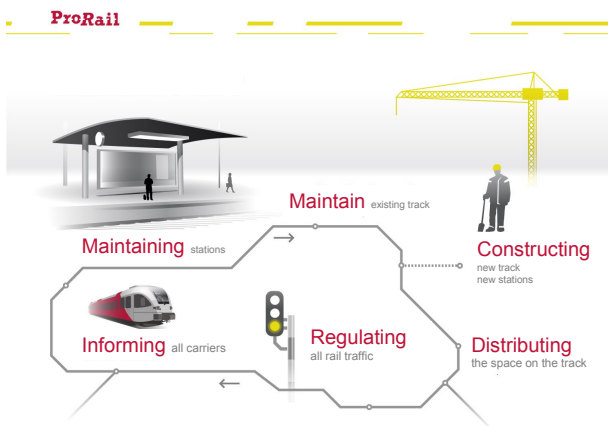


Figure 1: Main tasks of ProRail.

The usage of the railway tracks has increased in recent years, and is to become even more intensive the upcoming years. Space in urban areas is not always available, and budgets are limited, so ProRail is constantly exploring innovative ways to accommodate the increase of capacity and availability of the tracks. Every day, various irregularities or disruptions occur that limit the availability of the tracks. Irregularities are split up into different causes: engineering,

third parties, processes, weather and other. One way to increase the overall availability of rail-space is to reduce the hindrance caused by irregularities. Some irregularities are easier to influence than others. Weather is difficult to influence, and can be dealt with only by establishing more robust (and more expensive) infrastructure. Third-party causes of disturbance, such as people walking along the tracks or suicides, are also difficult to prevent. Engineering failures can sometimes be prevented by better design or maintenance (with higher costs). Beyond the number of irregularities, the impact of a disruption can be mitigated. ProRail is also responsible for managing the failure-recovery process. Railway-disruption processes can be described by the bathtub model, as can be seen in Figure 2. This bathtub model can be partitioned into three phases. In Phase 1, the traffic decreases when a disruption occurs, and the cause must be identified. In Phase 2, traffic is not possible or is possible only at a very low level, and the problem is being solved. The third and last phase starts when the problem is solved and traffic can return to a normal service level again. Technical failures are reported during Phase 1 and a mechanic is sent to the location of the failure. In Phase 2, the mechanic assesses the exact cause and location of the failing element and fixes the problem.

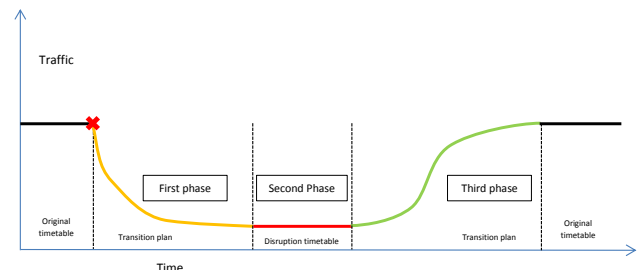


Figure 2: Bathtub model.

ProRail has to manoeuvre between different stakeholders, their clients (train-operating companies [TOCs], regional and local governments) within the boundaries imposed by laws and regulations, all in a political and media arena. Due to the intensive use of the rail network in the Netherlands, even a small disruption can effect many trains, and consequently passengers and freight. Since ProRail is only the operating, designing and managing organisation for maintenance and repairs, it depends on four *procescontractaannemers* [contractors] (PCAs). Maintenance and repairs have been split up by the PCAs and ProRail, into several areas of specialisation: *energievoorziening* [power supplies] (EV), *seinwezen* [signalling] (SW), *kunstwerken* [engineering



constructions] (KW), *baan* [track] and ICT, all with their own skilled personnel. Within this context, ProRail's Asset Management (AM) department is constantly trying to improve the availability and performance of the Dutch railway network.

### Problem Description

This study investigates the possibility of more effective failure recovery by identifying the possible cause and location responsible for generating a failure message from the *procesleiding rijwegen* [route-processing system] (PRL). Phase 1 and Phase 2 are therefore the systems on which this study primarily focusses. This study researches how additional information and data can facilitate earlier and remote cause-identification and location-determination. Internal research performed after two high-impact disruptions indicated that better usage of available data and information might contribute to faster failure-recovery. In practical terms, AM ProRail wants to know how they can better inform the PCAs, so that a mechanic will know the location of the failure and can anticipate what is needed to address that failure by using additional information about what the failure could be. Because the railway infrastructure elements can be spread over a large area, it would be useful for mechanics to know where the exact location of the element is or to know its control elements, so that these mechanics can work more efficiently on site.

### Research Objective

Therefore, the following research objective was formulated to guide this research:

*A more effective failure recovery through a more extensive and better use of operational information by Asset Management.*

### Research Question

To achieve the objective, this study had to discover whether information usage can contribute to better and faster identification of the nature, cause and location of a problem. In this way, a technician can better prepare for the problem, locate it faster and know what materials are needed to fix it. Therefore the research question arrived at to pursue the above objective was as follows:

*How can the use of more and better information contribute to the identification and isolation of the nature, cause and location of a failure of an infrastructure element based on a PRL failure notification in order to achieve a reduction in downtime and a higher availability?*

### State of the Art

This study employed exploratory research. Results were not known in advance, and the research was set-up to systematically explore the possibilities of wider and better use of in-

formation. In this way, possible relationships can be found and underlying structures mapped. All potentially interesting information was collected through qualitative research with a case study. The current disruption-management process was assessed, and a suitable method was selected.

### Disruption Management

At a given moment, a (technical) failure notification is generated by the PRL system, which is the control, monitoring and route-setting system of the dispatcher. Several sources are combined to help the dispatcher to control his/her designated area. The PRL system also passes on failure notification concerning the underlying interlocking/safety (DOSS/B-Relay/VPI/PLC), control (EBP/KEVCE/KBV) and monitoring systems (TROTS). The *treindienstleider* [dispatcher] (Trdl) receives those notifications. The dispatcher is part of the *verkeersleiding* [traffic control] (VL) and is responsible for the safety of the train traffic in his/her own designated area. The dispatcher also has direct contact with train drivers. This person can receive a notification from a train driver or as a system warning. It is also possible that a third party (emergency services, bystanders or a PCA) declares a failure. In that case, the notification is received by the call centre of the *meldkamer spoor* [railway control room] (MKS). The MKS is a generic name for the failure-handling organization of ProRail's AM department within the Operational Control Centre Rail (OCCR). The term covers the directors, call centre operators, the *operationeel besurtingscentrum infra* [operational control centre infrastructure] (OBI) and the back office. The OBI is responsible for the intake and forwarding of 40,000 (asset) failures a year, originating from several different channels to the different responsible PCAs. The failure is forwarded to the PCA in a so called *rapport van onregelmatigheid* [report of irregularity] (RVO) and contains the ID or name of the element, its location, a description of the irregularity and a priority level, all in an SAP environment. When the PCA mechanics arrive at the failure location and a safe working environment is established, the mechanics can start diagnosing the problem. Depending on the prognosis, diagnosis, priority, point of time and other influences, the MKS and dispatcher decide whether the problem needs to be fixed immediately or at another time. Depending on the outcome, the mechanics start to fix the problem or mitigate its effects. When the problem is fixed, Phase 3 starts, and the train service can be restarted. An RVO consists of several elements but does not indicate the root cause of the failure. For example, the following notification was received during the case study: '*Lunetten level crossing 36.5 disturbed and track between switches 1117 and 1115A is improperly occupied*'. Then the RVO states: '*Ln : WL-1117/1115A t.o.b.s., ovw 36.5 disturbed*'. What component is causing the *ten onrechte bezet spoor* [improperly occupied track] (T.O.B.S.) is not known, and the mechanics need to diagnose the exact problem.

Almost all events or actions performed by the PRL system are logged for every dispatcher and consequently for

the whole network. Also, all system layers have predefined error notifications. When something does not perform as planned, the relevant layer sends this notification to the PRL, which logs all internal failure notifications. The TROTS is used to monitor trains, when their route is set by the PRL system. This monitoring is achieved through a *treinnummer volgsysteem* [train number follow-up system] (TNV) and track element status updates from the control systems, as described earlier. Every TROTS event is logged and stored.

The VL or dispatcher can see the overall picture of what is going on in his control area, at all times. All is shown on the operating screen of their workstation. The downside is that only current failures are shown, so historic or short-lived failures cannot be recalled by the dispatcher. Historic and short notifications are stored in the log file and are accessible when they are stored by ICT-operations (ICT-O). Not all consequences of a failure are logged, because some are indirect effects and do not have individual failure messages. For example, it is normal for a switch to become inoperable when there is route set over the switch, and so it does not always signal a failure; on the other hand, sometimes it is an effect of a failure.

## Methodology

As mentioned earlier, the objective of this research is to identify useful information for improved identification and isolation in case of a technical failure notification. To achieve the objective, the useful information needs to be identified.

This identification can be made through exploratory research, where the results are not known in advance and the research is set up to explore systematically the possibilities of wider and better use of information. In this way, possible relationships can be found and the underlying structures are mapped. All potentially interesting information is collected. This investigation is conducted through qualitative research with a case study.

Qualitative exploratory research can be pursued with various methods. One of those methods is fault tree analysis (FTA), a systematic analysis technique to determine the root causes of a specified undesired event. An FTA can be used to evaluate complex dynamic systems to be understood and prevent potential problems. Using rigorous and structured methodologies, a fault tree (FT) can be constructed.

An FT is a logically and graphically represented combination of possible events or failures that lead to an undesired event or state. The FT shows the logical fault paths from all possible root causes, at the bottom, to the single undesired event, at the top. FTs consist of nodes, interlinked together in a treelike structure. The nodes represent fault or failure paths and are linked together by Boolean logic and symbols. The operators used for this research are shown and explained in Figure 3.

Symbol	Type	Description
	Node Text Box	Contains the text for all FT nodes. Text goes in the box, and the node symbol goes below the box.
	Primary Failure Code: X#	A basic component failure; the primary inherent, failure mode of a component. A random failure event.
	OR Gate Code: G#	The output occurs only if at least one of the inputs occurs.
	AND Gate Code: G#	The output occurs only if all of the inputs occur together.
	Transfer Out Code: T#	Indicates where a branch or sub-tree is transferred to the same usage elsewhere in the tree.
	Transfer In Code: T#	Indicates where a branch of sub-tree is inserted from another usage elsewhere in the tree.
	Secondary Failure Code: Z#	An externally induced failure or a failure mode that could be developed in more detail if desired.

Figure 3: Fault tree symbols.

The FTA was selected because it is a relatively simple and easy-to-understand top-down method. Since the start of the analysis is a top event (failure notification) and not a component failure, the FTA fits better than a bottom-up method, such as a failure mode effect and criticality analysis (FMECA). The FTA was used after the notification was created and was not used to predict a failure; therefore more complex methods, like Bayesian belief nets (BBN), do not suit this study. Since this research is qualitative and since probabilities are not quantified and only logical dependencies need to be identified, the complicated method of BBN is too powerful and too resource intensive. In addition, the FTA is a well known and proven method used in several other industries (aviation and chemical plants).

After the systems and elements that can cause failure notifications were identified, specific failure information about the specific component needed to be identified. The question, 'What happens if that component fails?', needs to be answered. ProRail had already constructed FMECAs that could be used. In the FMECAs, the effects of the failure of the element are described, which can be seen as side effects to the main failure notification.

For implementation and to identify the cause of the failure notification, the side effects were assessed. This assessment was performed by following a flow chart based on the known side effects. One commonly used flow chart type is



the event tree (ET). An event tree analysis (ETA) is an analysis technique used to identify and evaluate the sequence of events in a potential accident scenario following the occurrence of an initiating event'. By performing an ETA, a visual logic tree structure can be constructed, an ET. The ET allows one to determine whether the initiating event will develop into a serious mishap or is sufficiently controlled by the safety mechanism and procedures implemented in the system design. By answering several binary questions (yes/no, success/failure), the ET can manifest several different branches, all representing a different possible outcomes from a single initiating event.

Where as FTs flow from the sources in the direction of the undesirable event, ETs are reversed: they start with a single undesired top event and consequently model the effects that can occur. Several combinations of conditions lead to certain consequences. ETs start with the initiating event, followed by several questions for outcome identification. When a question is answered with 'yes/success' the upper branch is chosen, and if 'no/failure' the lower branch is followed. When all (relevant) questions for a branch are answered, the branch results in an outcome. The outcome can be a binary answer to a question or an individual result. The combination of the FT on the left and an ET on the right, along with the transformed FMECAs (as pivotal questions) in the ET, can be used to assess a failure notification.

### **'Power Supply Disturbed'**

To check whether the stated methodology works in practice, a test case was constructed for a specific notification. For some failures, it is immediately clear which mechanical expertise is required, as well as what and where the mechanic needs to fix the problem (for example, a level-crossing failure). Other failure notifications require mechanics of various expertise, and the cause could be on several places in a large area. In the case of a more general notification, it is not clear which mechanical discipline is required and where the mechanics need to go to solve the problem. Additional information could support the disruption-management process in assigning the right mechanics and sending them to the right location.

An example of an unclear notification is the '*stroomvoorziening gestoord*' ['power supply disturbed'] message. The notification is generated if the *treinbeveiligingen treinbeveiligingsinstallaties* [train control and train protection] (TBB) power supply is disrupted. Many of the (interlocking) elements, as well as railway safety in general, are dependent on power supply. This notification is generated around 2,000 times a year, of which 35 result in a train service disruption. In total 1,318 trains were effected, that led to 54,000 train delay minutes. In the past year, two disruptions were indicated as very large and were researched by ProRail. The internal research indicated that a better use of information could help the disruption-management

process and that up to 1 hour and 45 minutes of downtime could be reduced for those specific cases.

### **Background**

The 'power supply disturbed' notification is generated by the system that monitors all non-traction power and is displayed in the operating screen of the dispatcher. All non-traction power indicates power used for purposes other than moving the train: train detection, train control, route setting, switch setting and communication systems. The notification is generated when there is a slight decrease or very short interruption of the power supply. The different monitoring units are connected in series; hence if there is no power in one or more components or if one of the elements fails, the (same) notification is generated. Once the power supply is restored, the notification automatically disappears. The notification was introduced for two reasons: safety and reliability.

With regard to safety, because of the chosen relay interlocking system there is a theoretical chance that if the power supply is decreased or briefly intermittent, the system responds as if a train drove by and releases the granted route behind it. This response allows the system to set a new route, meaning that two trains can end up on the same track, potentially resulting in an accident. When the train detection power supply fails, the dispatcher is alerted to this failure by the 'power supply disturbed' notification. In addition to the notification, the system also prevents an accident from happening, through additional safety measures. When the train detection power supply fails, this failure triggers a mechanism that blocks the switches for operation and sets all signals, for the whole control area, into the stop position. This setting prevents trains from being guided to another (new) track and forces all nearby trains to stop in order to avoid an accident. When the power supply is restored, the dispatcher must check whether everything is safe and has to take a physical action to undo this blockade, preventing an unsafe situation from arising. Maintenance and repair of this problem is the responsibility of SW.

The second reason for the introduction of this notification is that some components require more reliability of their power supply. These critical components are provided with a back-up battery power supply, so that in case of a loss of normal power supply, they can still be operated. Once the normal power supply of those elements is interrupted, the 'power supply disturbed' notification is generated and the system switches to the battery back-up power supply. These batteries can supply the system with power for 3 hours, providing sufficient time to fix the problem or install another emergency power source. The maintenance and repair of these components is performed by EV.

Due to the design of the system, failure notification can also be activated when power is supplied by the grid but a component of the systems fails. If a component fails, it

Initiating Event	Proximal Events							Outcomes		
Power supply disturbed	Short message? AND Reported event? AND Under control?	Abnormal control area?	Entire control area?	Fallen signal(s)? (SW)AND Switch(s) locked?	TDR(s) visible?	Signal Extrapolated? (SW)AND Flashing power? (SW)AND Switch NC?	Switch closed?	Was power supply failure Ob?	Mechanics diagnosis	Failure
	Y	Y	Y	Y			Y	Y	P5	X8 - Z2
								N	SW/PS/EV/CT	Unknown - G3 branch
								N	SW/PS/EV/CT	Unknown - G3 branch
									SW/PS/EV/CT	Unknown
									SW/CT	X-8/9 - Z1
									EV	G-4/5 branch - X2 - Z1
		N	Y	Y	Y	Y		Y	P5	X8 /Z2
									EV	G12 branch
								N	SW	X6 / Z1
									SW	X5 / Z1
									SW/CT	Unknown - Z1
								Y	P5	X8 / Z2
	N	Y	Y	Y	Y	Y			EV	G12 branch
								N	SW	X6 / Z1
									SW	X3 / X5
								Y	P5	X8 - Z2
									EV	G12
								N	SW	G9
	N	N	N	N	N	N			SW/CT	Unknown
									EV/CT	X1 / X2

xiii



## Conclusions

For at least one failure notification, the cause could be identified faster, and if the PCA is better informed they can send the right mechanic to the right location. Thus, a reduction in downtime could be achieved. By analysing a failure notification in retrospect and using a system-wide approach instead of a component-based approach, the notification can be more effectively assessed. When an FT is constructed, it can be made visible which components are linked, and, if they fail, can trigger a specific failure message. If subsequently the individual components are assessed to see the (other) effects of a component failure, the side effects of the initial failure notification can be revealed. By combining and reformulating the side effects into binary questions, an ET can be constructed, and when followed the appropriate mechanic can be assigned. In certain instances of the test case, it is also possible to identify the specific cause and thereby the location of the failure. By answering the proposed questions, additional information is added to the RVO. To gain the extra information, the dispatcher and the OBI operator should communicate clearly, and all questions should always be answered. Codings and names of all specific components must be listed correctly. Only then is it possible for the PCA or ProRail to act thoroughly, and the additional information can provide added value. When the PCA receives a more specific RVO, it can act in a more effective way by immediately sending the right mechanic, bringing the right spare part and driving directly to the right location.

## Recommendations

In order to implement the method, further evaluation needs to be performed with the PCA to check how and whether they want to use it.

For implementation of the method, the process as shown in Figure 6 is recommended. To further expand the approach, further research must be performed on other discipline-transcending or hard-to-locate failures or notifications, like T.O.B.S. failures or multiple level-crossing failures. After expanding to other failures, the approach should be checked for every single location in the Dutch rail network to guarantee the success of the approach.

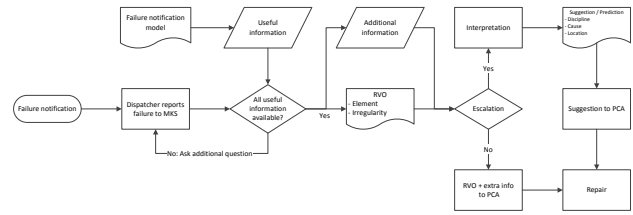


Figure 6: Method implementation process.

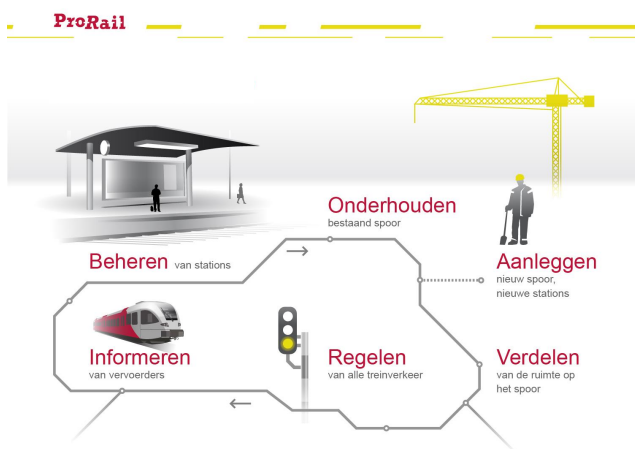
Implementation should be secured at all levels of ProRail, and it should be checked how the method performs when all required information is available. Therefore, the quality of the historical SAP data should also be improved, and a physical separation of the elements in the ‘power supply disturbed’ notification could be researched. To ensure the right questions are asked, a further development of a smart failure intake could be considered.

# Management Samenvatting

**Abstract** - Dit onderzoek bestudeert of het storingsmanagement proces, van de Nederlandse spoorbeheerder ProRail, kan worden verbeterd door optimaal gebruik te maken van beschikbare informatie. Het onderzoek is gedaan door elementen in kaart te brengen die, bij falen, een foutmelding in het procesleidingsysteem kunnen activeren. De elementen die gekoppeld zijn aan een bepaalde foutmelding zijn in beeld gebracht met een foutenboom. Hierna zijn randverschijnselen geïdentificeerd voor ieder (falend) element in de foutenboom. Op basis van de randverschijnselen en de foutenboom kan met behulp van een gebeurtenissenboom een beter beeld van de storing worden gecreëerd. Door de randverschijnselen te herformuleren naar identificerende vragen, kan in het geval van een storing de gebeurtenissenboom worden gevolgd en de oorzaak van de storing beter worden geïdentificeerd en geïsoleerd. De methode is getest op een generieke multidisciplinaire 'stroomvoorziening gestoord' melding. Deze aanpak draagt bij aan een effectievere aanpak van storingen. Bij de huidige aanpak van de 'stroomvoorziening gestoord' melding is de specifieke oorzaak, locatie en monteur discipline niet op voorhand duidelijk. De voorgestelde aanpak draagt bij aan het verduidelijken van aard, oorzaak, locatie en monteur discipline bij een storing door gebruik te maken van randverschijnselen van een procesleiding rijwegen storingsmelding.

## Introductie

Prorail is de Nederlandse spoor infrastructuur manager en daarmee verantwoordelijk voor de taken zoals weergegeven in Figuur 7.



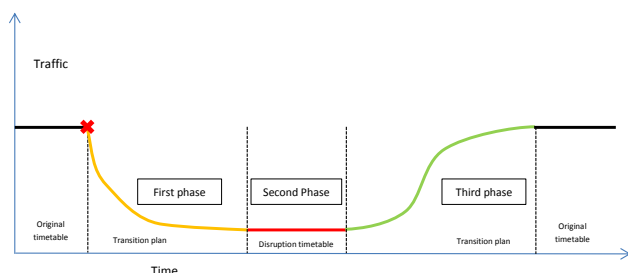
Figuur 7: Kerntaken van ProRail.

Het gebruik van het spoor is de afgelopen jaren toegenomen en zal ook de komende jaren verder groeien. De ruimte in stedelijke gebieden is beperkt en budgetten zijn gelimiteerd. Om deze groei te herbergen is ProRail constant op zoek naar innovatieve manieren om de capaciteit en beschikbaarheid van het spoor te verhogen. Elke dag zijn er verstoringen ten opzichte van de dienstregeling die de beschikbaarheid van het spoor beperken. Oorzaken van deze verstoringen zijn onder andere: falende techniek, invloed door derden, falende processen en bijzondere weersomstandigheden. De ene oorzaak is makkelijker te voorkomen of te beïnvloeden dan de andere. Het weer kan bijvoorbeeld niet direct worden beïnvloed. De infrastructuur kan echter, tegen een hogere prijs, wel robuuster gemaakt worden voor uitzonderlijke weersomstandigheden. Storingen door derden, zoals mensen die langs het spoor lopen of suicide, zijn lastig te voorkomen. Sommige technische storingen kunnen worden voorkomen door beter design en onderhoud maar tegen hogere kosten. Een andere manier om de algehele beschikbaarheid van het spoor te verhogen is om de impact en hinder in geval van verstoringen te verminderen. Naast het aantal storingen te verlagen kan ook de impact van een verstoring worden beperkt om de capaciteit te verhogen. ProRail is bij het storingsherstel verantwoordelijk voor het managen van het herstel proces. Het storingsherstel proces kan worden beschreven door middel van het badkuipmodel zoals weergegeven in Figuur 8. Het badkuipmodel kan worden opgedeeld in drie fases. In fase 1 nemen de treinbewegingen af doordat een storing zich voordoet, de oorzaak wordt achterhaald. In de tweede fase is er nauwelijks tot geen treinverkeer mogelijk, het probleem wordt verholpen. Bij de start van fase 3 is het probleem verholpen. Tijdens deze fase wordt het treinverkeer weer opgestart en teruggebracht naar een situatie zonder onregelmatigheden. Als het gaat om een technische storing dan zal deze worden gerapporteerd tijdens fase één en een monteur wordt aangestuurd om zo snel mogelijk naar de locatie van de storing te gaan. In fase twee inventariseert de monteur ter plekke het probleem, bepaalt hij de exacte oorzaak en locatie van de storing en verhelpt hij dit probleem.

Door het intensieve gebruik van het spoornetwerk in Nederland kan zelfs een kleine verstoring een grote aantal treinen, en daarmee passagiers en vracht, hinderen. ProRail moet, om haar taken zorgvuldig uit te voeren, manoeuvreren tussen verschillende stakeholders en belangen van de klanten (vervoerders, regionale en lokale overheden) binnen de grenzen van wet en regelgeving. Dit alles in een politieke en media arena. ProRail is alleen de operationeel beheerder, ontwerper en managementorganisatie. Voor onderhoud en



herstelwerkzaamheden is ProRail afhankelijk van vier grote procescontractaannemers (PCA). Het onderhoud en herstel zijn door de PCA en ProRail, opgedeeld in verschillende disciplines; energievoorziening (EV), seinwezen (SW), kunstwerken (KW), baan en ICT. De disciplines hebben allemaal hun eigen gespecialiseerde monteurs. Binnen deze complexe omgeving is de afdeling Asset Management (AM) van ProRail constant op zoek naar manieren om de beschikbaarheid te verhogen en prestatie van het Nederlandse spoorwegennetwerk te verbeteren.



Figuur 8: Badkuipmodel storingsherstel.

## Probleemstelling

In dit onderzoek wordt gekeken naar de mogelijkheden voor een effectiever storingsherstel door, op basis van generieke storingsmeldingen uit het procesleiding (PRL) rijwegen systeem, de oorzaak en locatie van een storing te bepalen. Hiermee wordt getracht fase 1 en 2 van het badkuipmodel positioneel te beïnvloeden. Daarbij wordt onderzocht hoe aanvullende informatie kan bijdragen aan een eerdere en identificatie op afstand, van de oorzaak en bepaling van het probleem. Spoor infrastructuur elementen kunnen verspreid zijn over een groot gebied. Wanneer een monteur meteen naar de juiste oorzaak of locatie kan worden gestuurd, zonder deze zelf te identificeren, kan dat het herstelproces versnellen. Een intern onderzoek van ProRail, naar aanleiding van twee storingen met hoge impact, heeft aangestipt dat het effectiever gebruik van beschikbare informatie mogelijk kan bijdragen aan spoediger storingsherstel. Praktisch gezien wil AM van ProRail weten hoe het de PCA beter kan informeren over een storing zodat de juiste (discipline) monteur direct naar de juiste locatie van de storing kan worden gestuurd door gebruik te maken van randverschijnselen, die zichtbaar zijn in andere operationele informatie bronnen.

## Doelstelling

Als basis voor dit onderzoek dient de volgende, vanuit de probleemstelling geformuleerde, onderzoeksdoelstelling:

*Effectiever storingsherstel door uitgebreider en beter gebruik te maken van operationele informatie door Asset Management.*

## Vraagstelling

Om de doelstelling te behalen moet onderzocht worden hoe informatiegebruik kan bijdragen aan een betere en snellere identificatie van de aard, oorzaak en locatie van een storing aan infrastructuur elementen. Zodanig dat het informatiegebruik er voor zorgt dat een monteur beter voorbereid is, waardoor de storing sneller gevonden en hersteld kan worden. Daarom is de volgende onderzoeksvraag opgesteld:

*Hoe kan het gebruik van meer en betere informatie bijdragen aan de identificatie en isolatie van de aard, oorzaak en locatie van een storing aan een infrastructuur element op basis van een PRL foutmelding om daarmee een reductie in uitval en een hogere beschikbaarheid te bereiken?*

## Praktische en Theoretische Achtergronden

Het uitgevoerde onderzoek is van exploratieve aard. Resultaten zijn vooraf niet bekend en het onderzoek is opgezet om de mogelijkheden van uitgebreider en beter gebruik van informatie op een systematische manier te onderzoeken. Met exploratief onderzoek worden op systematische wijze gegevens verzameld en kunnen mogelijke relaties en onderliggende structuren in kaart worden gebracht. In dit onderzoek is sprake van kwalitatieve dataverzameling en dataverzameling middels een praktijktest. Daarbij wordt het huidige storingsmanagement proces onderzocht en een bruikbare methode voor het onderzoek geselecteerd.

## Storingsmanagement

Een (technische) storingsmelding wordt gegenereerd door PRL. Het PRL systeem is het besturings-, monitorings- en rijwegen instel- systeem van de treindienstleider. Verschillende bronnen worden hierin gecombineerd om de treindienstleider te faciliteren in de beheersing van zijn/haar toegewezen controlegebied. Het PRL systeem geeft ook storingsmeldingen vanuit de onderliggende interlocking/veiligheidssystemen (DOSS/B-Relay/VPI/PLC), besturingssystemen (EBP/KEVCE/KBV) en monitoringssysteem (TROTS) door. De treindienstleider ontvangt deze meldingen op zijn/haar werkplek. De treindienstleider is onderdeel van de verkeersleiding (VL) en is verantwoordelijk voor de veiligheid van het treinverkeer in zijn/haar controlegebied en heeft daarbij ook direct (telefonisch) contact met de machinisten van de verschillende treinen. Een storingsmelding kan direct binnen komen via het PRL systeem of via een machinist bij een treindienstleider, of door een melding van een derde partij (hulpdiensten, omstanders of PCA) bij de meldkamer spoor (MKS). De MKS is de generieke naam voor de storingsafhandelingsorganisatie van de AM afdeling van ProRail en bevindt zich in het operationeel controle centrum rail (OCCR). In de MKS zitten de regisseurs, back office medewerkers en de bedieningsdeskundigen van het Operationeel Besturingscentrum Infra (OBI). Het OBI is verantwoordelijk voor de intake en het doorzetten van 40.000

(asset) storings per jaar vanuit de verschillende bronnen naar de verschillende verantwoordelijke aannemers. De storings vanuit PRL of storings die via machinisten zijn doorgegeven aan de treindienstleider of die door derden zijn gemeld aan de MKS, worden omgezet in een rapport van onregelmatigheid (RVO). Het RVO bevat de naam en code van het storende element, de generieke locatie, een beschrijving van de storing en krijgt een prioriteit toegekend. Het RVO geeft storende elementen weer, maar het geeft niet direct aan welk component stoort. Een voorbeeld, de volgende mededeling komt binnen bij de OBI operator: *‘Lunetten overweg 36.5 gestoord en de sectie tussen wissels 1117 en 1115A meldt onterecht bezet’*. Dan luidt het RVO als volgt: *‘Ln : Wl-1117/1115A t.o.b.s., ovw 36.5 gestoord’*. Welk component de onterechte bezetting veroorzaakt is op voorhand niet bekend en zal door de monteur moeten worden onderzocht. Het RVO wordt gecreëerd in een SAP omgeving en daarin direct door gezet naar de PCA van het betreffende contractgebied. De PCA stuurt vervolgens een monteur van een bepaalde discipline naar de storingslocatie. Zodra de monteur arriveert wordt er een veilige werkomgeving gecreëerd en kan de monteur beginnen aan de diagnose en het geven van een prognose. Na deze handelingen begint de monteur met het (tijdelijk) verhelpen van de storing. Zodra het element is gerepareerd kan de treindienst weer worden opgestart.

Bijna alle gebeurtenissen en handelingen die uitgevoerd worden door de treindienstleider of het PRL systeem worden opgeslagen. Daarbij kunnen alle lagen van het systeem voorgedefinieerde foutmeldingen genereren. Zodra een element niet werkt zoals het hoort, of het systeem zelf niet goed werkt, geeft het PRL systeem daar een melding van. Het trein observatie en tracking systeem (TROTS) wordt gebruikt om de treinbewegingen te monitoren. Dit gebeurt op basis van een treinnummer volgsysteem (TNV) en status updates van verschillende spoorelementen uit de verschillende controlesystemen. Alle TROTS gebeurtenissen worden ook opgeslagen.

De treindienstleider heeft op zijn/haar werkplek door alle systemen altijd een actueel totaal beeld van wat er gaande is in zijn/haar gebied. Een nadeel is dat het een actueel beeld is en dat daardoor alleen de actuele situatie zichtbaar is. Hierdoor kunnen korte meldingen voorafgaand aan een storing niet achterhaald worden door de treindienstleider. Deze historische en korte meldingen worden wel opgeslagen in log files maar worden pas op een later tijdstip door de ICT afdeling vrijgegeven. Niet alle, voor de treindienstleider zichtbare consequenties, worden opgeslagen. Dit komt doordat het gaat om indirecte effecten die geen eigen storingsmelding of status update hebben. Een niet meer te bedienen wissel is een normaal effect van een rijweg die is ingesteld over de wissel. Het kan echter ook het effect zijn van een storing.





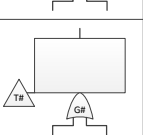


## Methodologie

Zoals eerder vermeld is het doel van dit onderzoek bruikbare informatie te achterhalen voor het beter identificeren en isoleren van een technische storing op basis van PRL foutmeldingen. Om dit doel te behalen moet achterhaald worden wat nuttige informatie is.

Kwalitatief exploratief onderzoek kan worden uitgevoerd door middel van verschillende methoden. Eén van deze methoden is een foutenboom analyse [*fault tree analysis*] (FTA). De FTA is een systematische analysetechniek om de beginoorzaak van een specifieke ongewenste gebeurtenis te achterhalen. Een FTA kan worden gebruikt om complexe dynamische systemen te evalueren, begrijpen en mogelijke problemen te voorkomen. Met behulp van een nauwgezette en gestructureerde FTA kan een foutenboom [*fault tree*] (FT) worden geconstrueerd. Een FT is een logische en grafische weergave van een combinatie van mogelijke gebeurtenissen of storings die kunnen leiden tot een ongewenste gebeurtenis of systeemstatus. De FT laat het logische fouten pad zien van alle mogelijke oorzaken (onderin de boom) naar één enkele ongewenste gebeurtenis (bovenin de boom). Een FT bestaat uit knooppunten die onderling met elkaar zijn verbonden in een boomachtige structuur. De knooppunten vertegenwoordigen fouten of storings die onderling zijn verbonden door Boolean logica symbolen. De in dit onderzoek gebruikte FT operatoren zijn weergegeven en uitgelegd in Figuur 9.

De FTA is gekozen omdat het een relatief simpele en eenvoudig te begrijpen top-down methode is. Deze top-down aanpak is nodig omdat het beginpunt een ongewenste gebeurtenis (storingsmelding) is en niet een component storing. Daarom past een top-down methode als de FTA beter dan een bottom-up benadering zoals een *Failure Mode Effect & Criticality Analysis* (FMECA). Ook wordt er bij FTA enkel gekeken naar de situatie waarin de storingsmelding zich al heeft voorgedaan. In een situatie waarin storings voorspeld moeten worden, zou een complexere methode als *Baysian belief nets* (BBN) beter passen. Het gaat om kwalitatief onderzoek waarbij kansen niet gekwantificeerd worden en er alleen gekeken wordt naar logische afhankelijkheden, past de FTA beter dan de BBN. Een BBN is namelijk een te zware en complexe methode. Daarbij is de FTA een bekende en bewezen methode die wordt gebruikt bij soortgelijke toepassingen in diverse andere industrieën (luchtvaart en chemische fabrieken).



Symbol	Type	Description
	Node Text Box	Contains the text for all FT nodes. Text goes in the box, and the node symbol goes below the box.
	Primary Failure Code: X#	A basic component failure; the primary inherent, failure mode of a component. A random failure event.
	OR Gate Code: G#	The output occurs only if at least one of the inputs occurs.
	AND Gate Code: G#	The output occurs only if all of the inputs occur together.
	Transfer Out Code: T#	Indicates where a branch or sub-tree is transferred to the same usage elsewhere in the tree.
	Transfer In Code: T#	Indicates where a branch of sub-tree is inserted from another usage elsewhere in the tree.
	Secondary Failure Code: Z#	An externally induced failure or a failure mode that could be developed in more detail if desired.

Figuur 9: Foutenboom Boolean logica operatoren.

Wanneer het systeem, elementen en componenten, die een storingsmelding kunnen activeren, zijn geïdentificeerd, is er meer informatie nodig over het falen van de individuele onderdelen daarvan. De vraag “Wat gebeurt er als een bepaald component stoort?” moet worden beantwoord om mogelijke randverschijnselen te kunnen identificeren. Daarvoor heeft ProRail al diverse FMECA's opgesteld. In de FMECA's zijn de effecten van een storing van een component beschreven. Deze effecten kunnen worden gezien als randverschijnselen bij de hoofdstoringsmelding die wordt geanalyseerd.

Deze informatie moet omgezet worden om te kunnen gebruiken bij het identificeren van de oorzaak als een storingsmelding zich voordoet. Hiervoor kan een stroomschema worden gevolgd op basis van de randverschijnselen. Een veel gebruikte methode hiervoor is een gebeurtenissenboom analyse [*event tree analysis*](ETA). De ETA is een analyse techniek voor de identificatie en evaluatie van een opeenvolging van gebeurtenissen die kunnen leiden tot een ongevalscenario naar aanleiding van een bepaalde ongewenste gebeurtenis. Door het uitvoeren van een ETA kan een visuele logische boomstructuur worden geconstrueerd, de gebeurtenissenboom [*event tree*](ET). De ET maakt het mogelijk om te bepalen of een initiërende gebeurtenis zal uitmonden in een bepaald scenario. Door het beantwoor-

den van verschillende binaire vragen (ja/nee, succes/falen) resulteert de ET in verschillende takken welke allemaal mogelijke en verschillende resultaten vertegenwoordigen

Foutenbomen stromen van de oorzaak richting de resulterende ongewenste gebeurtenis, in tegenstelling tot gebeurtenissenbomen die omgekeerd stromen. De gebeurtenissenboom start bij één enkel ongewenste gebeurtenis en komt zodoende uit bij een mogelijk gevolg. Bepaalde combinaties van omstandigheden leiden tot bepaalde gevolgen. ETs beginnen bij de initiërende gebeurtenis gevolgd door verschillende vragen die leiden tot een mogelijk gevolg. Als een vraag wordt beantwoord met ‘ja/succes’ dan wordt de bovenste tak gekozen en als het antwoord ‘nee/falen’ is, wordt de onderste tak gekozen. Als alle relevante vragen voor een tak zijn beantwoord resulteert dit in een mogelijke uitkomst. De combinatie van drie methoden, de FT aan de linkerkant en de ET aan de rechterkant waarbij de FMECA's zijn omgevormd tot cruciale vragen in de ET, is theoretisch erg geschikt om een storingsmelding te analyseren.

## ‘Stroomvoorziening Gestoord’

Om te valideren of de voorgestelde methodologie ook in de praktijk werkt, is deze getest voor een bepaalde storingsmelding. Voor sommige storingen is het direct duidelijk welke discipline monteur, wat en waar moet repareren. Bij andere storingsmeldingen is dit minder duidelijk omdat deze discipline overstijgend is of omdat de oorzaak op verschillende locaties in een groot gebied kan zitten. Zoals eerder al besproken, bij een generieke storingsmelding kan extra informatie bijdragen aan het storingsherstel proces door de juiste monteur direct naar de juiste locatie te sturen.

Een voorbeeld van een generieke onduidelijke storingsmelding is de ‘stroomvoorziening gestoord’ melding. Deze melding wordt gegenereerd als de Treinbeheersings- en Treinbeveiligingsinstallatie (TBB) voeding is verstoord. Deze melding lag ten grondslag aan de storingen waaruit dit onderzoek is voortgekomen. De melding ‘stroomvoorziening gestoord’ wordt ongeveer 2.000 keer per jaar gegenereerd en resulteert in 35 treinaantastende onregelmatigheden (TAO). Vorige jaar werden hierdoor 1.318 treinen gehinderd of opgeheven, wat leidde tot 54.000 trein vertragsminuten. Van de 35 TAO's afgelopen jaar zijn twee verstoringen aangemerkt als storingen met bijzonder grote klanthinder (categorie 1) en zijn daarom verder onderzocht door ProRail. Uit deze onderzoeken bleek dat de impact mogelijk beperkt had kunnen worden als bepaalde informatie sneller en beter geanalyseerd was. Dit had voor één van deze gevallen tot een verkorting van de storing van wel 1 uur en 45 minuten kunnen leiden waardoor de klanthinder substantieel verminderd had kunnen worden. Gezien de genoemde indicaties en de onduidelijkheid van de ‘stroomvoorziening gestoord’ melding is deze melding gekozen om te analyseren met de voorgestelde methode.

## Achtergrond Storingsmelding

De ‘stroomvoorziening gestoord’ melding wordt gegenereerd door het systeem dat alle niet-tractie voeding monitort en wordt weergegeven op de werkplek van de treindienstleider. De niet-tractie voeding wordt bijvoorbeeld gebruikt voor: trein detectie, trein beveiliging, rijweg instelling, wisselsturingen en communicatiesystemen. De melding wordt gegenereerd op het moment dat er een kleine dip, korte of langere onderbreking van de stroomvoorziening is. De verschillende controle eenheden zijn in serie geschakeld. Wanneer er één (of meerdere) element(en) geen voeding ontvangt of faalt, wordt er een (dezelfde) melding getoond. Zodra de voeding terugkeert, verdwijnt de melding automatisch. Deze melding is geïntroduceerd voor twee redenen: veiligheid en betrouwbaarheid.

De eerste reden is het veiligheidsaspect. Door het gekozen systeem van relais-beveiliging (interlocking) bestaat er een theoretische kans dat wanneer de stroomvoorziening een dip ondervindt, of kort wordt onderbroken, het systeem dit opvat als een gepasseerde trein. In dat geval wordt de rijweg achter deze zogenaamde trein afgereden en vrijgegeven voor nieuwe rijwegen. Hierdoor kunnen twee treinen op hetzelfde spoor terecht komen, wat potentieel kan resulteren in een ongeluk. Door de ‘stroomvoorziening gestoord’ melding wordt de treindienstleider geattendeerd op een storing in de stroomvoorziening van de treindetectie. Daarnaast voorkomt het systeem een ongeluk door extra veiligheidsmaatregelen te treffen. Als de treindetectie voeding een onderbreking ondervindt dan wordt een mechanisme geactiveerd dat ervoor zorgt dat alle wissels geblokkeerd worden voor bediening en alle seinen van het gebied in de stand ‘stop’ laat komen. Hierdoor kunnen geen nieuwe rijwegen naar andere sporen worden geleid, met als gevolg dat alle treinen in de omgeving zo snel mogelijk tot stilstand komen om een mogelijk ongeluk te voorkomen. Wanneer de stroomvoorziening is hersteld moet de treindienstleider het controlegebied controleren en een fysieke actie ondernemen om deze blokkade op te heffen. Deze veiligheidscheck voorkomt mogelijke onveilige situaties. Het onderhoud en reparatie van deze componenten is ondergebracht bij SW monteurs omdat ze impact hebben op de veiligheid van het systeem.

De tweede reden voor de introductie van deze melding is dat sommige componenten een hoger niveau van betrouwbaarheid van stroomvoorziening nodig hebben. Deze componenten zijn daarom uitgerust met een back-up voeding of batterij, zodat in het geval van een complete voedingsstoring deze nog steeds gebruikt kunnen worden. Wanneer de normale voeding van deze elementen is onderbroken, wordt ook de ‘stroomvoorziening gestoord’ melding gegenereerd en schakelen deze elementen over op de noodvoeding. De batterijen kunnen deze systemen over het algemeen nog drie uur van voeding voorzien voordat ze uitvallen. In die gevallen moet er ook een monteur worden gestuurd om het probleem op te lossen of om een andere noodstroom bron

te installeren. Het gaat hier om werkelijke voeding zonder directe impact op de treinbeveiliging. Voor het onderhoud en herstel van deze componenten zijn de monteurs van EV verantwoordelijk.

Door keuzes in het design van deze storingsmelding kan het zo zijn dat er wel degelijk voeding wordt geleverd vanaf het elektriciteitsnet maar dat een component faalt waardoor de storingsmelding wordt geactiveerd. Als een component faalt is het onduidelijk welke component dat is. Dit komt doordat één en dezelfde melding wordt gegenereerd voor een groter gebied. Deze configuraties voor de ‘stroomvoorziening gestoord’ melding zijn gekozen omdat het vroeger te duur was om dit voor alle componenten individueel te monitoren. Door deze keuze is de waarde van deze foutmelding, wat betreft oorzaak en discipline, afgenomen.

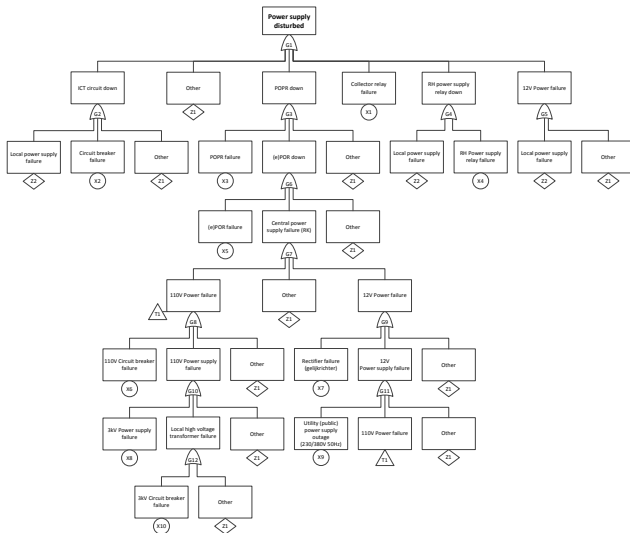
## Test Resultaten

Binnen de scope van dit onderzoek is een FT (Figuur 10) opgesteld voor de ‘stroomvoorziening gestoord’ melding. De FT is opgesteld voor meldingen die een substantiële tijd duren en waarbij een component van het meldingssysteem faalt maar waarbij er nog wel voeding wordt geleverd vanaf het elektriciteitsnet. Gebaseerd op de FT en de bijbehorende FMECA's zijn de effecten van individueel falende componenten onderzocht en geïntroduceerd als randverschijnselen van de ‘stroomvoorziening gestoord’ melding. De randverschijnselen van de verschillende falende componenten verschillen voldoende, er is dus voldoende grond voor het opstellen van een ET (Figuur 11). Door antwoord te geven op de geselecteerde vragen is het mogelijk om de verantwoordelijke discipline monteurs te bepalen en voor sommige gevallen de oorzaak te bepalen. Het belangrijkste resultaat is dat als er *geen* treinhinder wordt ondervonden, de storing kan worden verholpen door een *EV* monteur en wanneer er *wel* treinhinder is dit door een *SW* monteur kan worden verholpen. Een uitzondering daarop is als er werkelijk geen voeding meer geleverd wordt door de leverancier. Als er een SW-component faalt zullen er randverschijnselen optreden die kunnen bijdragen aan de identificatie en isolatie van het specifieke element dat dat verstoort. Voorbeelden hiervan zijn: een ten onrechte bezet spoor melding, afgevalen seinen, geblokkeerde wissels, wissels niet in controle kunnen bijdragen aan het vinden van de oorzaak. Voor het uiteindelijk bepalen van de oorzaak zijn aanvullende tekeningen en systeemkennis nodig om deze te interpreteren en de specifieke locatie en oorzaak aan te wijzen.



## Conclusie

Voor tenminste één storingsmelding is aangetoond dat de oorzaak sneller kan worden geïdentificeerd en dat de PCA beter geïnformeerd kan worden zodat de juiste monteur naar de juiste locatie wordt gestuurd. Hierdoor kan er mogelijk een reductie in storingsduur worden behaald. Door het analyseren van een storingsmelding in retrospectief en door gebruik te maken van een systeemaanpak in plaats van een componentaanpak, kan een storingsmelding effectiever worden geanalyseerd. Met behulp van een FT kan inzichtelijk worden gemaakt welke componenten aan elkaar gelinkt zijn en, als deze falen, een bepaalde storingsmelding activeren. Als daarna de individuele componenten worden geanalyseerd op andere effecten bij een component storing, kunnen randverschijnselen van de initiële storingsmeldingen zichtbaar worden. Door het herformuleren van de randverschijnselen naar binaire vragen en te combineren met de FT kan een ET worden gemaakt. Wanneer deze ET wordt gevolgd, kan de juiste monteur worden toegewezen. Voor speciale gevallen van de testcase is het ook mogelijk de specifieke oorzaak en daardoor de locatie van een storing te bepalen. Door het beantwoorden van de voorgestelde vragen kan extra (relevante) informatie worden toegevoegd aan het RVO. Om dit te bereiken dienen de treindienstleider en de OBI-medewerker duidelijk en helder te communiceren en moeten alle vragen altijd worden beantwoord. Hierbij is het van belang dat de juiste benaming van alle elementen wordt doorgegeven. Alleen dan is het mogelijk voor de PCA of ProRail om doortastend te handelen waardoor de informatie waarde kan toevoegen. Als de PCA een specifiekere RVO ontvangt kan deze effectiever reageren op een storing door direct de juiste monteur naar de juiste locatie te sturen.



Figuur 10: Foutenboom ‘stroomvoorziening gestoord’ melding.

[illegible]

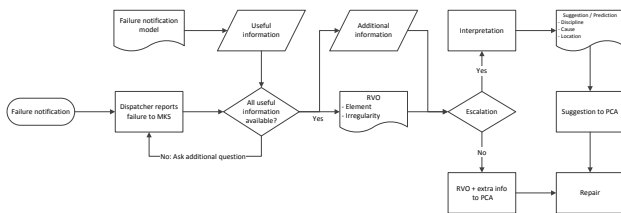
Figuur 11: Gebeurtenissenboom ‘stroomvoorziening gestoord’ melding.

## Discussie

Door het gebrek aan een deskundig oordeel, goede kwaliteit historische data of een test omgeving was het niet mogelijk de methode statistisch te bewijzen. Enkel voor de twee eerder genoemde en onderzochte gevallen was het mogelijk de methode volledig te doorlopen. Daaruit is gebleken dat wanneer de methode wordt gebruikt, er een substantiële verbetering in het storingsmanagement kon worden bereikt en mogelijke een reductie in storingsduur tot wel 1 uur en 45 minuten.

## Aanbevelingen

Voordat de methode kan worden uitgerold en geïmplementeerd, zal deze verder moeten worden geëvalueerd met de PCA om te bepalen of en hoe de PCA deze wil gebruiken. Om de methode te implementeren wordt het proces aanbevolen zoals deze te zien is in Figuur 12. Om de methode verder uit te breiden kan er verder onderzoek worden verricht naar andere discipline overstijgende storingsmeldingen of storingen die lastig te bepalen zijn, zoals ten onrechte bezet spoor-meldingen of de ‘meerdere overwegen in storting’-melding. Na het uitbreiden van de methode naar andere storingsmeldingen moet de aanpak gecontroleerd worden voor elke locatie van het Nederlandse spoornetwerk om te garanderen dat de aanpak daar ook werkt.



Figuur 12: Proces implementatie.

De implementatie moet vervolgens geborgd worden op alle niveaus van de storingsorganisatie van ProRail en de werking moet gecontroleerd worden wanneer alle benodigde informatie beschikbaar is. Daarvoor moet de kwaliteit van de historische data worden verbeterd. Daarnaast kan ook een verdere fysieke scheiding van de ‘stroomvoorziening gestoord’ melding worden onderzocht. Ook kan een andere aanpak van de storingsafhandeling worden onderzocht, bijvoorbeeld door middel van voorgedefinieerde vragen in een slim intake systeem.





BUITER **BETON** railinfra & ZEUS BETON BV  
Artikel: Betonpaal deergeslotenreus  
Prod. datum: 15-10-2012  
Gewicht: 225 KG  
Opmerking: 001







# Contents

<b>Acknowledgements</b>	<b>vii</b>
<b>Executive Summary</b>	<b>ix</b>
<b>Management Samenvatting</b>	<b>xv</b>
<b>List of Acronyms</b>	<b>xxvii</b>
<b>List of Terms</b>	<b>xxxix</b>
<b>1 Project Introduction</b>	<b>1</b>
1.1 General Introduction . . . . .	1
1.1.1 The Dutch Rail Network . . . . .	1
1.1.2 Company Description . . . . .	2
1.2 Problem Introduction . . . . .	3
1.2.1 Multi-Actor Environment . . . . .	6
1.2.2 Disruption Process . . . . .	7
1.2.3 Repair Process . . . . .	7
1.2.4 Data Availability . . . . .	7
1.2.5 Problem Description . . . . .	8
1.3 Research Objective . . . . .	9
1.4 Scope . . . . .	9
1.5 Research Question and Approach . . . . .	9
1.6 Relevance . . . . .	10
1.6.1 Scientific Contribution . . . . .	10
1.6.2 Practical Contribution . . . . .	10
1.7 Report Structure . . . . .	11
<b>2 State of the Art</b>	<b>13</b>
2.1 Research Methodology . . . . .	13
2.1.1 Fault Tree Analysis (FTA) . . . . .	13
2.1.2 Event Tree Analysis (ETA) . . . . .	15
2.1.3 Fault Tree (FT)-Event Tree (ET) Combination . . . . .	17
2.1.4 Case Study . . . . .	18
2.1.5 Fault Tree (FT)-Event Tree (ET) Evaluation and Validation . . . . .	18
2.1.6 Methodology Discussion . . . . .	19
2.2 Practical Background . . . . .	20
2.2.1 Failure Recovery Organisation . . . . .	20
2.3 Operational Data . . . . .	24
2.3.1 Asset Failure . . . . .	26
2.4 Conclusion . . . . .	27
<b>3 Disturbed Power Supply</b>	<b>29</b>
3.1 Power Supply System . . . . .	31
3.2 Relay Interlocking . . . . .	32
3.3 Power Monitoring . . . . .	33
3.4 System Architecture . . . . .	34
3.5 Fault Tree (FT) 'Power Supply Disturbed' Notification . . . . .	38
3.6 Event Tree (ET) 'Power Supply Disturbed' Notification . . . . .	40
3.7 Performance . . . . .	41
3.8 Conclusion . . . . .	45

<b>4</b>	<b>Discussion and Implementation</b>	<b>47</b>
4.1	Results Discussion . . . . .	47
4.2	Data Collection . . . . .	49
4.3	Process Implementation . . . . .	50
4.3.1	Usability Discussion . . . . .	51
4.4	Broader Context Discussion. . . . .	52
<b>5</b>	<b>Conclusions and Recommendations</b>	<b>55</b>
5.1	Conclusions. . . . .	55
5.1.1	Sub Questions Answers . . . . .	55
5.1.2	Answer Main Question. . . . .	57
5.2	Scientific Implications . . . . .	58
5.2.1	Scientific Contribution. . . . .	58
5.2.2	Practical Contribution . . . . .	58
5.3	Recommendations . . . . .	59
5.3.1	Recommendations For Further Research . . . . .	59
5.3.2	Recommendations For ProRail. . . . .	59
5.4	Personal Reflection . . . . .	60
	<b>References</b>	<b>62</b>
	<b>Appendices</b>	<b>67</b>
	<b>List of Figures</b>	<b>68</b>
	<b>List of Tables</b>	<b>71</b>
<b>A</b>	<b>SAP Report Content</b>	<b>72</b>
<b>B</b>	<b>ICT-O Components</b>	<b>73</b>
<b>C</b>	<b>Asset Failure Causes</b>	<b>77</b>
<b>D</b>	<b>FMECA ProRail</b>	<b>78</b>
<b>E</b>	<b>Technical Drawings Power Supply Monitoring Architecture</b>	<b>80</b>
<b>F</b>	<b>Test Case Performance Check</b>	<b>85</b>
<b>G</b>	<b>Werkwijze ProRail: Stroomvoorziening Gestoord Melding</b>	<b>87</b>







# Acronyms

AM	Asset Management	xxxi, 2, 3, 8–10, 20, 22, 53
ARI	<i>automatische rijweg instelling</i> [automatic route setting]	25
ASTRIS	<i>aansturing en statusmelding van de railinfrastructuur</i> [control and status-notifications for rail infrastructure]	32
ATB	<i>automatische treinbeïnvloeding</i> [automatic train control]	31, 33
BBN	Bayesian belief nets	19
CB	circuit breaker [ <i>zekering</i> ]	33–36
DVL	<i>decentrale verkeersleiding</i> [decentralized VL]	21
EBP	<i>elektronische bedienpost</i> [electronic control station]	25, 32, 33, 41, 47
EBS	<i>elektronische beveiliging SIMIS</i> [electronic security SicHERes Mikro-computersystem von Siemens]	25, 32, 47
ePOR	electrical power off relay	35, 45
ERTMS	European rail traffic management system	25
ET	event tree	15–19, 29, 40–42, 44, 45, 48, 56–59, 68
ETA	event tree analysis	15, 16, 18, 19, 51, 56, 71
EV	<i>energievoorziening</i> [power supplies]	7, 33, 39, 42, 45, 48, 52, 56
FMECA	failure mode effect and criticality analysis	19, 26, 39, 56, 78
FRT	failure recovery time	1, 8–10, 27
FT	fault tree	13–19, 29, 39, 42, 45, 56–59, 68



FTA	fault tree analysis	13, 14, 18, 19, 51, 56, 71
HIJSM	<i>Hollandsche ijzeren spoorweg maatschappij</i>	1
ICT-O	ICT-operations	2, 3, 7, 24, 25, 34, 73
IHC	<i>instandhoudingsconcept</i> [conservation concept]	78
ILS	<i>informatie levering specificatie</i> [information supply specification]	78
IM	infrastructure manager	1–3
IRA	<i>instandhouding risico analyse</i> [conservation risk analysis]	78
KBV	<i>koppeling beveiliging (post)21 vervoer per trein</i>	25, 32, 47
KEVCE	<i>koppeling EBS vervoer per trein</i>	25
KW	<i>kunstwerken</i> [engineering constructions]	7, 34, 56
LCE	<i>lokale controle eenheid</i> [local control unit]	32–35, 41, 47, 52
LVL	<i>landelijke verkeersleiding</i> [national VL]	21
LWB	<i>leider werkplek beveiliging</i> [chief workplace safety]	21
MKS	<i>meldkamer spoor</i> [railway control room]	xxxi, 20, 21, 52, 55, 59
NS	<i>Nederlandse spoorwegen</i> [Dutch railways]	1, 2
OBI	<i>operationeel besturingscentrum infra</i> [operational control centre infrastructure]	xxxi, 20, 21, 45, 49–52, 55, 57–59
OCCR	operational control centre rail	xxxi, 6, 8, 9, 20, 49, 52
OPC	output process contract	23
OR-scheme	overview reverse links-scheme [overzicht spoor- en wisselisolatie en retourverbindingen]	36, 45, 68
PCA	<i>procescontractaannemer</i> [contractor]	6, 9, 10, 20, 21, 23, 27, 41, 47, 48, 50, 51, 55–59, 68, 78
PGO	<i>prestatiegericht onderhoud</i> [performance-based maintenance]	23
PI	performance indicator	3, 5, 58
PLC	programmable logic controllers	32, 47

POPR	power off repeater relay	34, 35, 37, 45, 68
POR	power off relay	32, 34
POSR	power off stick relay	34
POTER	power on time element relay	37
PRL	<i>procesleiding rijwegen</i> [route processing systems]	9, 25, 27, 33
RH	<i>relais huis</i> [relay house, or sub-station]	34–36, 42, 45
RK	<i>relais kast</i> [relay box]	35, 36, 45, 68
RVO	<i>rapport van onregelmatigheid</i> [report of irregularity]	21–23, 27, 41, 50, 51, 55, 57, 58
SS	<i>maatschappij tot exploitatie van staatsspoorwegen</i>	1
SW	<i>seinwezen</i> [signalling]	7, 34, 37, 45, 47, 48, 52, 56
TAO	<i>treindienst aantastende onregelmatigheid</i> [train depleting irregularity]	3, 5
TBB	<i>treinbeheersings- en treinbeveiligingsinstallaties</i> [route control and train protection]	29, 31, 33
TEV	<i>tractie-energievoorziening</i> [traction power supply]	31
TIS	<i>trein incident scenario</i> [train incident scenario]	22, 34
TNV	<i>treinnummer volgsysteem</i> [trainnumber follow-up system]	25
T.O.B.S.	<i>ten onrechte bezet spoor</i> [improperly occupied track]	25, 45, 51, 57, 59
TOCs	train operating companys	1, 2, 6, 10, 58
Trdl	<i>treindienstleider</i> [dispatcher]	20, 21
TROTS	train observation and tracking system	7, 25, 27, 49, 56
UPS	uninterruptible power supply	31, 33
VL	<i>verkeersleiding</i> [traffic control]	20, 25
VPI	vital processor interlocking control system	25, 32, 47





# Special Terms

Central power supply	The electrical energy is taken from the grid at two separate power points and delivered to several (groups of) users in multiple locations. Mostly used for track side power supply.	31
Local power supply	The electrical energy is taken from the grid in one feeding point and delivered to a single (group of) user (s) at a single location. Mostly used for powering all element on shunting yards and station areas and the control structure.	31
MKS	The <i>meldkamer spoor</i> [railway control room] (MKS) is a generic name for the failure-handling organisation of ProRail's AM within the OCCR. By which, the directors, call centre operators and the <i>operationeel besturingscentrum infra</i> [operational control centre infrastructure] (OBI) are covered, also known as the back office.	20
OBI	The <i>operationeel besturingscentrum infra</i> [Operational control centre infrastructure] (OBI) is responsible for the intake and forwarding of 40,000 (asset) failures originating from several different channels to the different responsible PCAs. Additionally, the OBI performs around 9,000 'switching commands' to interrupt the catenary section and 6,000 commands to switch of the local and central power supply, by which the contractors can safely perform maintenance and repairs to the different systems.	20
Post21	Virtual landscape in which all the IT-systems are connected to each other. From the workplace of the dispatcher to the infrastructural elements outside.	7, 24, 73
PRL	The <i>procesleiding rijwegen</i> [route-processing system] (PRL) includes planned activities and route conditions by service control point, material relationships, delays, and the like. In addition, the dispatcher can adapt the process plan. A routing function supports traffic control in situations where the dispatcher for some period for one or more trains wishes to adapt the routing by its operating area. Routing changes are automatically reflected in the plan rules on trains.	25
TIS	A TIS is a standard scenario corresponding with certain characteristics of an incident. It consist of 5 scenarios (1-5) and 4 indicators of severity (1-4). Example "TIS 1: Train service disruption TIS 1.4: Total blockage. Train service no longer executable" or "TIS 3: Collision / impact and derailment with casualties TIS 3.3: Derailment with victims or collision with train/shunting equipment/large road vehicle (with victims or victims unknown) car set not deformed, stacked or tilted and catenary group has not failed"	22, 47













# Project Introduction

failure recovery time (FRT) is the time between the arrival of a mechanic at the rail track and the moment the mechanic leaves the site after the repair action. The reduction of (major) disruptions and their impact is a continuous objective for ProRail, the Dutch rail infrastructure manager (IM). To reduce hindrance for train operating companies (TOCs) and their customers, the FRT needs to be as short as possible. ProRail wants to explore the possibilities of using additional information to reduce FRT. This research explores those possibilities.

Chapter 1 introduces the research: Section 1.1 presents a general introduction to the rail network in the Netherlands and ProRail as a Rail IM. Section 1.2 defines the problem regarding failure recovery time. The problem definition results in drafting the research objective characterised in Section 1.3. The scope of the research is presented in Section 1.4, while Section 1.5 articulates the main research question, along with the sub-questions and the research approach. The relevance of the research, both scientific and practical, is described in Section 1.6. Finally, Section 1.7 outlines the structure of this report.

## 1.1. General Introduction

This section gives an insight in the rail network of the Netherlands. First, a broad outline of the entire sector is presented in Section 1.1.1, and Section 1.1.2 describes ProRail as a company.

### 1.1.1. The Dutch Rail Network

The first private railway company founded in the Netherlands appeared on August 8, 1837, The *Hollandsche ijzeren spoorweg maatschappij* (HIJSM). The founders started to build the first railway route between Amsterdam and Haarlem, which was put into operation two years later, in 1839. In 1860, only 325 kilometres of track had been constructed, so the national government decided to build a state rail network to speed up construction. Most state-owned lines were operated by the *maatschappij tot exploitatie van staatsspoorwegen* (SS), a private company founded in 1863. In 15 years, the railway network grew to cover 2,610 kilometres of track, and by the year 1900, the rail network as we know it today was almost completed. Many rail-and-tramway companies were founded, and many stations constructed. In 1938, the HIJSM and the SS merged into one state-owned company, the *Nederlandse spoorwegen* [Dutch railways] (NS).

Since 1995, major changes have taken place in the organisation of the Dutch rail system. In 1995, NS divided itself, commissioned by the government, into a commercial NS Group and three ‘task organisations’: *Railinfrabeheer* [management and maintenance], *Railned* [capacity management and railway safety], rail traffic control. Regional rail line

organisations were merged. The task organisations were commissioned and paid for by the government to construct, maintain and manage the railway tracks. In 1997, the privatisation of the maintenance division of the NS followed. Around 3,000 maintenance workers were transferred to three private sector contractors. Instead of performing the maintenance tasks, the remaining maintenance staff had, and still has, to manage the maintenance process through contracts and tendering. In 2004, the Dutch parliament approved the new Railway Act, which created ProRail as the government commissioned IM for the Dutch rail network (NS Groep N.V., 2016a). ProRail was created of a fusion of the different task organisations.

### 1.1.2. Company Description

The Dutch state owns 100% of ProRail shares. In 2015, 152 million train kilometres and 45 billion tons kilometre (ProRail, 2016i) were realised on the Dutch rail network under ProRail's supervision, resulting in 1.2 million train trips per day (2015) (NS Groep N.V., 2016b). The combination of ProRail being state owned (and largely state funded) and the great number of people travelling by train every day results in a high social relevance and responsibility. The main goal of ProRail is therefore to deliver reliable and safe railway paths for TOCs.

In its role as IM, ProRail is responsible for capacity allocation, railway maintenance, safety, extension and control of, according to 2015 numbers, 2,589 level crossings, 7,021 km of railway track, 7,071 switches, 12,036 signals and 404 stations in the Netherlands (ProRail, 2016i). ProRail takes care of one of the busiest and densest railway networks in the world, with an organisation of 3,958 employees and a budget of €2.2 billion per year (2015). The activities ProRail performs are versatile and comprehensive and can be divided into six pillars, as represented in Figure 1.1.

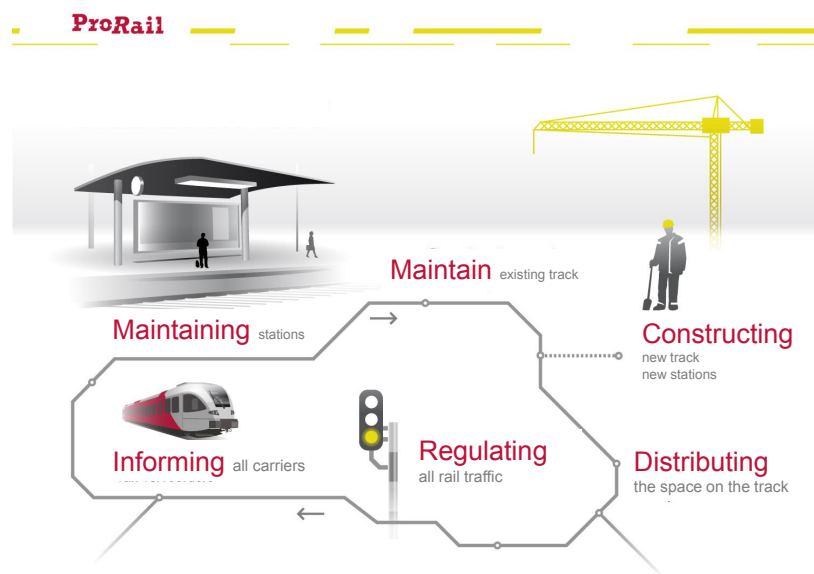


Figure 1.1: Main tasks ProRail.

These pillars are classified by three main business units: projects, operations, and *vervoer & dienstregeling* [transport and scheduling]. Projects focusses on the management and development of new (rail) infrastructure and stations, along with the renewal of old infrastructure and stations. The department of transport and scheduling provides the timetable, and so distributes the space on the track. The pillar of operations consists of traffic control, AM and ICT-operations (ICT-O). Traffic control is the decentralised train dispatcher's offices that control railway route setting and traffic flows for a designated



territory. AM is responsible for managing the maintenance of existing infrastructure and stations. This maintenance is not performed by ProRail itself but by specialised contractors. Since the introduction of computers, system interlocking is partially digitalised together with other operational systems and are managed by the ICT-O department.

## 1.2. Problem Introduction

Every day small irregularities in the timetable occur, and sometimes large ones. In unconventional operating conditions, ProRail is considered to be a key player for dealing with and settling both small disturbances and large ones. ProRail, as IM, and other stakeholders are working hard to prevent and reduce the impact of disturbances. The performance of ProRail is measured by several performance indicator (PI)s. There are several PI's, with some related to punctuality and others to the services ProRail provides, such as paths and the cancellation of trains. Another PI is the influence of irregularities on the standard train services, the so-called *treindienst aantastende onregelmatigheid* [train depleting irregularity] (TAO). Despite all efforts in recent years, and although a slight improvement was seen on some PIs, most were stable or fluctuated slightly, as can be seen in Table 1.1.

Every day there are small and sometimes large irregularities in the timetable. In unconventional operating condition ProRail is considered to be a key player for dealing and settling small disturbances or large disruptions. ProRail, as IM, and other stakeholders are working hard to prevent and reduce the impact of disturbances. The performance of ProRail is measured by several performance indicator (PI)'s. There are several PI's, some are related to punctuality and others to the services ProRail is providing such as, provided paths and cancellation of trains. Another PI is the influence of irregularities on the standard train services, i.e. the so-called *treindienst aantastende onregelmatigheid* [train depleting irregularity] (TAO). Despite all effort over the last years there was a slight improvement on some PI's but most were stable or fluctuated a bit, as can be seen in Table 1.1.

Table 1.1: Operational performance of ProRail (ProRail, 2016i).

Performance Indicator (PI)	2013	2014	2015
Punctuality passenger traffic (<3 minutes)	87.2 %	90.2 %	89.5 %
Punctuality main rail network (<5 minutes)	-	-	91.0 %
Punctuality freight traffic (<3 minutes)	79.6 %	83.0 %	80.0%
Punctuality regional rail network (<3 minutes)	92.5 %	94.9 %	95.0 %
Provided paths	97.8 %	97.9 %	97.9 %
Cancelled trains	2.4 %	1.8 %	2.1 %
<i>treindienst aantastende onregelmatigheid</i> [TAO] (#)	10,953	10,017	10,974

The Dutch railway network nevertheless performs at a high level and is one of the busiest in an international context (Ramaekers et al., 2009; Hansen et al., 2012) as can be seen in Figures 1.2 and 1.3. The Dutch rail network is almost twice as heavily used as the European average. Only Switzerland and Japan have busier rail networks and perform with greater reliability (Figure 1.4). ProRail also performs well in terms of performance versus costs, although due to different organisational setups, it is hard to compare different countries. Still, based on 'The 2015 European Railway Performance Index' from Boston Consulting Groep (2015), the Dutch railway network performed better than the average ratio of performance to cost, as can be seen in Figure 1.5.

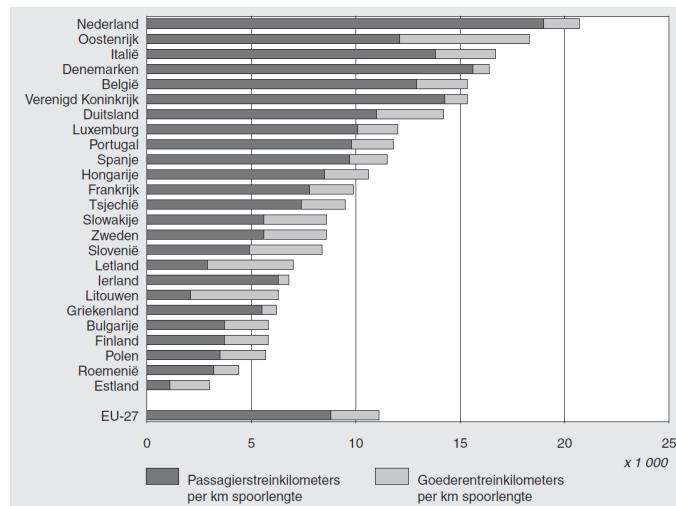


Figure 1.2: Passenger-and-freight-train kilometres per kilometre of train track in the EU (2006) (Ramaekers et al., 2009).

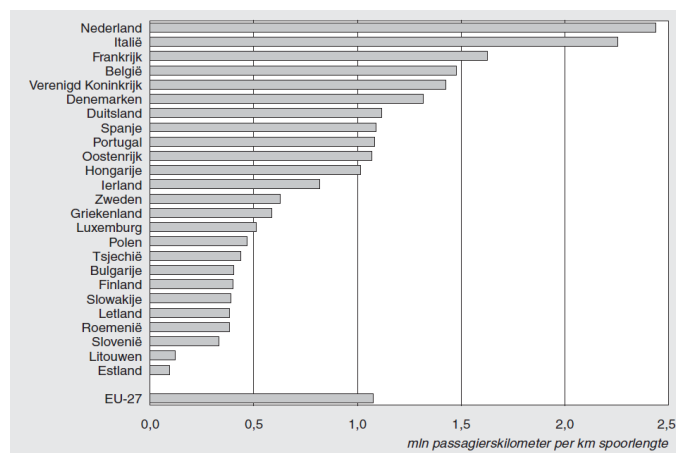


Figure 1.3: Passengers per kilometre train track in the EU (2006) (Ramaekers et al., 2009).

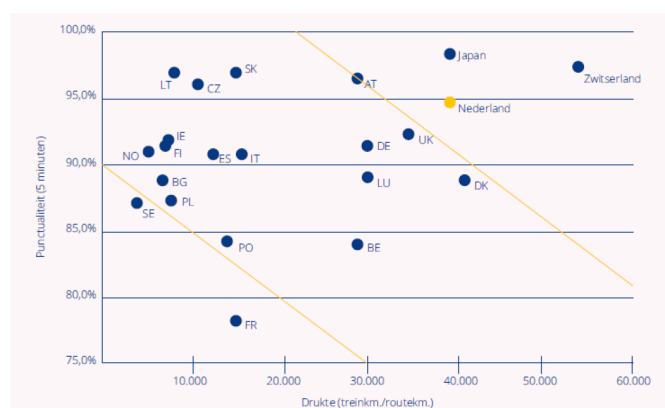


Figure 1.4: Punctuality (<5 min) versus crowdedness in different countries (NS Groep N.V., 2016b).

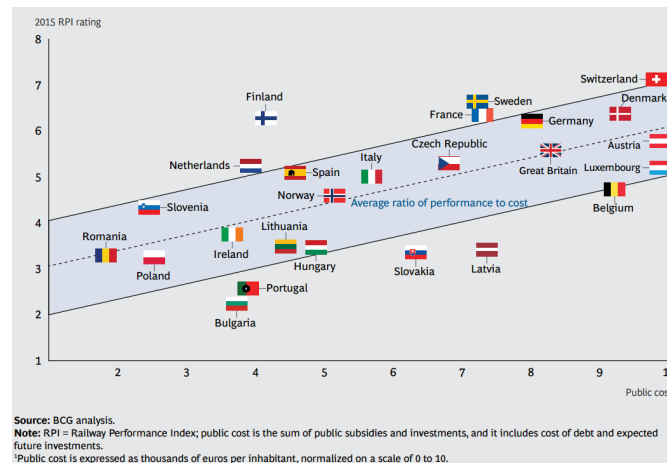


Figure 1.5: 2015 Railway performance index rating to public cost (Boston Consulting Groep, 2015).

Despite the international position of the Dutch rail network, ProRail wants to perform better on the presented PIs. Therefore a strategic objective was formulated for a reliable railway network: 'Prevent avoidable disruptions by allowing more and better preventative maintenance on the track, and an alert response to disruptions and a sharp analysis of repetitive failures' (ProRail, 2016i).

As suggested by ProRail's objective, not all disruptions can be avoided, nor can all be blamed on ProRail. In Table 1.2, the main causes for TAOs can be seen. In their objective statement, ProRail refers specifically to the TAOs caused by engineering and processes. This targeted concern acknowledges that extreme weather cannot be influenced and that third-party causes, like people walking along the tracks and like suicides, are not to be blamed on ProRail. The company can influence the impact of extreme weather only by creating more robust infrastructure or by limiting access to the tracks. Despite the fact that TAOs caused by engineering mistakes have been reduced in recent years, they still represent a major portion of total TAOs. Thus, ProRail focusses on allowing more and better preventive maintenance on the track to reduce engineering-caused TAOs.

Table 1.2: TAO causes (ProRail, 2016i).

Causes for TAO's	2013	2014	2015
Engineering	38% (4,163)	36% (3,606)	32% (3,512)
Third parties	43% (4,710)	47% (4,708)	50% (5,487)
Processes	9% (985)	10% (1,002)	9% (988)
Weather	9% (985)	6% (601)	7% (768)
Other	1% (110)	1% (100)	2% (219)
Total	100% (10,953)	100% (10,017)	100% (10,974)

In an ideal world, no TAOs result from engineering problems. Unfortunately, this ideal work is not (yet) the real world. Therefore, ProRail has decided to focus on alert response to disruptions and a sharp analysis of repeated failures.



For better cooperation between stakeholders, the operational control centre rail (OCCR) was introduced. Here all stakeholders are represented, and all are in close contact to handle disturbances. This complex multi-actor environment is elaborated in Section 1.2.1.

A problem with the railway system effects the schedules of many people and the delivery of goods. In the past, such impacts have led to political pressure, reputation damage and extra costs. Therefore, ProRail has a consistent ambition to reduce (major) disruptions and their impact on shippers and travellers (ProRail, 2015a).

### 1.2.1. Multi-Actor Environment

ProRail is the monopolist for maintaining and managing the Dutch rail network, but that position does not imply they can determine policies and actions single-handedly. Since ProRail impacts its surroundings, its business structure, and its active contracts, ProRail has to manoeuvre between different actors. Five main categories or stakeholders are recognised by ProRail, as summarised by Brinkman (2009), seen in Figure 1.6.

#### ProRail and stakeholders

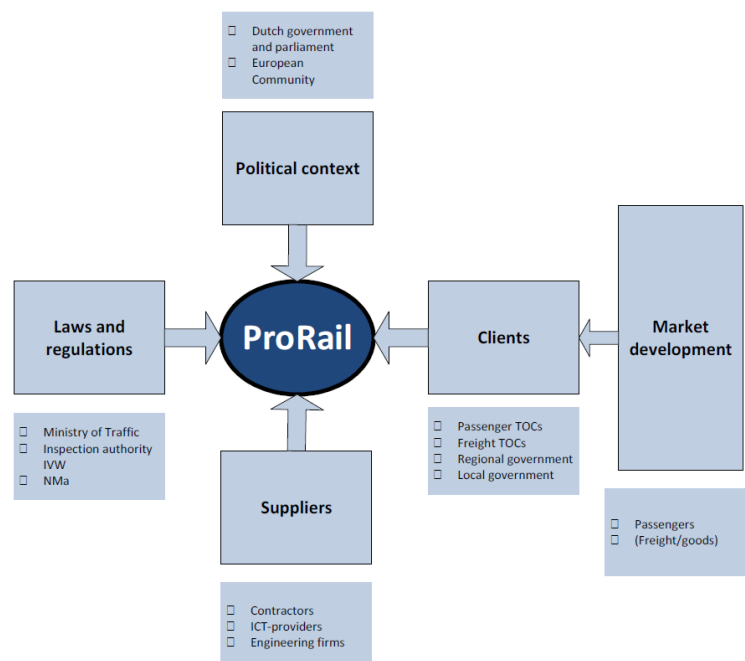


Figure 1.6: ProRail and the surrounding stakeholders (Brinkman, 2009).

ProRail has to satisfy their clients (train operating companies (TOCs), regional and local governments) within the boundaries imposed by laws and regulations, all in a political and media arena. ProRail is only the operating, designing and managing organisation, however. For maintenance, ProRail depends on four recognised track-maintenance contractors: ASSET Rail, Strukton Rail, Volker Rail and BAM Rail. The contractors are called, *procescontractaannemer* [contractor] (PCA). In this complex surrounding, the OCCR is the location to solve complex operational problems in a limited time.

ProRail created the OCCR in 2010. Since the foundation of the OCCR, it has operated 24 hours a day, 7 days a week, coordinating and settling incidents and emergencies in rail traffic. Almost all (operational) stakeholders in the Dutch rail sector (clients and suppliers in Figure 1.6) are somehow represented at the OCCR and work together to minimise disruptions and to negotiate how to solve problems.

### 1.2.2. Disruption Process

The railway-disruption processes can be described by the bathtub model (Ghaemi & Goverde, 2015), as can be seen in Figure 1.7. This bathtub model can be partitioned into three phases. In Phase 1, the traffic decreases when a disruption occurs, and the cause must be identified. In Phase 2, traffic is not possible or is possible only at a very low level, and the problem is being solved. The last phase, Phase 3, starts when the problem is solved and traffic can return to normal. The bathtub model is used to describe traffic over time. The main objective of this research is to reduce the 'length' of the bathtub. The main influences on the length of the disruption are traffic or infrastructure related. This research focusses on the infrastructure-related aspects of the disruption, and traffic aspects are not considered. Within these infrastructure-related aspects the focus is on physical problems. Physical problems are split up in two parts in this study: finding the problem and fixing the problem.

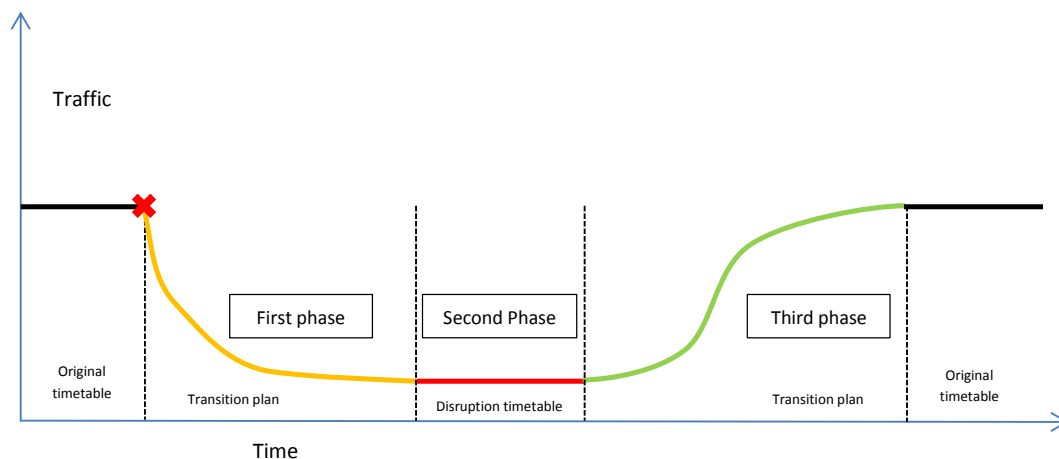


Figure 1.7: Bathtub Model by Ghaemi & Goverde (2015).

### 1.2.3. Repair Process

Finding and fixing problems is a process that has been done for years. Since the railways became more complex, though, finding and fixing problems became more complicated as well. Over the years, the railway-asset repairs were split up into several specialities: *energievoorziening* [power supplies] (EV), *seinwezen* [signalling] (SW), *kunstwerken* [engineering constructions] (KW), *baan* [track] and ICT, all with their own skilled personnel. Contractors performing maintenance and repairs on behalf of ProRail needed to educate their personnel for all possibilities of failure. As a result, those mechanics are educated and gained experience on site; they learned with the new systems. They arrive at a disturbed element with a blank sheet and use their training and experience to fix the problem.

### 1.2.4. Data Availability

Since ICT was introduced in railways, data has been logged to monitor the ICT processes, in order to find the failure in an environment where it was no longer possible to physically see the problem. Increasingly, more elements are now controlled or managed by ICT systems. Those systems generate data for monitoring those elements. All data generated by the operation of trains is called ICT-operations (ICT-O) data. Those data sets include data about, for example, Post21 (control system) and the train observation and tracking system (TROT). As mentioned, this data is already used when a system malfunctions. Aside from ICT-O data, data is also available about the history of asset failures. This data takes the form of manual log files in an SAP database where mechanics log their activities concerning failure repair.

The dispatchers can see whether elements are locked, used or disrupted at their workstation. ProRail wants to know whether all sources combined could help AM to identify and isolate failures of physical elements, to enhance the failure-recovery management process and possibly to speed up repairs.

### 1.2.5. Problem Description

This research is commissioned by the department of AM, housed within the OCCR, an independent operating unit within the department of AM at ProRail which focusses on handling disruptions. AM is interested in how the available information can contribute to a reduction in FRT.

Because of the intensive use of the rail networks in the Netherlands, even a small disruption can effect numerous trains and, consequently, passengers and freight. Furthermore, the number of train passengers and freight is expected to grow (Ministerie van Infrastructuur en Milieu, 2014). Projections for passenger growth show nationwide growth of 4%–27% in the period 2011–2020 and 3%–2% in the period 2020–2030. The recalibrated goods forecast predicts a growth of 17%–107% by 2020 and a growth of between 10%–29% for the period 2020–2030 (data 2011). Most of the growth will be clustered around the *Randstad* (a dense urbanised region in the western part of the Netherlands).

The space in the urban areas is restricted, and resources like finances and assets are limited, so ProRail is forced to make choices on how to cope with the predicted growth, along with the company's ambitions and constraints. One of the options is to use all assets more efficiently. If infrastructure is used more efficiently or intensively, failure of infrastructure also has a bigger impact. Indeed, a failure at a critical node will have a huge effect, and therefore the impact of failures must be minimised, along with when their frequency and the downtime associated with them.

Internal research (ProRail AM Infrabeschikbaarheid, 2016a) has already shown existing data could effectively be used for ProRail to reduce disruption time. The research was performed after a large disruption on February 18, 2016, near Gouda. That day, a circuit breaker [*zekering*] malfunctioned, causing a power outage. This malfunction resulted in a 'track occupied' message on all tracks across the *Gouwespoorbrug*, and it locked all switches on the control area of Gouda. As a result, no traffic was possible for 3 hours and 15 minutes; consequently, 37 trains were delayed, 1 diverted and 158 cancelled. Researchers concluded that if all operation-generated data and information available was shared with all stakeholders, disruption time could have been reduced by 1 hour and 45 minutes. This reduction included 1 hour and 15 minutes saved by identifying the problem faster and 30 minutes saved by speeding up the repairs. These findings raised the question of why this information is not shared at an earlier point in time.

ProRail (AM, OCCR) wants to know whether and how (directly) available (operational) information can help to shorten the FRT. In practical terms, ProRail wants to know whether it is possible to inform contractors better, so that a mechanic knows the right location of the failure and can anticipate what that failure could be. Because the railway infrastructure elements can be spread over a large area, it would be useful for mechanics to know the exact location of the element or its control elements, so that they can be faster on site, reducing the duration of the first and second phase represented in the bathtub model.



### 1.3. Research Objective

This study aims to understand the available information sources (real-time), system-element relations and failure locations, to develop a possible application to enhance the FRT by exchanging comprehensive failure-related information between ProRail and PCA.

Therefore, the following research objective was formulated to ground this research:

*A more effective failure recovery through a more extensive and better use of operational information by Asset Management.*

### 1.4. Scope

This research focusses on FRT from the perspective of the OCCR and AM. In order to be useful, the information needs to be available within 45 minutes (PCA response time), and the faster the better. Therefore real-time operational data sources are used. Information on how an element can fail and how a failure appears should be determined in advance. Only track-side elements are considered, which are controlled or monitored by the *procesleiding rijwegen* [route processing systems] (PRL) system or its users, based on relay interlocking. Complex structures, for example tunnels, are excluded because they involve another division and require other inside knowledge.

### 1.5. Research Question and Approach

To achieve the objective, it needs to be checked whether information usage can contribute to better and faster identification of the nature, cause and location of a problem. In this way, a technician can prepare for the problem, locate it faster and know what materials are needed to fix it. The investigation needs to show whether additional information, if at all possible, can contribute to identification, localisation and isolation of a rail-infrastructure element failure, whereby a reduction in disruption time can be achieved.

Given these demands, the main research question is as follows:

*How can the use of more and better information contribute to the identification and isolation of the nature, cause and location of a failure of an infrastructure element based on a PRL failure notification in order to achieve a reduction in downtime and a higher availability?*

The main question is broken into several sub-components. Sub-questions correspond to each sub-component:

1. How does the ProRail disruption-management process (from original timetable to first train, after repair) work, and how does it relate to the different track side elements?
  - (a) How is disruption management organised?
  - (b) What information is shared with the PCA?
  - (c) How and what assets can fail?
2. What theoretical and real-time data can be linked to a disruption or an asset failure?
3. How can the qualitative risks of a system failure be assessed?
  - (a) How can potential failure modes be identified?
  - (b) How can potential failure causes be identified?
4. How can a qualitative risk assessment be applied?

5. How can a qualitative risk assessment be implemented in the disruption process, to use its full potential?

When all sub-question are answered, it should be possible to answer the main question, determining whether ProRail and PCAs can use additional information to identify, localise and isolate an asset failure to reduce disruption time.

Where these questions are assessed is lined out in Section 1.7, and answers to all the above questions are presented and discussed in Chapter 5.

## **1.6. Relevance**

The research is commissioned by ProRail and in partial fulfilment of the requirements for the degree of Master of Science in Civil Engineering, Transport and Planning. As such, the study aims for both scientific relevance and relevance for ProRail.

In general, this research provides better insight into failure recovery time (FRT) and the processes for solving a railway disruption. It presents an overview of available operational information sources and qualitative risk assessment of failure modes, along with how a failure manifests in operation.

### **1.6.1. Scientific Contribution**

This research contributes to the scientific field in various ways. It clarifies whether and how a combination of operational information and theoretical qualitative risk assessment can enhance the identification, localisation and isolation of a railway-asset failure. It also points out how combining resources can lead to better instructions and full use of information. This study's literature review also presents an overview of the disruption process 'behind the scenes'.

During the research, no study or conceptual framework could be identified for research on operational rail information in the context of the disruption process, failure analyses or FRT. Therefore, the research will contribute to closing the knowledge gap between theoretical data analyses and railway AM. It will thus significantly contribute to the growth of the current academic literature on the subject.

### **1.6.2. Practical Contribution**

This study potentially reduces inconvenience for train operating companies (TOCs) and their passengers and goods, looking for ways to reduce disruption time.

It clarifies whether and how ProRail can enhance their information services for different contractors. It also highlights the importance of using all available resources to cope with the (potential) growth in the number of trains, passengers and freight on the Dutch rail network. The research prepares a method to identify, localise and isolate particular notifications or combinations that refer to specific situations or locations. This method can investigate such combinations to find out whether a common factor is influencing the indicators concerned. The study also tries to engage mechanics and other employees to reflect on and possibly rethink their ways of doing business. Finally, this research can help to reveal new growth opportunities and cost reductions through efficiency gains.

## 1.7. Report Structure

Figure 1.8 gives the structure of the main report with its chapters, content and relations. Chapter 2 states the used methods used to answer the research questions and gives a background of the failure recovery system and related information. In Chapter 3, this method is applied to a test case. Possible generalisation of the test case and method are presented in Chapter 4. Finally, the study's conclusions are stated and discussed in Chapter 5, together with recommendations and personal reflection.

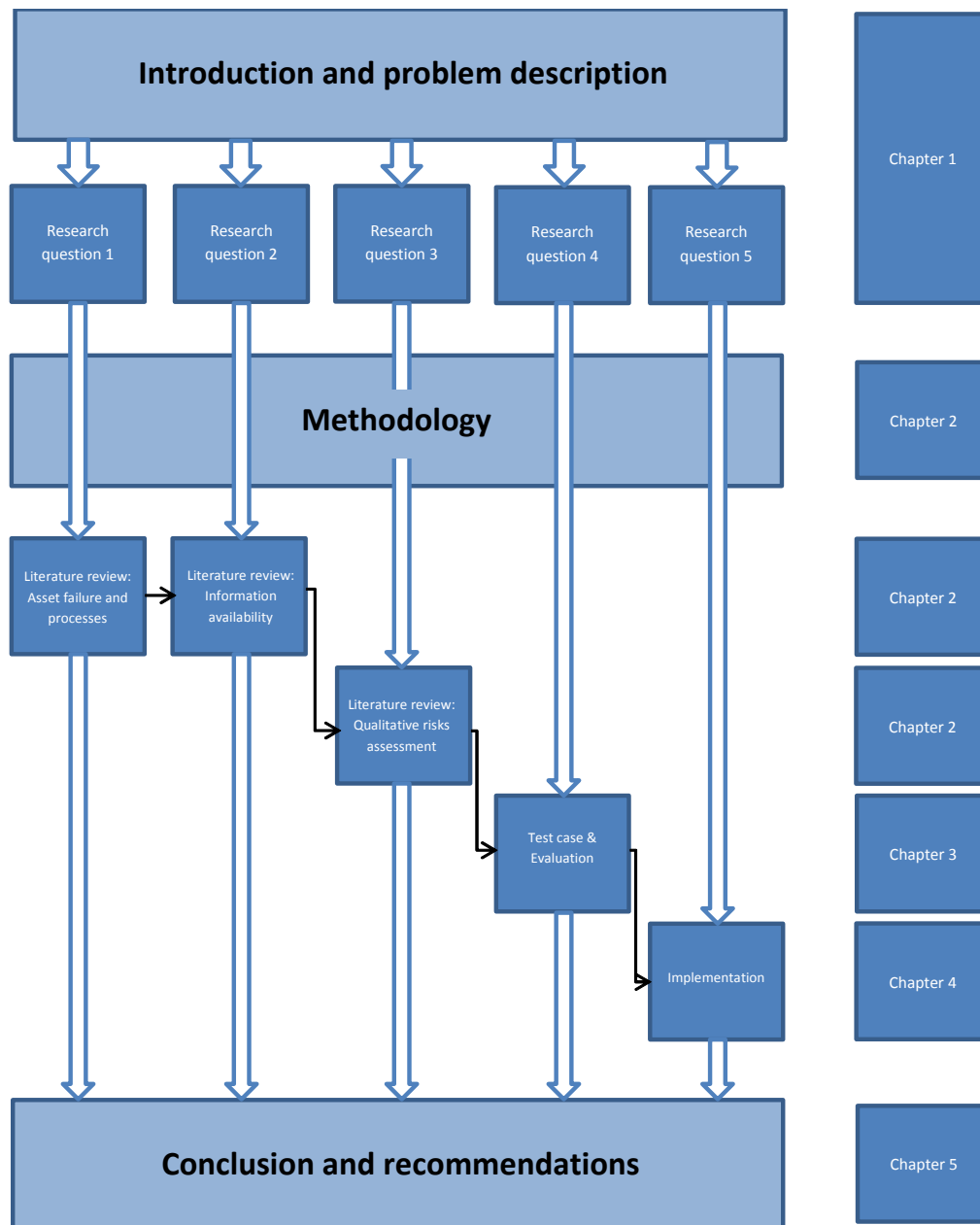


Figure 1.8: Report structure.





# 2

## State of the Art

This chapter provides a background for the research. Section 2.1 gives a theoretical background and states which research methods are used for this research. A wide-reaching literature study is presented concerning how the current disruption process is organised. It specifically addresses questions such as, Which organisation is responsible for what action? How it is executed in practice? What is the problem, and how it could be solved? Section 2.2 gives the practical background of the organisation of failure recovery and asset failure. Section 2.3 elaborates on what kind of information is available. For this research, many acronyms are used, and most railway acronyms are described by the infrasite (Infrasite.nl, 2016).

### 2.1. Research Methodology

The performed research is exploratory, set up to explore the possibilities of wider and better use of information in a systematic way. With such open-ended research, possible relationships can be found, and underlying structures are mapped. All potentially interesting information is collected through qualitative research by a case study. The underlying methods and theory guiding the case study are found in the literature, as presented in the following sections.

#### 2.1.1. Fault Tree Analysis (FTA)

Fault Tree Analysis (FTA) is a systematic analysis technique to determine the root causes of a specified undesirable event (Ericson, 2005). An FTA can be used to evaluate complex dynamic systems to better understand and prevent potential problems. Using rigorous and structured methodologies, a fault tree (FT) can be constructed. An FT is a logically and graphically represented combination of possible events or failures that lead to an undesired event or state. The FT envisions the logical fault paths from all possible root causes, at the bottom, to the single undesired event, at the top. An FT is easy to perform and easy to understand; it can also provide useful system insights and show all of the possible causes for a problem or event. The FT uses logic gates and fault events to model the cause-effect relationships involved. Where AND- and OR-operators indicate whether causes are occurring in parallel or in series.

According to Ericson (2005), there are eight basic steps for performing an fault tree analysis, as shown in Table 2.1.

Table 2.1: fault tree analysis (FTA) process steps obtained from Ericson (2005).

Step	Action	Description
1.	Define the system	Understand system design and operation. Acquire current design data (drawings, schematics, procedures, diagrams, etc.).
2.	Define top undesired event	Descriptively define problem and establish the correct undesired event for the analysis.
3.	Establish boundaries	Define analysis ground rules and boundaries. Scope the problem and record all ground rules.
4.	Construct Fault Tree	Follow construction process, rules and logic to build FT model of the system.
5.	Evaluate Fault Tree	Generate cut sets and probability. Identify weak links and safety problems in the design.
6.	Validate Fault Tree	Check if the FT model is correct, complete, and accurately reflects system design.
7.	Modify Fault Tree	Modify the FT as found necessary during validation or due to system design changes.
8.	Document the Analysis	Document the entire analysis with supporting data. Provide as customer product or preserve for future reference.

FTs consist of nodes, interlinked in a tree-like structure. The nodes represent fault or failure paths and are linked together by Boolean logic and symbols. Operators used for this research are shown and explained in Figure 2.1.


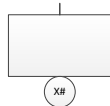
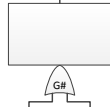
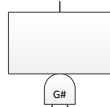
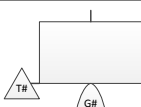
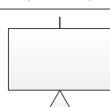
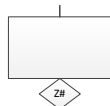
Symbol	Type	Description
	Node Text Box	Contains the text for all FT nodes. Text goes in the box, and the node symbol goes below the box.
	Primary Failure Code: X#	A basic component failure; the primary inherent, failure mode of a component. A random failure event.
	OR Gate Code: G#	The output occurs only if at least one of the inputs occurs.
	AND Gate Code: G#	The output occurs only if all of the inputs occur together.
	Transfer Out Code: T#	Indicates where a branch or sub-tree is transferred to the same usage elsewhere in the tree.
	Transfer In Code: T#	Indicates where a branch of sub-tree is inserted from another usage elsewhere in the tree.
	Secondary Failure Code: Z#	An externally induced failure or a failure mode that could be developed in more detail if desired.

Figure 2.1: fault tree (FT) symbols.



Figure 2.2 depicts a simplified example of an FT where the top unwanted event is that a car will not start. All nodes have a unique identifying code for easier reference.

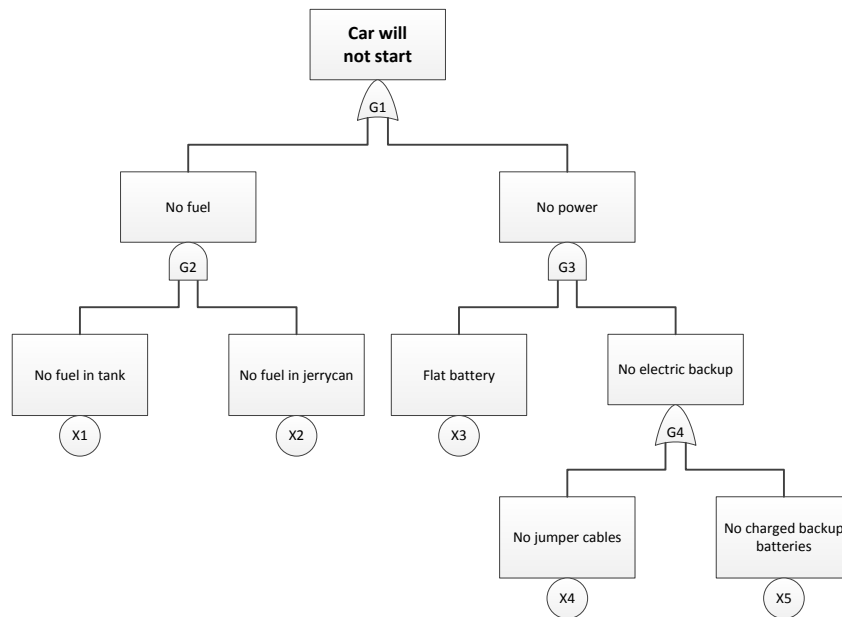


Figure 2.2: fault tree (FT) 'Car will not start' example.

As can be seen, the unwanted top event in Figure 2.2 is that the car will not start. The causes of this failure may be that there is either no fuel or that there is no power to start the engine. If the top event is caused by no fuel, then there is no fuel in the tank and there is no back-up fuel in the jerrycan.

### 2.1.2. Event Tree Analysis (ETA)

According to Ericson (2005), an event tree analysis (ETA) is an 'analysis technique for identifying and evaluating the sequence of events in a potential accident scenario following the occurrence of an initiating event'. By performing an ETA, a visual logic tree structure can be constructed, an event tree (ET). The ET allows one to determine whether the initiating event will develop into a serious mishap or whether it is sufficiently controlled by the safety mechanism and procedures implemented in the system design. By answering several binary questions (yes/no, success/failure), the event tree can produce many different branches, all of which represent different possible outcomes from a single initiating event.

According to Ericson (2005), there are 10 basic steps for performing a complete and accurate ETA, as shown in Table 2.2.

Table 2.2: event tree analysis (ETA) process steps obtained from Ericson (2005).

Step	Action	Description
1.	Define the system	Examine the system and define the system boundaries, subsystems, and interfaces.
2.	Identify the accident scenarios	Perform a system assessment or hazard analysis to identify the system hazards and accident scenarios existing within the system design.
3.	Identify the initiating events	Refine the hazard analysis to identify the significant IEs in the accident scenarios. IEs include events such as fire, collision, explosion, pipe break, toxic release, etc.
4.	Identify the pivotal events	Identify the safety barriers or countermeasures involved with the particular scenario that are intended to preclude a mishap.
5.	Build the event tree diagram	Construct the logical ETD, starting with the IE, then the PEs and completing with the outcomes of each path.
6.	Obtain the failure event probabilities	Obtain or compute the failure probabilities for the PEs on the ETD. It may be necessary to use FTs to determine how a PE can fail and to obtain the probability.
7.	Identify the outcome risk	Compute the outcome risk for each path in the ETD.
8.	Evaluate the outcome risk	Evaluate the outcome risk of each path and determine if the risk is acceptable.
9.	Recommend corrective action	If the outcome risk of a path is not acceptable, develop design strategies to change the risk.
10.	Document ETA	Document the entire ETA process on the ETDs. Update for new information as necessary

Where FTs flow from the sources in the direction of the undesirable event. ETs are reversed: they start with a single undesired top event and model the effects that can occur. Several combinations of conditions lead to certain consequences. Figure 2.3 shows an example of an ET for the ‘car will not start’ example. There can be seen that the ET starts with the initiating event, followed by several questions for outcome identification. When a question is answered with ‘yes/success’, the upper branch is chosen, and if ‘no/failure’, the lower branch is followed. When all (relevant) questions for a branch are answered, the branch results in an outcome. The outcome can be a binary answer to a question or an individual result.

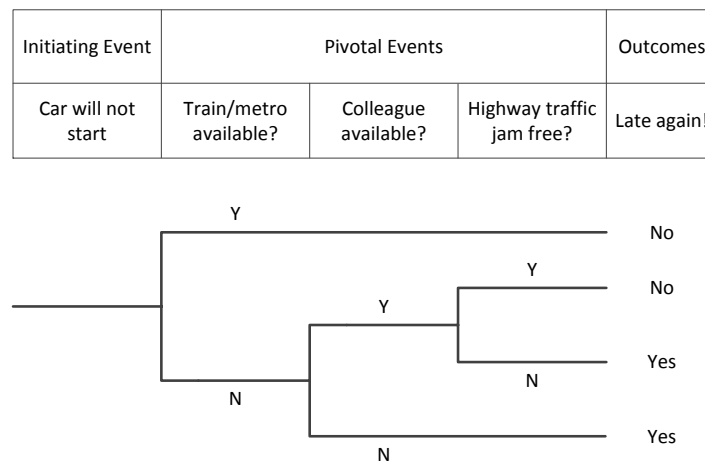


Figure 2.3: event tree (ET) ‘Car will not start’ example.





Initiating Event	Pivotal Events					Outcomes
Car will not start	Are the lights working?	Fuel gauge level at zero?	Full jerrycan absent?	Jumper cables present?	Full backup battery present?	

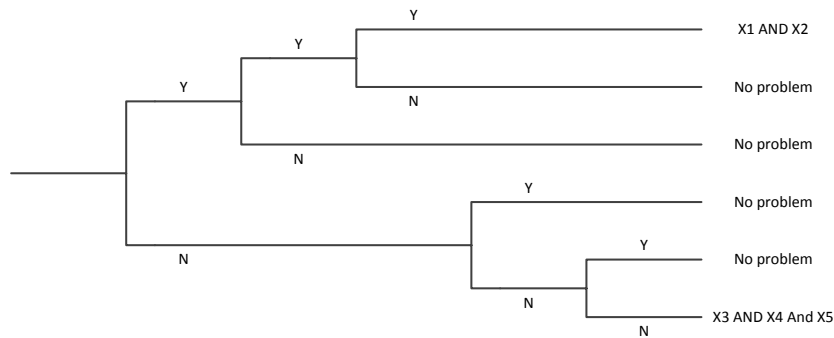


Figure 2.5: Adapted pivotal events, event tree (ET) 'Car will not start' example.

#### 2.1.4. Case Study

The above method is applied in a case study to incorporate and evaluate the relevance of the framework: 'A case study is an empirical inquiry which: investigates a contemporary phenomenon within its real-life context, when the boundaries between phenomenon and context are not clearly evident, and in which multiple sources of evidence are used' (Yin, 1994). A case study is a strong method because it involved flexible research design that allows one to draw conclusions about empirical events in a real-life context (Schell, 1992) by tweaking and testing the design (Yin, 1994).

Case studies are the subject of criticism as a research strategy, however. Much the criticism of the case study method relates to its labour-intensive nature, its 'unreliable' or 'invalid' conclusions, its limited basis for scientific generalisation, especially with single cases, and its potential ethical issues (Schell, 1992). The criticism of its labour-intensive nature is particularly prevalent when observations have to be performed and processed. For this specific research, this criticism can be dismissed because of the use of already available information and theoretical knowledge, and since only one test case is performed to show the added value and information gain of the combination of FTs and ETs. The research aims at the development of theory and not at testing a specific hypothesis. The design framework also bridges the gap for a small scientific base, by implementing an FTA and ETA. Potential ethical issues are considered within the literature review stage. Therefore, the use of case studies suits the need of a flexible and creative method to address the problem.

#### 2.1.5. Fault Tree (FT)-Event Tree (ET) Evaluation and Validation

After the analysis was performed, the approach was tested and validated for several historic cases. All (available) information was used to check whether the right outcomes are achieved. If not all necessary information was available, it could be checked whether the right branch(es) can be reached.

### 2.1.6. Methodology Discussion

The chosen methods have some known pitfalls, as noted by Ericson (2005). FTA can become the goal rather than the tool and can easily become time consuming. Modelling multiple phases and sequential time is difficult. Also, the appropriate depth of the FTA can be discussed. The FT can still have undeveloped events in which the FT fails to pinpoint all components. The ETA has some disadvantages as well. It can only have one initiating event, for example; therefore multiple ETAs will be required to evaluate the consequence of multiple initiating events. Also, the ETA can overlook subtle system dependencies when modelling the events. The resulting ET is binary, so partial successes and failures cannot be distinguished. Furthermore, to perform a thorough FTA and ETA requires an analyst with some training and practical experience.

Both methods are quite old-fashioned, as well. A more data-driven method like a common-cause analysis was more preferable. Because of the lack of digital system information, links in the network and links between the elements, this method and more automation was not possible.

The FTA was selected because it uses a relative simple and easy-to-understand top-down method. Since the start of the analysis is a top event (failure notification) and not a component failure, the FTA fits better than a bottom-up method like a failure mode effect and criticality analysis (FMECA). The method is used after the notification is created and is not used to predict a failure; therefore more complex methods like Bayesian belief nets (BBN) are unsuitable. Since this is a qualitative research and probabilities are not quantified, and since only logical dependencies need to be identified, the complicated method of BBN is too powerful. In addition, the FTA is a well-known and proven method used in several other industries (aviation and chemical plants), and it fits the purpose of this study.

With the combination of the FT on the left and an ET on the right, and the transformed FMECAs (as pivotal questions) in the ET, the three methods can be used to assess a failure notification.

## 2.2. Practical Background

As mentioned in Chapter 1, the environment of the railway network in the Netherlands is very complex, due to its many stakeholders. When the network experiences a failure, all stakeholders want to do what is best for their own organisation. A common aim is to recover as fast as possible. As stated earlier, this speedy recovery precipitated the introduction of the OCCR. What happens in case of a disruption is outlined out in the following section.

### 2.2.1. Failure Recovery Organisation

At a given moment, a failure notification is received. In most cases the *treindienstleider* [dispatcher] (Trdl) receives this notification. The Trdl is part of the *verkeersleiding* [traffic control] (VL) and is responsible for the safety of the train traffic in her designated area. This person also has direct contact with train drivers, and she can receive a notification from a train driver or a system warning. It is also possible that a third party (emergency services, bystanders or a PCA) declares a failure. In that case, the notification is received by the call centre of the *meldkamer spoor* [railway control room] (MKS).

The MKS is the generic name for the failure-handling organisation of ProRail's AM department within the OCCR. The term covers the directors, call centre operators and the *operationeel besturingscentrum infra* [operational control centre infrastructure] (OBI) and the back office. The OBI is responsible for the intake and forwarding of 40,000 asset failures, originating from several different channels to the different responsible PCAs. Additionally, they perform around 9,000 'switching commands' to interrupt a catenary (*bovenleiding*) section and 6,000 commands to switch the local and central power supply, because of which the contractors can safely perform maintenance and repairs to the different systems. The director (*regiseur*) is responsible for managing the whole recovery process when it impacts the train services. Therefore, the director stays in contact with all stakeholders and communicates status updates during a disruption.

The process is described in detail in the *Storingshandboek* (ProRail AM Infrabeschikbaarheid, 2016b), and a simplified version is presented, as explanation, for the case of a Trdl receiving a failure notification. The main actors of the process can be seen in Figure 2.6.

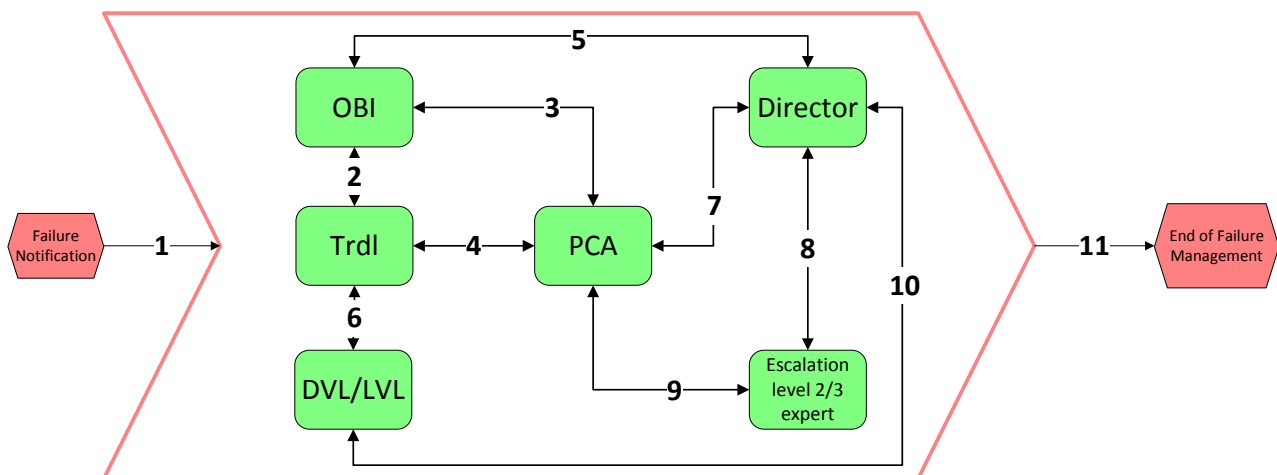


Figure 2.6: Main actors failure recovery process ProRail (simplified).



When a failure occurs, a notification is received by the Trdl (Link 1). The Trdl informs the OBI operator (Link 2) about the failure. The Trdl explains the location and the type of failure, while the OBI operator creates an item in the SAP database. The goal in this step is to determine appropriate priority and discern the time the failure occurred ( $T_{-2}$ ), the time the failure notification was reported to the OBI operator ( $T_{-1}$ ) and the time the PCA is notified ( $T_0$ ) (Link 3). The ( $T_0$ ) notification is called a *rapport van onregelmatigheid* [report of irregularity] (RVO) and contains the ID and name of the element and its location, along with a description of the irregularity. When the right PCA receives an RVO, the PCA has to interpret and accept it, in order to send the right mechanics with the right skills, resources and priorities to the failure location. When all personnel needed to start the repair are present at the location, the PCA mechanic informs the Trdl that they have arrived and registers it in the SAP database ( $T_1$ ). The mechanics can then begin to diagnose the problem. Depending on the nature of the failure, the track is taken (completely) out of operation to create a safe working environment for the mechanics, or they can safely examine elements outside of the track. If necessary, the track is taken out of operation by direct contact from the *leider werkplek beveiliging* [chief workplace safety] (LWB) and Trdl (Link 4). When it is safe, the mechanics can start diagnosing the problem. After the problem is diagnosed, the PCA notes in the SAP database the PCA's estimated repair time and whether the element can be used in the meantime (Link 4). Considering the prognosis, diagnosis, priority, time and other influences, the MKS and Trdl decide whether the problem needs to be fixed immediately or at another time. This determination is communicated by several links. Depending on the outcome, the mechanics start to fix the problem.

When the priority is high enough, a director is also assigned (Link 5) to the repair process. The director monitors the whole process and is the central contact person. When the impact is high or the failure is elusive, the director can 'escalate', meaning he can contact a higher level of management or experts for more problem solving (Link 8). The director has contact with the *decentrale verkeersleiding* [decentralized VL] (DVL) and *landelijke verkeersleiding* [national VL] (LVL) (Link 10) for coordinating the impact for the whole timetable with a local and national overview.

When the prognosis cannot be achieved, the PCA needs to update the prognosis ( $T_6$ ) in the SAP database. When the failure is discovered, the PCA needs to inform the SAP database of whether the repair was successful or in which way and to what degree the element can be used ( $T_3$ ) (Links 3, 7, and 4). When the failure is repaired, the track can be operated again. The PCA will inform the Trdl by Link 4 they can operate the track again ( $T_5$ ). When everything is completed and all information is (correctly) added to the SAP database, the failure is closed ( $T_4$ ) (full SAP report content is stated in Appendix A). All ordered time stamps can be seen in Figure 2.7.

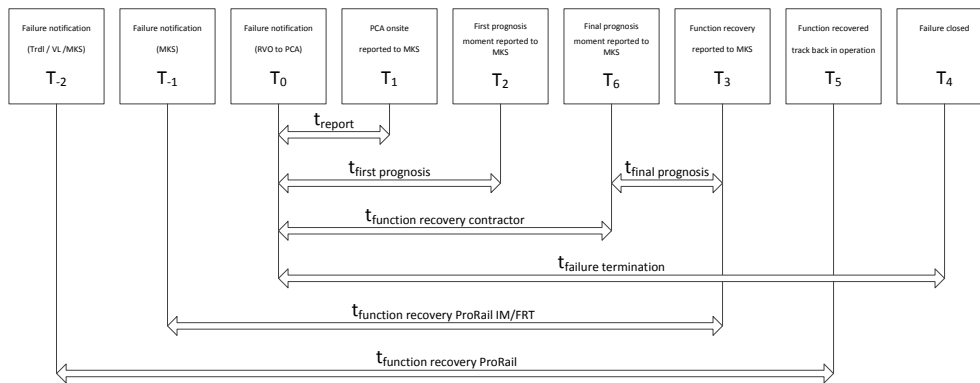


Figure 2.7: Failure-recovery time line ProRail (ProRail AM Infrabeschikbaarheid, 2016b).

### Priority Classification

As mentioned a priority level needs to be assigned to a failure notification to determine when it needs to be fixed. The classification is based on the damage, impact and the *train incident scenario* [train incident scenario] (TIS). A TIS is a general classification of all kinds of disruptions, not specific to AM failures. All possible AM failure priority classifications are presented in Table 2.3.

Table 2.3: Failure priority classifications (ProRail AM Infrabeschikbaarheid, 2016b).

Priority	Urgency	Notification type	Repair	TIS-scenario	Characterize
1	Urgently	Infra-emergency	Immediately	Yes	- Major infrastructure damage - Very large impact - Direct repair
2+	Urgently	Disruption	Immediately	Yes	- Impact on the train service - Direct repair
2	Urgently	Disruption	Immediately	Yes	- Direct repair
5	Urgent with time agreement	Disruption	Postponed	Dependent	- Time agreement between VL and MKS on function recovery
4	Not urgently	Disruption	Postponed	No	- Not urgent - No immediate repair needed
8	Preventive	Preventive	Depending on necessity	No	- No loss of functionality
9	Administrative	Administrative	n.a.	No	- Messages are not sent to contractor

### Function Recovery Classes

As stated before, there are several options for element repairs. Ideally, the element is repaired fully at the first possibility. In the real environment of the Dutch rail network, this is not always achievable. Sometimes mitigating solutions are performed to reduce repair time, or some parts are not available at that time. Therefore, there are different classes for function recovery. All classes are outlined in Table 2.4.

Table 2.4: Function recovery classes (ProRail AM Infrabeschikbaarheid, 2016b).

Code	Status	Proceedings
1	Fully restored function	Contractor carried out repairs completely. There is no remaining work needed.
2	Temporarily restored function	Contractor has conducted repairs but not yet finalized. At a later time, function will be restored permanently. The disturbed object is functioning 100%.
3	Partially restored function	Contractor has conducted repairs but not yet finalized. At a later time, function will be restored permanently. The disturbed object is functioning partially.
4	No function recovery	Contractor has conducted examination but not (yet) repairs.
6	Examination/Recovery -hindered	Contractor may or may not have performed examination but can not enter tracks for examination or repairs.

### Practice

In reality, the process is sometimes more turbulent. Most links in the failure-recovery process of ProRail (Figure 2.6) are performed in an office environment and are relatively easy to manage. However, the repair process is performed 'outside'. The only thing the mechanics receive is the RVO, most of the time consisting of the following asset-related elements:

- Abbreviation route section/yard,
- Abbreviation object,
- Indication kilometre set (if known),
- Brief description irregularity, and
- Brief description result(s) irregularity.

For clarification, two examples are given.

- Example 1
  - Notification:
    - ◊ Lunetten level crossing 36.5 disturbed and track between switches 1117 and 1115A is improperly occupied.
  - RVO:
    - ◊ Ln : Wl-1117/1115A t.o.b.s., ovw 36.5 disturbed.
- Example 2
  - Notification:
    - ◊ On the route section between conjunction Amersfoort and Zwolle the bells of level crossing 30.2 are not working.
  - RVO:
    - ◊ Ama-Zl : Ovw 30.2, bells out of service.

When someone is not used to reading an RVO, it looks like a coded language. After some training, however, this problem is solved. A bigger issue is that it contains minimal information. The location of an element is sometimes quite clear when it comes to, for example, a level crossing, but it can also be less precise in the case of a section on the open track. Experienced mechanics know their way around the different objects and locations within their contract territory, but the notification does not mention the need for this prior knowledge. The mechanics have to search on (paper) maps to find their location, and then discover a route towards it. Also, the exact nature of the failure is not indicated, only the effect of the specific failure. The RVO does not show any failure history of the element. Such history of an element can be obtained, but is not supplied by default. Therefore the repair process of the element relies on the experience, inventiveness and training of the mechanics. With frequently occurring failures and experienced mechanics, this reliance does not need to be a problem, but otherwise it could be a cause of delay.

### Maintenance Contracts

As mentioned earlier, ProRail is responsible only for managing the railway system. Maintenance and repairs are tendered to a PCA. ProRail is now in a transition phase from output process contract (OPC) to *prestatiegericht onderhoud* [performance-based maintenance] (PGO) contracts. An OPC is a contract form which, based on a prearranged maintenance schedule, the maintenance of the railway infrastructure is performed. A PGO is a contract form in which the outcome (the desired level) availability of the railways is crucial and set in the contract, but the manner of how this level is reached is primarily the responsibility of the contractor, meaning that the contractor has more responsibility and freedom on how to reach that level. Therefore, ProRail cannot directly prescribe a method of how to solve a particular failure or order a PCA to do something. One could say ProRail has no responsibility anymore and should therefore not interfere in the processes of the PCA. Remarkable to this sentiment is that for the PCA it does not matter where a malfunction occurs. For them, every piece of track in the Netherlands is equal, while ProRail is judged on client inconvenience, so large nodes and critical sections have much more impact for ProRail than quiet and less-travelled sections of track. In addition, the levels of availability for the important parts are greater than for less-important parts of the network (All information adapted from '*Factsheet: Kenmerkende verschillen OPC - PGO*' (ProRail, 2008)).



## 2.3. Operational Data

Since the introduction of computers, almost every element and action has become controlled or performed with the use of a computer. All interlocking systems are centralised and can be controlled and managed by computers. Over time, technology has provided more and more possibilities. Over the years those possibilities have supplemented the ICT systems. The current ICT-O systems and applications, and their relations, can be seen in Appendix Figures B.1, B.2. This research focusses on Post21 elements, and these elements are shown Figure 2.8.

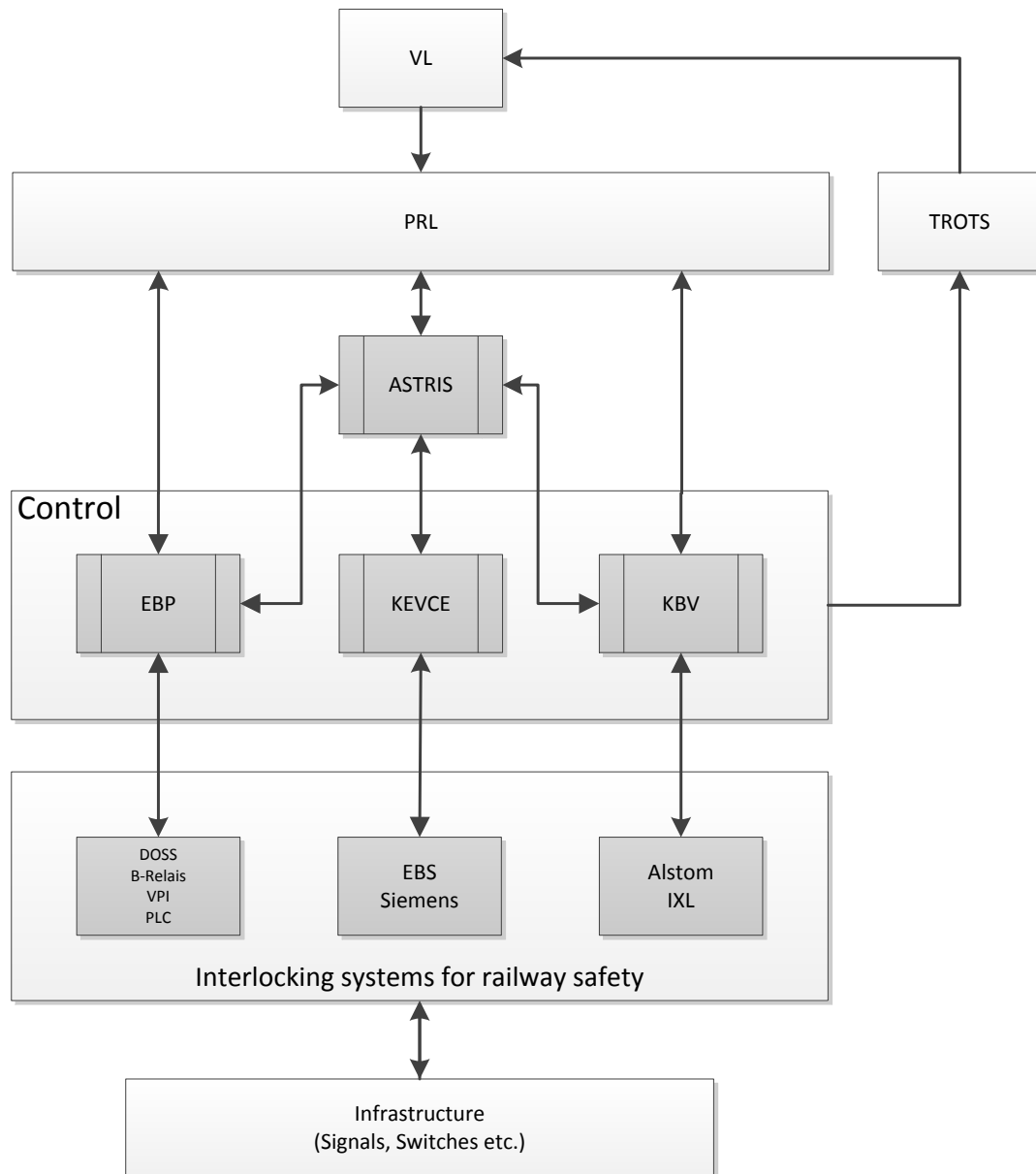


Figure 2.8: Post21 configuration adopted from InTraffic (2016).

Operating a schedule starts with a plan for the year: where, when, how and which train drives. This overarching plan becomes a day plan because every day deviations and adaptations to the year's plan are necessary. The year's plan is transformed into a local plan for a specific dispatcher or working station and a national plan. The outcome of both plans, combined with external plan changes, are the input for VL and *procesleiding rijwegen* [route processing systems] (PRL). PRL can be seen as the brain of the Dutch railway network, as it enables all trains in the Netherlands to arrive safely and on time. It sets the routes by controlling interlocking and infrastructure elements. This control is executed manually by a dispatcher, or it is executed automatically by the tool *automatische rijweg instelling* [Automatic route setting] (ARI). PRL controls the different control systems (EBP, KEVCE/EBS, KBV), which controls the underlying interlocking systems, like conventional B-Relays and vital processor interlocking control system (VPI)s or European rail traffic management system (ERTMS) by, Alstom, Bombardier and Siemens. The interlocking systems control the physical elements 'outside' like switches and signals.

Almost all events or actions performed by the PRL system are logged for every dispatcher and consequently for the whole network, generating a great deal of data (18 gigabytes of data and csv files a year). All underlying ICT systems also generate data. At the lowest level of ICT systems (interlocking), not every log is stored. Only when an operator manually commands the system to do so will it store events and logs. Also, the control level does not store everything. Only the command and the final 'safe' message are normally stored. On the other hand, both systems' layers have predefined error notifications. When something does not perform as planned, the system sends a notification to the PRL. The PRL systems themselves also log all internal failure notifications. The failure notifications of the PRL system and underlying systems are stored and are shown in the 'Interface Design Document - CARE Meldingen' (InTraffic, 2015).

The TROTS is used to monitor trains, when their route is set by the PRL system. This is achieved through a *treinnummer volgsysteem* [trainnumber follow-up system] (TNV) and track element status updates from the control systems as described earlier. Every TROTS event is logged and stored and can be assessed by the 'TOON' applications. It combines the TROTS logs and the infrastructure database, so one can see what was happening at a location at a certain time. The TROTS system also recognises failures, for example a *ten onrechte bezet spoor* [improperly occupied track] (T.O.B.S.) alert. The failure notifications are included in the TROTS log. The TROTS system is further described in the 'Interface Design Description - TROTS' (ProRail, 2013).

From his control area, the VL dispatcher gets an overview picture of the situation, at all times, as shown on the operating screen of his workstation. The downside is that only current failures are shown, so historic or short failures cannot be recalled by the dispatcher. Historic and short notification are stored in the log file and are accessible when they are stored by ICT-O. Not everything is logged that appears on the dispatcher's screen. Not all consequences of a failure are logged because these are indirect effects that do not produce individual failure messages. For example, it is normal for a switch to become inoperable when there is a route set over the switch, so becoming inoperable is not always a failure; on the other hand, sometimes it is the effect of a failure.

### 2.3.1. Asset Failure

According to Isermann (1984), 'A fault is defined as an unpermitted deviation of at least one characteristic parameter of a system from normal (healthy) status' (Isermann, 1984). By contrast, 'A failure is defined as the state of a permanent invalidation of a system to perform normal functions', according to Bai (2010).

Bai (2010) states that there are four main categories of time-varying faults, as can be seen in Figure 2.9.

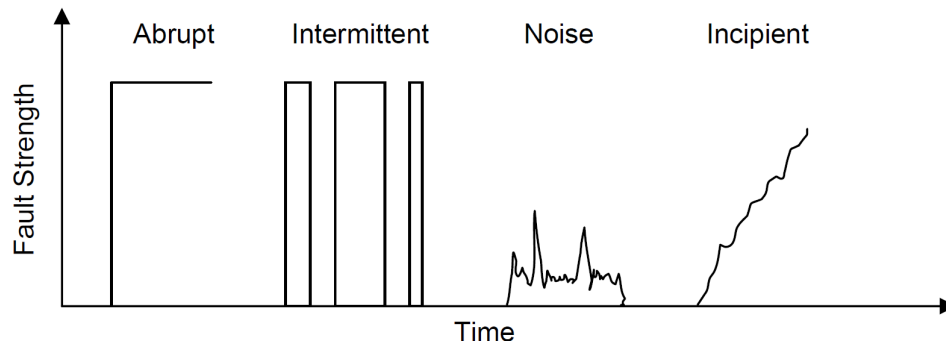


Figure 2.9: Time-varying faults by Bai (2010).

If an abrupt fault occurs, the system jumps from a healthy status to a failure without any sign. Intermittent faults can happen when electrical connections are unstable. Disturbance or noise take the form of an unknown extra input to a system and can randomly cause malfunctions or failures. Mechanical systems typically have incipient faults; when an element is used, it gradually degrades due to wear.

An asset can fail for various reasons. The various causes used determined and logged (in the SAP database) by ProRail can be seen in Appendix C.

As stated before, only failures are reported by the various systems. For a mechanic to solve the problem, the fault has to be diagnosed. For that reason an FMECA was constructed for most critical elements, an example of which can be seen in Appendix D. Based on the FMECAs and other sources, mechanics are trained to find a fault and know how to repair it. The FMECAs centre on elements and are not directly related to a notification. In other words, when a notification appears, it tells the recipient that the system is not working as designed, and in most cases it does not identify the failing element.

## 2.4. Conclusion

The purpose of this chapter was to introduce the used methods, explain the failure-recovery organisation and identify available sources of information. When information can be combined with theoretical failure modes, this the combination can (partially) fill the knowledge gap between a notification and the failing object. This bridging can enhance the information supplied to a PCA and thus improve the failure recovery time (FRT).

As stated, the Post21 system includes many useful sources. PRL and TROTS failure notification are the basis of an RVO. Combined with the information on the dispatcher's operating screen, the systems contain a much information. When the information can be combined with better insight into failure notifications, an enormous potential gain in understanding failure processes presents itself.

The present practice for failure information transfer between ProRail and PCA can be seen in Figure 2.10.

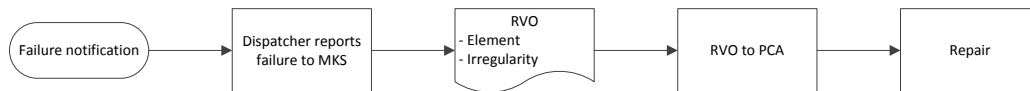


Figure 2.10: Current information stream between ProRail and PCA.

The most recent literature suggests a composition for failure information as shown in Figure 2.11. The composition is applied, tested and evaluated in subsequent chapters of this study.

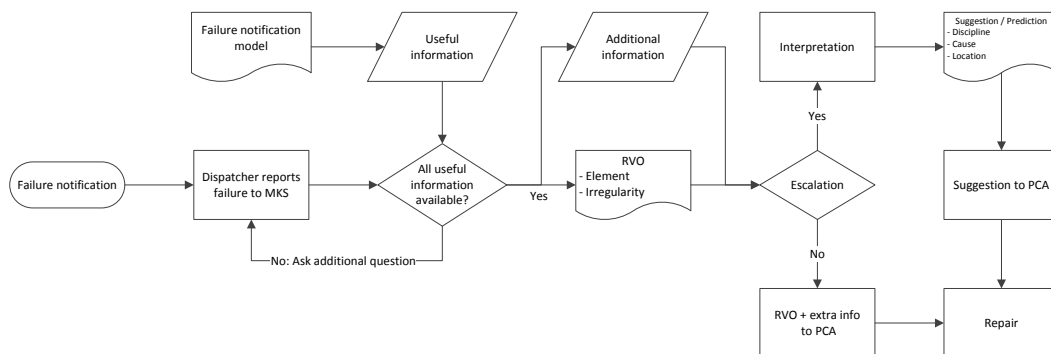


Figure 2.11: Proposed information stream between ProRail and *procescontractaannemer* [contractor] (PCA).





# 3

## Disturbed Power Supply

To check whether the stated methodology is working in practice, a test case was constructed for a specific notification. For some failures, it is immediately obvious which mechanical expertise are required, what and where they need to fix it (for example, in the case of a level-crossing failure). Other failure notifications require various mechanical skill sets, and the cause could stem from several places over a large area. In the case of a more general notification, it is not clear which mechanical discipline is required and where they need to go to solve the problem. Additional information could support the disruption-management process in assigning the right mechanics and sending them to the right location.

An example of an unclear notification is the *Stroomvoorziening gestoord* [disturbed power supply] message. The notification is generated if the *treinbeheersings- en treinbeveiligingsinstallaties* [route control and train protection] (TBB) power supply is disrupted. Many of the (interlocking) elements and railway safety measures are, in general, dependent on power supply. This notification is generated around 2,000 times a year, of which 35 result in a train service disruption. In 2015, a total of 1,318 trains were effected, leading to 54,000 train delay minutes. In the past year, two disruptions were indicated as very large and were researched by ProRail. The internal research indicated that a better use of information could help the disruption-management process, and the downtime could be reduced for those specific cases by up to 1 hour and 45 minutes. Considering the objective and specifics of the ‘power supply disturbed’ notification, the methods described in Chapter 2 were applied to this notification. This chapter will line out the performed test case for this notification.

In Section 3.1 and Section 3.2, a useful background of the power supply system and relay interlocking is presented. The function of power monitoring and its challenges are explained in Section 3.3. Section 3.4 outlines the system architecture. The resulting FT and ET for the ‘power supply disturbed’ notification are presented in Sections 3.5 and 3.6. Finally in Section 3.7 the performance of the model is validated, based on historical cases.

All information presented in this chapter is based on the following sources:

- Bedrijfsvoeringshandboek - Energievoorziening, Niet-tractievoeding (ProRail Assetmanagement, 2012);
- Technisch beleid - Energievoorzieningsstelsel Railinfra voedingen (ProRail Assetmanagement, 2010);
- B-relais stationsbeveiliging - NX-systeem ‘68 (Railinfra Opleidingen, 2011);
- Instandhoudingsdocument - Voeding TBB - Deel 1 Centrale Voeding 3kV (ProRail, 2005);

- Instandhoudingsconcept - Voeding TBB - Centrale Voeding (ProRail, 2016c);
- Instandhoudingsrisico Analyse- Voeding TBB - Centrale Voeding (ProRail, 2016g);
- Instandhoudingsconcept - Voeding TBB - Lokale Voeding (ProRail, 2016d);
- Instandhoudingsrisico Analyse - Voeding TBB - Lokale Voeding (ProRail, 2016h);
- Instandhoudingsrisico Analyse - Laagfrequent Spoorstroomlopen (GRS) (ProRail, 2016f);
- Instandhoudingsconcept - Laagfrequent Spoorstroomlopen (GRS) (ProRail, 2016b);
- Instandhoudingsrisico Analyse - B-relais IXL (ProRail, 2016e);
- Instandhoudingsconcept - B-relais IXL (ProRail, 2016a);
- Ontwerpvoorschrift - Voeding TBB - Deel 1 Algemeen (ProRail, 2012a);
- Ontwerpvoorschrift - Voeding TBB - Deel 2 Centrale Voeding (ProRail, 2012b);
- Ontwerpvoorschrift - Voeding TBB - Deel 3 Lokale Voeding (ProRail, 2012c); and
- Ontwerpvoorschrift - Voeding TBB - Deel 4 Ontwerphandleiding (ProRail, 2012d).

Additionally several internal ProRail technical system drawings for specific location were obtained and consulted.

### 3.1. Power Supply System

Railway power supply can be divided into two parts, *tractie-energievoorziening* [traction power supply] (TEV) and TBB power supply. TEV represents the power needed to run the (electric) trains. For this case, the ‘disturbed power supply’ notification was analysed; this notification is based on the TBB power supply. The absence of the power supply leads directly to a disruption of train service. TBB includes power supply systems for train protection and control equipment, including the critical telecom and telematics systems. The TBB power supply can also be split up into two main components, the ‘Local power supply’ and the ‘Central power supply’. For local power supply, the electrical energy is taken from the grid at one feeding point and delivered to a single (group of) user(s) at a single location. For the central power supply, the electrical energy is taken from the grid at two separate power points and delivered to several (groups of) users in multiple locations. In general, local power supply is used for traffic control locations, relay houses, one third of the switches and power for level crossings (on shunting yards, station areas). The central power supply is the 3kV power supply system that provides electric power to the track-side elements in areas between stations (two-thirds of the switches and the power of level crossings) and for all train detection and *automatische treinbeïnvloeding* [automatic train control] (ATB) components. The local power supplies deliver a greater availability than the central power supply due to the connected grid and the use of redundancy, emergency power generators, uninterruptible power supply (UPS) and batteries. The UPS component provides power when the power supply of the grid is lost. The central power supply is also redundant but has no possibility to store the energy necessary in a situation involving a full loss of power. An overview of both the local and central power supply can be seen in Figure 3.1 and 3.2.

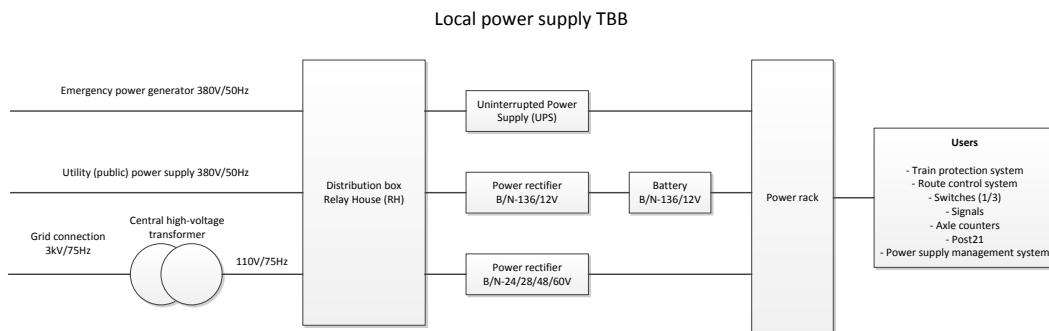


Figure 3.1: Overview local power supply (Railinfra Opleidingen, 2011).

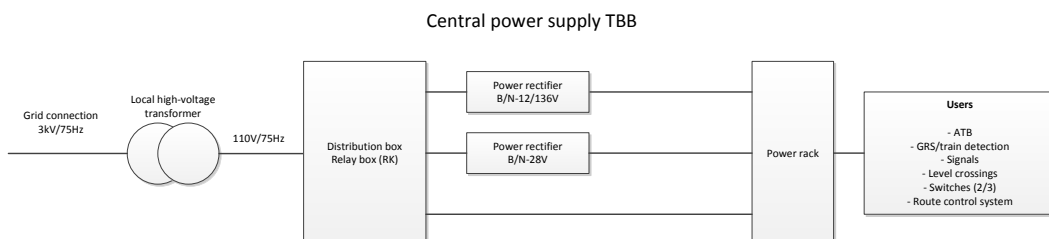


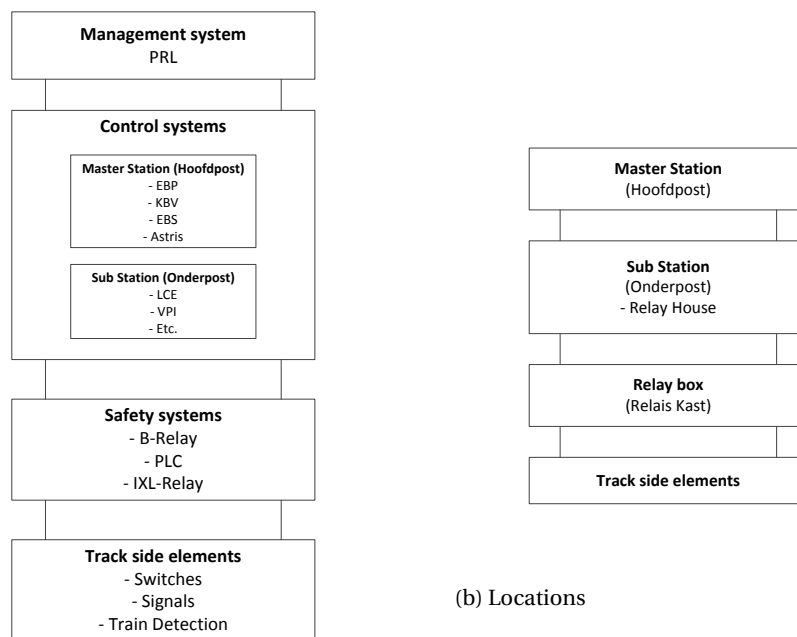
Figure 3.2: Overview central power supply (Railinfra Opleidingen, 2011).



### 3.2. Relay Interlocking

The control structure for the railway infrastructure is composed of several layers and locations. As shown in Figure 3.3a and 3.3b. There are several master station systems used in the Dutch railway network. These include EBP, KBV and EBS, further to which a top layer of *aansturing en statusmelding van de railinfrastructuur* [control and status-notifications for rail infrastructure] (ASTRIS) could be applied. The EBP master station is executed with several kinds of sub-stations, such as *lokale controle eenheid* [local control unit] (LCE) or VPI. The master and sub-stations control the interlocking systems; these could, for example, be based on B-relays (NX '89) or PLC interlocking technology.

The system of an EBP master station with an LCE substation based on B-Relay interlocking (NX '89) is analysed for this research, since this system is the most frequently used in the Dutch rail network.



(a) Structure

(b) Locations

Figure 3.3: Railway control structure.

By making use of relay or power off relay (POR) interlocking, the control system can detect at every moment in time where a train, for example, is located. This knowledge can be achieved by using isolated track circuits. The relay is on when there is a current and off when there is no power. When a train drives on a section, it breaks the power circuit, so the system detects an occupied track. Likewise for other elements, the system can detect in what position the element is or what the status of an element is, by which it can check whether a route is safe, and when it is safe it can also set a (safe) route by the same principle. The route (when set) is then kept with relays until the train drives over the track and clears the route setting. For the system to function, different power sources are needed. The communication system needs 230/380V AC, a relay needs 12V DC, for switches to turn 136V DC is needed, and for train detection and other track side elements 110V/75Hz is used.

### 3.3. Power Monitoring

Many of the (interlocking) elements and railway safety, in general, depend on power supply. Therefore the power supply is monitored by several systems, and notifications are generated in the case of a failure. One of these notifications is the 'disturbed power supply' notification. This message is generated and sent by the master and sub-stations and monitored by the dispatcher in the traffic control systems.

In a sub-station, the TBB power supply generally consists of a local power supply and an exit point of a central power line. As mentioned earlier, electrical power is required for different users: signals, switches, ATB, security, but also for the EBP (a control and reporting system). These users require different types of power with different reliability requirements.

The control circuits in the sub-station (e.g. LCE) are protected against an overload and short circuit (*kortsluiting*) by making use of breakers (*automaten*). The aim of the breakers is to efficiently disconnect the LCE interface circuits, thereby protecting them against high current intensities and the wiring from high-temperature damage. Given that a circuit breaker [*zekering*] (CB) opened, the system could no longer work fully, and a notification would be generated by the PRL system. Fortunately, this system is redundant, so the LCE can change to another power supply. Therefore the system can still work normally, but the CB needs to be replaced, and the cause of the fault needs to be identified. When the 12V, 136V or 110V supply is interrupted, regardless of duration, there is no power supply for the track-side elements or the relays. Switches cannot be switched, signals are extinguished, no train detection is possible (i.e. all sections look occupied), and all relays are down. The system executes a fail safe when one of these things happen, and the complete local area system comes to a standstill. When the power supply returns, the system behaves as if the route is cleared by a running train, because a relay went down, while in fact the train has yet to come. When the route is cleared a new and different route can be set. To prevent this from happening unnoticed, a safety mechanism is implemented here. When the power is interrupted, all switches are immediately locked. When the switch is locked, it cannot be redirected in another direction, so all 'old iron routes' remain untouched, and the route is still as safe as possible. The dispatcher has to physically give a command to the system to clear the switch(es). To be sure power is back and stable, a time relay of 20 seconds is built in to let problems subside. After this time, all elements are checked and set again, and 140 seconds later the system is once more up and running.

When any component experiences a TBB power failure, the master or substation reports this in one single combined notification for all components. When the system was engineered, it was costly to install many different power failure detectors; therefore all elements are connected in series. If there is no power in one of the elements, the PRL system generates a notification. For every master station there is one 'power supply disturbed' notification. Since areas of a master station can be comprehensive, many switches, sections, signals, and relays are represented by one notification that does not specify where there is no power.

There is an exception for some elements which are supplied by the local power system. For those elements (UPS, rectifiers, B/N-12/24/48/60/136V), separate failure notifications are created and can therefore be quickly identified. However, this determination is made locally, and there is no generic distribution over the area of the Netherlands; therefore this possibility is not considered.

In fact, there can still be power put into the system, but somewhere an element of the system can break down and then a notification is also generated. In addition to this notification, the various elements are the responsibility of different disciplines of mechanics. The 3kV, 380V and rectifiers are part of the discipline EV. For the high-voltage

transformer, power rack, batteries and all track-side elements, SW is responsible. The LCE, other communication and ICT systems in the sub-station fall within the purview of ICT-O. Besides the rail elements, the power supplier is responsible for an adequate and stable power supply. In case there is a bridge in the area, KW can even be involved. For this case study, however, KW is ignored. Another factor is that every location is different; therefore it is difficult to create model applicable to every location. In order to demonstrate the value of this research, a general model is constructed which can be generally applied to an area. Special elements and local conditions are not included in this research, as it is a proof of concept.

The 'power supply disturbed' is referred to as the A/B/E/S-0228 CARE code. The different letters in the code represent the different intermediate systems as stated in Section 2.3 (A: Astris | B: KBV | E: EBP | S: EBS). The notification A/B/E/S-0228 is generated around 2,000 times per year (unique notifications). Around 500 result from a disturbance item in the SAP database. Of these SAP items, 35 are classified as a TIS scenarios, and around twice a year it causes a total blockade (average over the years October 2012–October 2016).

For a better understanding of this notification system, the next section considers how the system is constructed, with reference to technical drawings.

### 3.4. System Architecture

The system architecture behind the 'power supply disturbed' notification is explained by the existing architecture around Gouda station. As mentioned before, the 'power supply disturbed' notification is linked in series and finally connected to a relay. An example of such a circuit at Gouda can be seen in Figure 3.4. The represented circuit is located inside the *relais huis* [relay house, or sub-station] (RH) in Gouda (RH10).

CLASSIFIED

Figure 3.4: 'Power supply disturbed' notification linked series Gouda.

Where:

<b>IS-Voeding</b>	Incoming power supply.
<b>A/A - 62/62</b>	A clamp or connector (Faston klemmenblokken element).
<b>21 - WE - 10</b>	Connector, connects rack 21 row WE to rack 10.
<b>11C - N12CB1 - 3d/5b</b>	For LCE POR rack 11 row C, CB1 monitoring Negative (-) 12V, installed at connection 3d and 5b.
<b>11B - Voeding - C1/NO1</b>	LCE rack 11 row B, power supply, installed at connection C1 and NO1.
<b>Gd - POSR - 12</b>	Gouda, power off stick relay (POSR), rack 12.
<b>A11/12/3/4/6/8 - POPR - 15</b>	power off repeater relay (POPR) for relay boxes 11A/12/13/14/15/16/18 on clamp 15.
<b>Gd - POPR - 3A/3B 3D/3C</b>	Power supply disturbed relay Gouda, connected at rack 3 row A/B/C/D.

When one of the described elements fails, the 'power supply disturbed' notification is generated. For some of the elements, it is immediately clear what the problem is and that the problem is located in the RH of Gouda. A CB can be opened when the power

supply of the LCE is disturbed or a connection is broken. When a POPR is down, it is not immediately clear because the POPR is just a repeater relay. It is connected to one or multiple other locations. For POPR A11/12/3/4/6/8, the underlying circuit can be seen in Figure 3.5.

CLASSIFIED

Figure 3.5: Underlying power off repeater relay (POPR) A11/12/3/4/6/8 circuit Gouda.

The POPR connects several or one *relais kast* [relay box] (RK) to RH10. Within the different RKs an electrical power off relay (ePOR) is located. An ePOR is a relay which monitors (+/-) 12V and (+/-) 110V; if one of the four currents is not detected, the relay will switch off. Downstream, POPR A11/12/3/4/6/8 and POPR Gd will go down, so a notification is generated.

Further upstream of ePOR RK16, other power circuits are present (Figure 3.6), including the circuits B/N (+/-) 12V and B/N (+/-) 110V as shown in Figure 3.6. The ePOR16 is linked in a series, so if one of the other track-side elements has no power, the ePOR has no power as well, and therefore it will switch off. For this specific case, there are no batteries to feed the 12V (relay power). There is a rectifier that transforms the 110V/50Hz in 12V. The 110V circuits are fed by 'HS kast 16' (high-voltage box 16), which passes a CB (6 amps), goes to the different track-side elements and returns.

CLASSIFIED

Figure 3.6: Power supply B/N-12/110V RK16 Gouda.



Train detection elements which are connected to the power supply of RK16 can also be viewed, more comparable to the infrastructure, on an overview reverse links-scheme [overzicht spoor- en wisselisolatie en retourverbindingen] (OR-scheme), as shown in Figure 3.7 and Figure 3.8. RK16 supplies the train detection power (B/+) for sections 244AT, 242AT, 234AT and 236AT and receives train detection power (N/-) from sections 244BT, 242BT, A234T and A236T.

**CLASSIFIED**

Figure 3.7: OR-scheme zoom part I RK16 Gouda.

**CLASSIFIED**

Figure 3.8: OR-scheme zoom part II RK16 Gouda.

As can be noted, the (upstream) elements of a 'power supply disturbed' notification is a visceral, branched system, and it contains many different elements on various locations. The above-outlined structure is only one branch of the system. Twenty-two relay boxes 'under' RH10 Gouda remain, along with and many sections, switches and signals, for example underneath those relay boxes. All are connected with each other and receive their power from different sources. If only one element breaks down in the whole 'tree' under RH10 Gouda, the same 'power supply disturbed' notification is generated. When a notification is generated, it can mean that there is no 3kV supply at all, but it can also imply that a 6 ampere CB in RK16 is open.

When a relay box POPR (like the A11/12/34/6/8 - POPR - 15 in Figure 3.4) goes down and the 'power supply disturbed' notification is activated by the GD POPR (Figure 3.4), the 'A11/12/34/6/8 - POPR - 15' simultaneously activates the system to lock all switches for operation. This system is pictured in Figure 3.9.

**CLASSIFIED**

Figure 3.9: System to lock switches for operation in Gouda.

This system was described earlier and makes sure no train can be sent to another track to avoid a collision in case of a short power supply failure. The 20-second time relay is represented as the power on time element relay (POTER), and the physical action of the dispatcher is transferred to the system by the 'IF GD-B/D POPBPR'. If one of the SW components (relay box POPRs) experiences a power disruption, all switches are locked until the power for all SW components is restored.

### 3.5. Fault Tree (FT) 'Power Supply Disturbed' Notification

To identify all possible failure causes which can lead to the notification, an FT was constructed based on several existing cases and theoretical information from the system. The resulting FT can be seen in Figure 3.10.

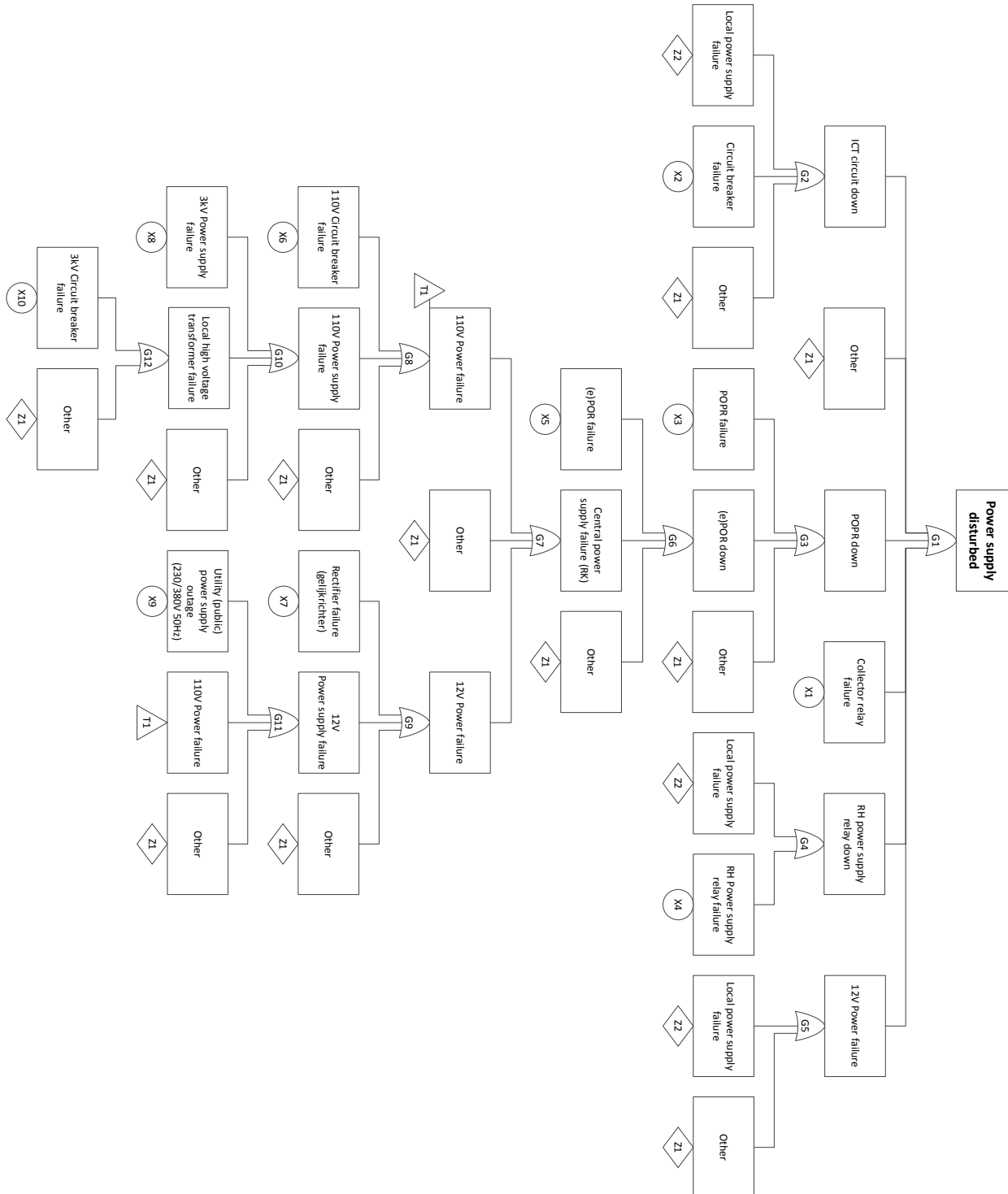


Figure 3.10: Fault Tree (FT): 'Power Supply Disturbed' notification causes.

The starting point for the construction of the FT was the study book 'B-relais stations-beveiliging - NX-systeem "68"' by Railinfra Opleidingen (2011), in which the functioning of the system is extensively described. Following the technical drawings in the book, a first draft of the FT was sketched. Subsequently, the FT was complemented and improved by four randomly picked existing situational drawings, such as shown in Figures 3.4–3.8, based on the actual situation in Alkmaar, Nijmegen, Maastricht and Eindhoven. All example locations were equipped with an EBP master station and an LCE sub-station. These drawings do not clearly indicate where and what cabling is used, how connections are made and what input/output cards (I/O-cards) are used. Therefore connections, cables and I/O-cards are gathered under the undeveloped failure events, 'Other - Z1'. Generally, it is assumed that a failure of such components will look like or be represented similar to a failure event on the same level as a gate event. The undeveloped 'Local power supply failure - Z2' events are all events in which an EV-component fails. Several drawings were checked for an EV-component, but no FT-branch could be developed due to the lack of additional side effects and the in-series elements. For all those components, a back-up power supply is available, and therefore they are not further developed. In some situations the 12V is converted from the 110V, in which case a 110V failure will cause a 12V failure. Therefore, the transfer event '110V Power failure - T1' is added to compress the FT. The whole FT is further developed with reference to educational drawings Railinfra Opleidingen (2011).

Based on the different FMECAs for all components, the effects of failing components, as can be noticed in the data, are shown in Table 3.1. Also, the general location and responsible mechanics are coupled with the effect and shown in Table 3.1, as based on the drawings.

Table 3.1: Notification cause - Side effect - Mechanic expertise.

Event	Effects	Mechanic discipline	Location
G1	Power supply disturbed	EV/SW/ICT	RH
G2	G1 + normal control area + enduring notification	EV/ICT	RH
G3	G1 + switches locked	SW	RH
G4	G1 + No control	EV/SW	RH
G5	G3	SW	RH
G6	G3 + T.O.B.S + fallen signals/no control	SW	RK
G7	G3 + T.O.B.S + fallen signals/no control	SW	RK
G8	G3 + fallen signals/no control	SW	RK
G9	G3 + T.O.B.S + fallen signals/no control	EV/SW	RK
G10	G3 + fallen signals/no control	SW	RK
G11	G3 + T.O.B.S + fallen signals/no control	EV/SW	RK
X1	Power supply disturbed + normal control area + enduring notification	SW	RH/RK
X2	Power supply disturbed + no control/route setting	EV/ICT	RH
X3	Power supply disturbed + switches locked	SW	RH
X4	Power supply disturbed + switches locked	SW	RK
X5	Power supply disturbed + switches locked + T.O.B.S	SW	RK
X6	Power supply disturbed + no control + switches locked + T.O.B.S	SW	RK
X7	Power supply disturbed + no control + switches locked + T.O.B.S	EV	SS
X8	Power supply disturbed + no control + switches locked + T.O.B.S	EV	RH
X9	Power supply disturbed + no control + switches locked + T.O.B.S	EV/SW	RK
Z1	Multiple side effects possible depending on cause	EV/SW	RH/RK/SS
Z2	Multiple side effects possible depending on cause. Check OBI on locale power supply messages	EV/SW	RH



### 3.6. Event Tree (ET) 'Power Supply Disturbed' Notification

As Section 3.5 describes, the causes for a 'power supply disturbed' notification can vary. However, every cause can have side effects, and these side effects are not always the same. Therefore, by mapping these side effects for different causes, the required mechanical expertise can be identified. Also when a particular side effect can be assigned to one specific cause, this identification is easily made. The results of the identification process can be seen in Table 3.1. From these results, questions are formulated to determine the different side effects. After some adaptation and better careful formulation, the side effects in Table 3.1 the ET were reconstructed and can be seen in Figure 3.11.

Initiating Event	Pivotal Events								Outcomes	
Power supply disturbed	Short message? AND Reported once? AND Under control?	Abnormal control area?	Entire control area?	Fallen signal(s)? OR/AND Switch(es) locked?	TOBS(en) visible?	Signal Extinguished? OR/AND Flashing power? OR/AND Switch NIC?	Switch cleared?	3kv power supply failure OBI?	Mechanic discipline	Failure
	Y						Y	Y	PS	X8 - Z2
								N	SW/PS/EV/ICT	Unknown - G3 branch
									SW/PS/EV/ICT	Unknown - G3 branch
									SW/PS/EV/ICT	Unknown
		Y	Y	N					SW/ICT	X-8/9 - Z1
									EV	G-4/5 branch - X2 - Z1
		N				Y		Y	PS	X8 / Z2
								N	EV	G12 branch
									SW	X6 / Z1
									SW	X5 / Z1
	N	Y	Y	N		Y		Y	PS	X8 / Z2
								N	EV	G12 branch
									SW	X6 / Z1
									SW	X3 / X5
		N	N			Y		Y	PS	X8 - Z2
								N	EV	G12
									SW	G9
									SW/ICT	Unknown
		N							EV/ICT	X1 / X2

Figure 3.11: Event tree (ET): 'Power supply disturbed' notification diagnosis by side effects.

### 3.7. Performance

To check the performance of this approach, historical cases are tested and compared with the results of the ET prediction. Based on the known historical information and SAP data, the ET is followed to check whether the right mechanic expertise, location and cause can be identified by the approach.

A frequency table can be constructed to layout the mechanical issue, location and cause for each case, based on historical SAP logs. Only 500 of the 2,000 notifications per year are logged in the SAP database, resulting in substantial bias in the data because it is not known which notifications are logged and which are not. Probably the very short messages are not reported, so one branch of the ET will never be reached. Also, not every SAP item can be used, because a selection needs to be made if the specific area has B-Relay interlocking and an LCE and EBP sub-master station. In many cases, no cause can be identified when the mechanic examines the situation, because the failure has already disappeared by that time. The overall time-savings also cannot be calculated based on the SAP reports. Most time stamps cannot be verified, and possible PCA mistakes often go unreported. Therefore the 'real' added value or time savings cannot be calculated. To further assess the SAP data, many assumptions need to be made, and much interpretations needs to be done. Particularly to arrive at root cause identification, the full ET needs to be completed. Not all needed information is yet logged, and therefore considerable tweaking was needed to produce results. The most likely cause was then selected by the researcher.

Based on SAP items from July 1, 2015, through July 1, 2016, 435 SAP items could be identified. After manual selection, 143 complete and consistent SAP items remained. After a check of whether the master station and sub-station were within the scope, 98 items remained. After checking whether the SAP items' cause could be correctly recorded, 82 remained. After another final check, 74 were determined suitable for the approach. The cases were anonymised based on their RVO number. The mechanical issue, location and cause identification of the RVOs and the resulting ET results can be seen in Appendix F, Table F2.

To evaluate the performance of the ET, it was investigated whether the ET predicted the SAP logging for each of the 74 cases. The frequency table of all predictions and SAP logging are shown by mechanical issue in Table 3.2, location in Table 3.3 and cause in Table 3.4. If the ET predicted the SAP outcome, the number of times is represented on the main diagonal; otherwise the number of deviations are presented in the corresponding elements of the table.

Table 3.2: Absolute results by mechanical issue from Event Tree (ET) prediction relative to observed SAP data.

Event Tree	SAP	
	EV	SW
EV	54	3
SW	-	17

Table 3.3: Absolute results by location from Event Tree (ET) prediction relative to observed SAP data.

Event Tree	SAP		
	RK	RH	Other
RK	13	1	1
RH	-	36	23
Other	-	-	-

Table 3.4: Absolute results by cause from Event Tree (ET) prediction relative to observed SAP data.

Event Tree	SAP						
	X1	X2	X5	X6	X8	Z1	Z2
X1	0	-	-	-	-	-	-
X2	-	2	-	-	-	2	-
X5	-	-	4	-	-	3	1
X6	-	-	-	4	-	-	-
X8	-	-	-	-	1	-	-
Z1	-	-	-	-	-	0	-
Z2	-	-	-	-	2	1	54

Based on the absolute number, the ET predicts the right mechanical issue in 96% of cases. The location is predicted right in 66% of cases, and the cause in 88%.

Some deviation can be seen between the outcome of the ET and the SAP logs. In this research, connectors and cables are specified only as ‘Other’ causes. Locations and usage of cables differ and are not specified or even unknown. The evaluation showed that in a number of cases, a broken cable was the cause of the failure. This cause is difficult to trace and can only be tracked by the side effects of the specific branch and level of the FT. If a component failure is ruled out, all cables must be measured. A cable failure is considered a secondary option; therefore Table 3.3 shows many wrong predictions because the ‘other’ location cannot be reached by the model. The ‘Z2’ failure is most frequent cause identified by the model and in the SAP data. Unfortunately, the exact cause cannot be further identified by this model. Fortunately, however, all possible causes can be fixed by EV mechanics, and all are located within the RH, so the model can still be used for those failures.

To check whether the performance of the ET holds statistically, a goodness of fit test was performed. A goodness of fit test describes how well the model fits a set of observations. Measures of goodness of fit typically summarise the discrepancy between observed values and the values expected under the model in question. Such measures can be used to test whether outcome frequencies follow a specified distribution. Based on ‘Data, Modeling & Decision Making’ by Verhaeghe (2007), a Pearson’s chi-square ( $\chi^2$ ) test was performed to test the performance. The test compares groups with a nominal measuring scale for independences where no information on the strength of the relationship or the direction is provided. Based on the squared differences between observed frequencies and expected frequencies, the fitness of the approach can be checked.

The Pearson’s chi-square test could be performed based on the same frequency table as constructed earlier (as can be seen in Appendix F Table F.2). Testing the approach was also performed in three phases: first, the mechanical discipline, then the location, and finally root cause. Therefore three hypothesis were tested.

1. *Is there a significant difference between the observed disciplines and the mechanical issues predicted by the model?*
2. *Is there a significant difference between the observed location and the locations predicted by the model?*
3. *Is there a significant difference between the observed cause and the cause predicted by the model?*

In which,

$H_0$  The distribution criteria are statistically independent

$H_A$  The distribution criteria are not statistically independent

The null hypothesis assumes that there is no statistical relationship. If  $H_0$  is rejected, then there is a statistical relationship.

The formula for the Pearson's chi-square is as follows:

$$\chi^2 = \sum_{i=1}^r \frac{(O_i - E_i)^2}{E_i} \quad (3.1)$$

Where:

$\chi^2$  test statistic

$O_i$  observed frequencies of cell  $i$  (event) from the historical SAP data

$E_i$  expected frequencies of cell  $i$  (event) from the ET simulation

$\sum_{i=1}^r$  summation over all cells (row  $i$ ).

The null-hypothesis is to be rejected, and the approach is valid, if  $\chi^2 \geq \chi_c^2$  where  $\chi_c^2$  is the critical predefined criteria based on the level of confidence and the degree of freedom. If  $0 \leq \chi^2 < \chi_c^2$ , the  $H_0$  will not be rejected, and the approach is not statistical valid.

Table 3.5: Mechanical issue test based on Table F2.

	Observed	Event Tree	$O - E$	$(O - E)^2$	$(O - E)^2 / E$
EV	57	60	-3	9	0.15
SW	17	13	4	16	1.23
$\chi^2 = \sum (O - E)^2 / E$	74	73			1.38
Degree of freedom (D.f) =					$(2 - 1) \times (2 - 1) = 1$
$\chi_C^2 =$					3.84

Table 3.6: Location test based on Table F2.

	Observed	Event Tree	$O - E$	$(O - E)^2$	$(O - E)^2 / E$
RH	37	59	-22	484	8.20
RK	13	15	-2	4	0.27
Other	24	0	24	576	
$\chi^2 = \sum (O - E)^2 / E$					8.47
Degree of freedom (D.f) =					$(2 - 1) \times (2 - 1) = 1$
$\chi_C^2 =$					3.84

Table 3.7: Cause test based on Table F2.

	Observed	Event Tree	$O - E$	$(O - E)^2$	$(O - E)^2 / E$
X1	0	0	0	0	
X2	1	4	-3	9	2.25
X3	0	0	0	0	
X4	0	0	0	0	
X5	4	8	-4	16	2
X6	4	4	0	0	0
X7	0	0	0	0	
X8	3	1	2	4	4
X9	0	0	0	0	
Z1	6	0	6	36	
Z2	54	57	-3	9	0.15
$\chi^2 = \sum (O - E)^2 / E$					8.41
Degree of freedom (D.f) =					$(5 - 1) \times (2 - 1) = 4$
$\chi_C^2 =$					9.49



With a confidence 95% level, the results are shown in Table 3.8.

Table 3.8: Pearson's Chi-squared test 'power supply disturbed' notification diagnosis.

	$\chi^2$	$\chi^2_c$	$H_0$
Hypothesis 1: Mechanic discipline	1.38	3.84	True
Hypothesis 2: Cause location	8.47	3.84	Rejected
Hypothesis 3: Root cause	8.41	9.49	True

This research was initiated by two major disruptions which precipitated the 'power supply disturbed' notification as an initial failure notification. Both cases were tested with the approach, and both had the correct cause specified by the ET.

Yet it is debatable whether the Pearson's chi-square is the right method, or whether the approach can be validated at all. Since there is no better alternative, the Pearson's chi-square method was used for this research in order to try to test the approach. The chi-square test has the downside that the value of  $\chi^2$  is influenced by the number of cells of the contingency table and the number of observations (n). When there are more cells, more numbers are added up. And when the number of observations increases, the  $\chi^2$  also increases, because the values of the numerator are squared, and those of the denominator are not.

### 3.8. Conclusion

To conclude, for the 'power supply disturbed' notification, it could be useful to obtain and communicate additional information in some situations. Based on duration and effect, or the lack of impact, the appropriate mechanic could be sent to the failure area. In the case of an SW failure, providing additional information can possibly yield even more gains. Unfortunately, the problem does not always originate with a component failure, as described in Section 3.7. Often, when it is an SW failure, a third party has caused the failure, where, for example cables are effected, and therefore the ET could not be entirely completed, and the specific cause could be found. When the information is interpreted correctly, nevertheless, a better understanding of the location or cause of the failure might yet be achieved. As stated earlier, aside from a complete loss of power, SW failures have the biggest effect on the availability of the track.

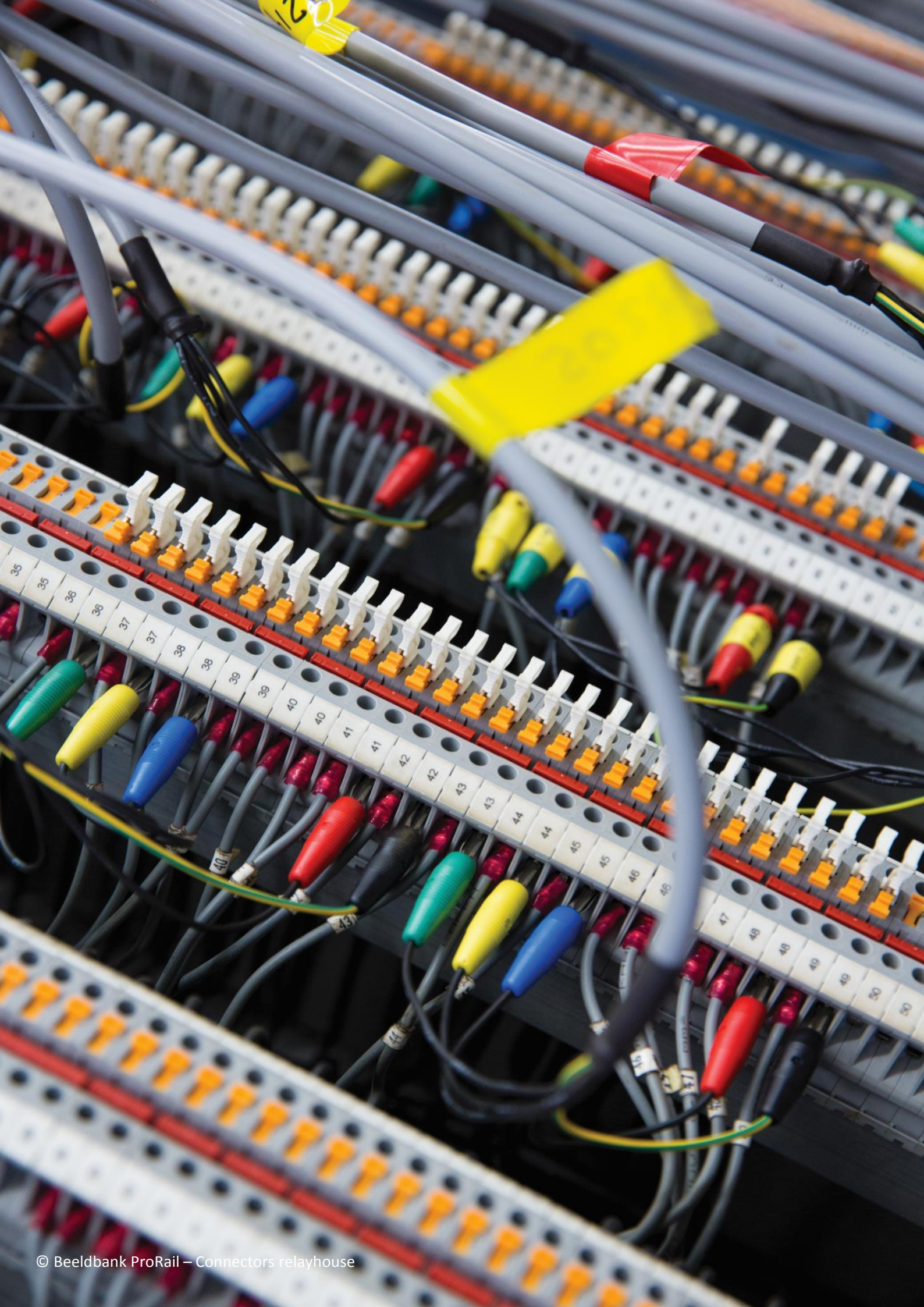
When the train service is effected, there are three cases are of particular interest:

1. A 3kV power disruption.
  - All control system are effected.
  - T.O.B.S. are visible.
  - Switches are out of control.
  - Switches are locked.
  - Signals are fallen or extinguished.
2. An ePOR failure.
  - Switches are locked for operation.
  - Signals are fallen.
  - No further side effects present.
3. A 110V circuit breaker failure.
  - T.O.B.S. are visible.
  - Signals are fallen.
  - Switches are locked for operation.

When a 3kV power disruption occurs, this circumstance is known by the OBI operator, and a specific approach to solve the problem is already present. When an ePOR failure occurs, the specific location cannot be determined beforehand. The EV mechanic needs to check which POPR is down in the RH and then, systematically, all related RKs need to be checked to determined which ePOR failed. When a 110V circuit breaker fails, the corresponding OR-scheme for the area needs to be checked. A corresponding factor (RK) to all T.O.B.S. notifications should be found, after which the mechanic can be sent to the specific RK.

Statistically, the approach cannot be validated. The SAP data of mechanic issues is of inferior quality: the data is inconsistent and often wrong. To be able to test the location based on the SAP data, another problem arises, the 'other' location cannot be selected in the approach, because a cable's location cannot be determined and is described by the approach as another cause and not as a primary failure. Since in real life, it often is the primary cause, the wrong location is selected. In such a case, the statistical test is valid, but the wrong location was selected, and therefore the model is incorrect and considered invalid. For the cause test, many causes could not be assessed because only lasting failures are noted with a cause in the SAP database. Therefore, various causes cannot be reached due to a lack of information, and all EV-component failures are considered Z2 and are not specified. The statistical validation should be performed again when the SAP data and all information needed is available after a test or implementation. Despite that the approach cannot be statically validated, the constructed FT and ET can contribute to the objective of this research: to achieve a reduction in downtime during a disruption, for several specific cases.







## Discussion and Implementation

This chapter discusses the results (Section 4.1) and details how the methodology, and the test case in particular, can be implemented. Section 4.2 outlines the possibilities for gathering useful data, and Section 4.3 considers the process implementation possibilities. Section 4.4 discusses a broader context.

### 4.1. Results Discussion

The results of the test case are promising for some cases. This notification is generated around 2,000 times a year, of which 35 result in a train service disruption. In total, 1,318 trains were effected in 2015, leading to 54,000 train delay minutes. In the past year, two disruptions were indicated as very large and were researched by ProRail. The impact has the potential to be quite substantial. Out of the 2,000 items, 35 are classified scenarios. Therefore, for 35 cases, the model can perform at the highest level and a root cause might be identified with use of the model. Subsequently, the PCA should also consider how to solve the problem to gain an advantage from the model. Unfortunately, the recent year showed that such disruption could happen twice in a high-impact location. Apparently, it is still needed to secure this process and to make everyone aware (again) of the possible impact of this kind of failure.

The test case was performed on theoretical data for conventional B-Relay interlocking (NX'89) with an EBP master station and LCE substation, the most frequently used system in the Netherlands. The usage on other master stations systems (KBV, EBS, etc.), sub-station systems (DOSS, etc.), safety systems (IXL-relay, etc.) and combined sub-station/safety systems (VPI, PLC) cannot be guaranteed. This lack of certainty arises because for some newer systems, more specific notifications are realised, and some systems no longer rely on relay interlocking but are computerised. Only the general rule—if train services are disturbed, send an SW mechanic, except when all power is down—can probably be applied to all. Specific details are needed to assess carefully whether they hold for all systems.

Since the test case is based on a general system, and all systems installed in the Netherlands are different, the specifics for each control area will differ. Therefore, expert judgement of the responsible mechanic or second line management of ProRail is still needed to verify the information for the specific location. If a failure notification occurs, the specific technical drawings must be checked, as mentioned in Section 3.4. Due to the lack of digitalisation of the information on the drawings, it was not possible for this study to fully automate the failure assessment based on the operational data and element relations.

The cause can in some cases be obvious, due to, for example, the combination of major



excavation work along the track and the ‘power supply disturbed’ notification. Technically, the failure is then caused by a third party (not a technical cause), for which Pro-Rail cannot be held responsible. Still, it disturbs train services and should be avoided and repaired as quickly as possible. A connector and I/O-card failure could cause the problem. The high reliability of those I/O-cards make it unlikely to be the cause, but occasionally this could be the case, and such a contingency should be checked as a last resort when all other avenues fail.

When a 3kV-circuit breaker causes a power supply disruption, the root cause is most likely a short circuit in an SW component. In that case, the SW mechanic should be sent to the failure location, because the train services are disturbed. But the SW mechanic can (due to regulations) change the 3kV-circuit breaker only once, since it is the responsibility of the EV mechanic. Therefore, if this rule is observed by the SW-mechanic, the EV-mechanic needs to assist when needed, because it is unlikely that the SW-mechanic will find the short circuit causing the 3kV-circuit breaker to switch without power on the system. The assistance of the EV-mechanic, in other words, might help to avoid further delay.

This research focusses on finding the failing component: what needs to be fixed or replaced in order to resume, or continue the train services. The underlying reasons that the component fails are kept out of the scope of the research, as these do not (directly) influence the failure-recovery time. When it comes to failure prediction, the identification of the failing component is a key indicator for in predicting a failure. During the research, some suggestions for indicators found arose that could be researched more closely to enhance failure prediction. In the examination of the SAP logs, a large amount of ‘in examination nothing found’ was indicated. These comments are added by the PCA when they sent to the location after a ‘power supply disturbed’ notification, but when they arrived, the notification disappeared. To be sure, they examine ‘some things’, and they do not find anything out of the ordinary. Unfortunately, what they have examined is not often stated. It is unlikely that the PCA has checked all the components, though, because of the scattered and comprehensive network of elements. It may also be that the failure is time dependent, so if there are two switches operated at the same time, nothing is happening, but when three are switched at the same time, a circuit breaker or relay almost fails, but when the operation is done it can return to a normal state. The relays are set to a certain level, but these settings can be worn over time. All of these possibilities can signal an upcoming failure with a higher impact. The constructed EV can also give an indication of where the mechanics need to measure a particular setting to help predict an upcoming failure. For this more targeted examination to be implemented, further research is required, because this topic could not be fully attended to here, and no more than indications to be pursued in future have been noted.

Due to the lack of expert judgement, high-quality historical information or a test environment, the approach could not be validated. The results of the statistical test cannot be simply assumed to be correct. A number assumptions were needed, and many data needed to be removed from the sample. The sample for one year was, therefore, biased, and it very likely presents an incorrect representation of the situation. Besides the inferior data, the approach assumes cable issues are a secondary cause which can be researched after the system components are checked. Therefore, a cable can never be the first outcome named in the ET, so cannot be reached by the ET. In addition, the Pearson’s chi-square test interpreted another finding by the model then the SAP item as a good thing, because then it is not luck but really different. For the approach to be correct it must be the same, and this also contradicts to the Pearson’s chi-square test. Despite that the validity cannot be checked, the approach was tested on theoretical data for the two main cases which led to this research, and the approach gave the right conclusions.

Altogether the results are useful and present added value for some cases. This value is more pronounced in light of the fact that the CEO of ProRail, Pier Eringa, again, stated in the 'Algemeen Dagblad' of 18 October 2016, that ProRail has the goal to prevent disruptions by better and preventive maintenance, but if a disruption or failure occurs it needs to be fixed as fast as possible (or, in Dutch, '*Voorkom storingen door beter onderhoud en als ze er zijn, zorg dan als de sodemieter dat ze opgelost worden.*') (Voermans, 2016). Thus, this research will contribute to his and ProRail's desire to fix problems as efficiently as possible.

## 4.2. Data Collection

As specified in Section 2.3, various operational data and information sources are available. All various sources collect different data, and all are presented in another way or presented at different places, resulting in a fragmented and chaotic pile of data. The lack of a combined unified repository makes it difficult to automate the collection and assess useful data. Similarly, due to the lack of a digital overview of component relationships, it is not possible to automatically determine the effect of one component failure on the system. In particular, a visual representation would be useful, but is impossible, with the consequence that the failure analysis is more complex. In addition to these difficulties is the lack of data. Most preferably, the status of all assets would be available; unfortunately, this option has only recently developed and is not yet integrated into the existing rail system. In sum, at the moment it is unrealistic to fully automate the collection of data, so the analysis of a failure cannot be automated within the proposed time frame.

If the approach is introduced in an operational context, the data-collection must be performed manually. For the test case of the 'power supply disturbed' notification, the information could be collected this way. All preferred information is present on the operating screen of the dispatcher. Unfortunately, this screen cannot be viewed elsewhere because of security and privacy regulations. Some information on the screen can be displayed in almost real time at the OBI or OCCR, however. Therefore an application called 'VIEW' can be used or the TROTS data logs can be loaded into the 'TOON' application. To be able to access the TROTS data logs in near real time, a procedure needs to be completed where a higher-level manager needs to approve the flush of this data. This can be done in exceptional situations where the motivating and added value of this approval can be shown. The 'VIEW' application is easier to access but does not display all information needed, and only a 'live' image is displayed, so temporary effects cannot be recovered. With the TROTS data logging and TOON, the situation can be replayed, but it does not contain all information as described in Section 2.3, and not all proposed questions can be answered through its use.

To gain all information as easily and quickly as possible, the 'old-fashioned' way of calling the dispatcher is preferable. Fortunately, the dispatcher already calls the OBI operator to report the 'power supply disturbed' notification. When this call is made the dispatchers have to provide all information needed to get the whole picture of the failure. The OBI operator has to ask control questions to be sure all and correct information is reported. In this way, the information can be simply, quickly, inexpensively and efficiently obtained.

### 4.3. Process Implementation

As mentioned earlier, ProRail is responsible only for managing the railway system. Nevertheless, ProRail will make every effort to get a fault repaired as quickly as possible. A part of that task is to pro-actively support problem solving. As such, an important part is to provide the contractor the right information regarding the failure. The better this information, the faster the cause is found and the failure repaired. ProRail has a number of data sources that are unavailable for contractors, as described in the previous section.

The current process for failure recovery is, in principle, appropriate to accommodate the proposed modifications for extra information transfer between ProRail and the PCA. The SAP application provides much freedom to clarify a failure. Since the SAP item is sent to the PCA, they can immediately see the extra information. In addition, it is necessary that the SAP item is connected to the right element and that the element is linked to the right mechanic. Second-line management, inspectors, directors, route teams, dispatchers and OBI operators need to be informed of the proposed approach and informed of why it is important, followed by securing the improved approach in the different operational instructions and manuals. The process must be monitored and, where necessary, strengthened and improved to ensure that it is used and its value is maintained. The proposed approach should be evaluated with the PCAs to validate its practical utility. Afterward, new information should be shared with the contractors in the RVO, so they know that they can ask for this information when it is unfortunately missing. In principle, mechanics are well trained to fix the different failures. However, some failures exceed a single field of mechanical expertise, in which case experience from another field is needed to assess the underlying cause of the failure. This cannot be instantly expected of each mechanic; therefore it is necessary to study how cross-system failures are treated in training and how interdisciplinary failures, like the ‘power supply disturbed’ notification, fit in. In sum, it seems that the proposed process adjustment (as displayed in Figure 4.1) could be introduced without much challenge.

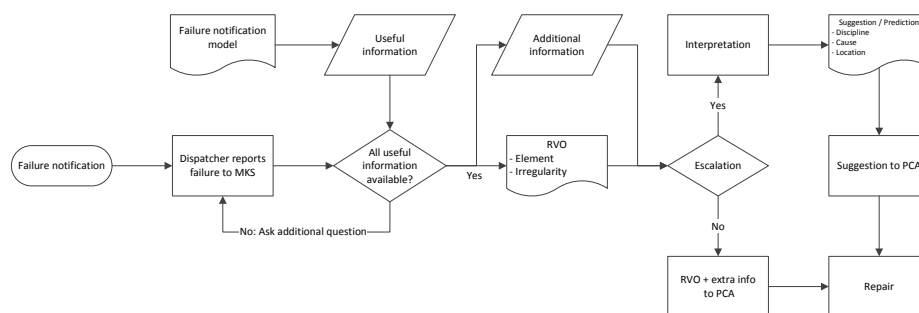


Figure 4.1: Proposed information stream between ProRail and PCA.

In addition to the realistic and direct implementation of the test case, a vision will be given in the discussion section of the trends and future procedures within ProRail for the specific case and the wider perspective of the failure-recovery process.

The proposed method should be applied to other failure notifications for further practical implementation. In further research, the possibility of placing sensors should also be considered, by which other useful information might be obtained. The PCA should be involved in a follow-up study to make sure all potentially useful information is gained and used in practice. For the ‘power supply disturbed’ notification, a manual in ProRail style has been written for implementation in the current processes. This manual can be found in Appendix G.

### 4.3.1. Usability Discussion

As mentioned earlier, the value of the model depends on the information available. As with many usages of data, trash in equals trash out. Seeing that is the case, the information should be correct and complete in order to be useful. If not, the wrong conclusions might be drawn, meaning that finding and fixing the failure takes longer than necessary. Unfortunately, it is not yet possible to automatically transmit the information from the source to the PCA. Since this data still needs to be passed manually by phone, from dispatcher to the OBI operator, incorrect information can be communicated. A clear call discipline where things are repeated for an extra check of the information could mitigate such mistakes.

The PCA should also be involved in the implementation of the modified process of adding extra information to the RVO, since this study researches only one part of what ProRail could do to shorten failure-recovery time. For the extra information to be used by the contractor, another check is needed together with the PCA to consider how they can use the additional information. The PCA must realise that this investigation will contribute to their cause as well. It implies that mechanics must be instructed on how the additional information will help them to perform their job and how they should deal with it. If this implementation does not take place, the effects of the additional information will be minimal and useful only for very high-impact disruptions when senior (ProRail) management or inspectors are involved and make a suggestion to the PCA about what they can do to fix the problem. In most cases, the first 45 minutes have already passed by then, and valuable time is lost in order to do it right at the first time. Even then, the method can still ensure that the worst is prevented.

ProRail should also inform and educate all layers of their organisation in order to successfully implement the proposed method and processes. All should be aware what they should do and why it is so important that they do so, to ensure that it will actually happen. To guarantee the effective use of the process, the process should also be monitored, and if it falters someone has to intervene to improve it, keeping it up to date, useful and used.

This research tested the method for only one failure notification as a proof of concept. The method could be useful for other unclear failure notifications. Most failure notifications are not specific to a single component but a failing element, such as a level-crossing failure. The 'level crossing' (element) sends out a failure notification, but it is unclear whether the bells (component) do not work or the barriers (component) do not close any more. For this kind of notifications, it could be helpful to perform an FTA and ETA. Some obvious or common failure notifications that can be examined for this purpose are:

- (multiple) level crossing failure(s),
- switch out of control,
- *ten onrechte bezet spoor* [improperly occupied track] (T.O.B.S.), and
- route setting failed.

Specific failures can be assessed where different kinds of mechanics can be involved: for example, 'normal' failure notification around engineering constructions like bridges or tunnels. As for the 'power supply disturbed' notification, the discipline designation contributes largely to the failure-recovery time.



## 4.4. Broader Context Discussion

This section highlights some developments, influencing factors, and a vision for the future beyond the scope of this research.

A recent development is that the 'power supply disturbed' notification will no longer be shown in the operating screen of the dispatcher, but will be shown in operating screen of the OBI operator, since many of the 'power supply disturbed' notifications do not influence train operation directly, as has been noted in Section 3.3. If an EV component fails, train service can be operated for several hours and nothings else happens, so this can look like a false notification for the dispatcher. However, the dispatcher needs to inform the OBI operator about the notification, and just passing on notification is not one of the core tasks of a dispatcher. To avoid reporting fatigue, this notification will be removed from the dispatcher's operating screen. At first, this move seems logical, but the 'power supply disturbed' notification is two-fold. It is also the reminder for the dispatcher that after the power supply has been intermittent, whether the whole operating area is still safe to continue must be checked. When the dispatcher is no longer notified if a disturbed power supply, he loses the ability to perform the check based on the notification. As far as this research has studied the system of the 'power supply disturbed' notification, for an EBP master station with a LCE sub-station and B-relay (NX'89 ) interlocking, this notification is in some ways crucial for safety after a short power supply interruption. Switches will be locked as well, but this locking is a side effect of the 'power supply disturbed' notification and is not reported as if it was a notification. Therefore, only the effect is visible, but the reason why is absent. The SW components of the 'power supply disturbed' notification and the notification itself are therefore crucial to the situational awareness of the dispatcher and therefore to railway safety.

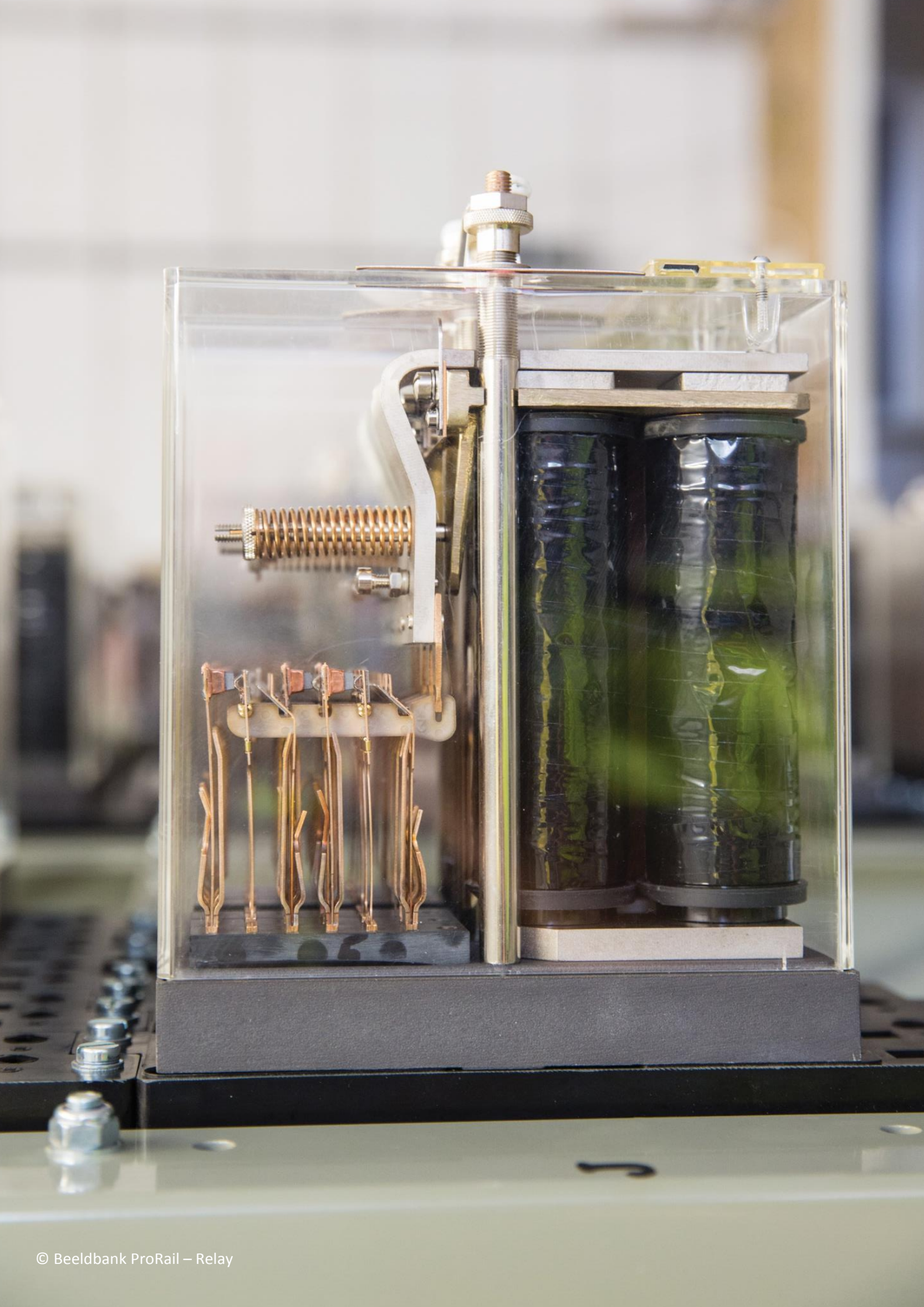
It is desirable that everyone focusses on their core business, and it is debatable whether passing on messages is a task for the dispatcher. Reporting fatigue needs to be avoided where possible, and false positives must also be avoided. To address both of these needs, another solution should be found. Disconnecting the SW components from the ICT and EV components could be an option. Then one input to the LCE and one collector relay is needed, and the ICT configuration needs to be changed. The financial impact and secondary effects cannot be immediately and completely overlooked, but this solution could provide a way to adapt this change quickly and with minimal impact. Nevertheless, the impact should be examined and needs further research.

The OBI operators are assigned to all technical failure intakes. This responsibility has grown, and all operators are doing their best to fulfil this task as best they can. Their main task is still to switch and control the EV elements of the railway system, as described in Section 2.2.1, and the failure intake is a side job. Therefore a special unit within the OCCR, the MKS call centre, will perform all the failure intakes starting in mid-2017, from emergency services, third parties and technical failures. The MKS will be the call centre from which the appropriate mechanics are called for. Those people are not trained to assess technical or other disruptions; they are only trained to pass this information on to the right people. They fully rely on the information as provided, supported by a tool called 'Sporweb' in which scenarios are predefined so they know how to act. The MKS operators are supported by technically skilled people (CHI-team) when needed. Unfortunately, not even to most experienced person knows everything about every component failure. The predefined scenarios are not developed for technical failures, only for the processes on how to act in a certain kind of disruption. It could be further researched to what extent technical failures could be generalised within 'Sporweb' by the CHI-team, to support the MKS operators in asking the right questions for every (technical) failure in every failure intake, regardless the experience of the person.

Ideally, a failure is assessed automatically, with human errors excluded, and specific

knowledge can be secured by a pre-generated system. During the research, however, it became clear that in the current state of technology and information within ProRail this cannot be accomplished. In the current system, only drawings are digitally available. The drawings are specified for the specific mechanics in which no active system links are present. As Hardin and Hardin & McCool (2015) describe, building information modelling (BIM) could be a way to take the step to a digital rail infrastructure visualisation, in which an xD model could be a way to fully integrate all components needed in the rail infrastructure. An 8D model is described by Kamardeen (2010) and combines 3D(dimensions), X;Y;Z, in which the geographical elements and components are visualised, and 5D(omains): time, costs, sustainability, maintenance and prevention through design. There is not yet an application known of such an 8D model in railways, but useful elements to build, maintain, manage and operate a railway system could be implemented in such a model. The 8D model can then contain information about operational details which are not now accessible. Element relations across disciplines and common cause failure could be more easily assessed. It can also be examined whether failures could be predicted within the system using the right conditions and pre-calculated or real-time calculated requirements. For now, this is not possible, but perhaps in the future it will be, and its possibilities can be further researched.

During the evaluation phase for the test case, it became clear that ProRail's AM business structure is extremely divided. Every employee has their own (specifically) defined responsibilities for a specific component. All components also have dedicated employees who manage policy, function, development and conservation. All tasks are performed by highly specialised and skilled people. By this specialist approach, the system philosophy of the bigger picture is sometimes lost. This characteristic was revealed by the examination of the 'power supply disturbed' notification. For this notification, several varieties of specialist within ProRail are involved. But none of them had the complete picture of the functioning of this problem and component-transcending system notification. Therefore, it was impossible to let a system expert check the model because there was not a system expert who could oversee the full effect and functioning of it. All employees of ProRail's AM department are working hard to manage a safe and reliable railway network, now and in the future, but further research could be performed to examine whether the specialist approach is best for the system as a whole.



# 5

## Conclusions and Recommendations

The previous chapters have described the process of asset-failure recovery on the Dutch railway network. Additional information sources are presented by which, if they are used, the failure-recovery time could be reduced. This chapter contains the conclusions of this research, describes its scientific implications, gives its recommendations and reflects on the research. Section 5.1 contains the main conclusions of this study, answering the research questions. The answers to the research questions and underlying assumptions are then discussed in Section 5.2, together with the recommendations for ProRail and further research. Finally, the research is reflected on in Section 5.4.

### 5.1. Conclusions

For this study, the following research question has been formulated:

*How can the use of more and better information contribute to the identification and isolation of the nature, cause and location of a failure of an infrastructure element based on a PRL failure notification in order to achieve a reduction in downtime and a higher availability?*

To answer this question, several sub-questions were deduced from the main question. The sub-questions will be answered in Section 5.1.1, after which the main research question is answered. The answers to the component questions that underlie the sub-questions can be found in the relevant, section as shown in Figure 1.8, and are integrated into the answers to the sub-question.

#### 5.1.1. Sub Questions Answers

*1. How does the ProRail disruption process (from original timetable to first train, after repair) work, and how does it relate to the different track-side elements?*

ProRail is, overall, responsible for the railway system in the Netherlands. Maintenance and repair of the system (i.e. its areas) is outsourced to different sub-contractors (PCAs). If an asset failure occurs and it has an impact on train services, this is usually reported by the dispatcher to the OBI operator. It could also be that failure notifications are directly reported to the OBI operator by various systems or by other (third) parties to the MKS call centre. In whatever way the notification is received, the OBI operator creates an RVO in a SAP item. The RVO consists of a general location or route section, the failed (general) asset or element, a brief description of the irregularity and a description of the resulting effects. In addition, the RVO is linked to a specific object, element, or

component in the SAP database. For every object, element, or component, a specific mechanical discipline is assigned. The SAP item is automatically sent to the responsible PCA. Based on this information, the PCA sends the responsible technician to the specified location.

The assets can be split up into roughly five different kinds: EV, SW, KW, track and ICT. All have their own skilled mechanics. They are trained to find and fix a failure and maintain the different objects and components of it. Assets can fail in different ways, abruptly or intermittently, depending on the cause. The different failure modes for all components and their effect are described in an FMECA. When the mechanic is on site, the trains (for that area) are stopped for safety reasons (if that was not already the case, due to the failure itself). Then the mechanic can start her repair process. When a mechanic locates the cause of the failure, she tries to fix the problem or temporarily mitigates the effects, anticipating later resolution. After the repair is performed, the track becomes available for operation again, and the train services can be restarted.

### *2. What theoretical and real-time data can be linked to a disruption or an asset failure?*

Various sources are available that can be linked to a disruption or asset failure. Theoretical information about how elements are connected and which components are present can be derived from technical drawings and outline drawings. Failure modes and effects are mentioned in the FMECAs. In addition, all components have a product specification and specialised engineers who have extensive knowledge about the functioning of a particular component.

Besides the theoretical (static) data, there are also numerous real-time operational data sources. These can be divided into three different fields: command data, in which the commands for route settings for trains by the dispatcher are logged; control data, in which the status reports for various (controllable or active) elements is logged; and operational status logs, in which the locations of trains are stored (i.e. TROTS). From these three main sources irregularities are derived, which result in failure notifications presented to the user or responsible operator.

### *3. How can the qualitative risks of a system failure be assessed?*

To assess how a component failure can lead to a general failure notification, a system and retrospective method is needed, instead of one centred on a single component failure. One needs to know what component failures can lead to which failure notifications and to which effects. By combining two qualitative risks methods, this can be achieved. Analysing the system using a FTA is a systematic way to identify all components, which can lead to a specific event. If the effects of a single component failure are examined, the effects and component failures can be combined in an ETA. In a resulting ET, a cause can be linked to a specific event by passing a binary flow chart based on yes-or-no answers to indicative questions.

### *4. How can a qualitative risk assessment be applied?*

A test case is performed to check how the qualitative risk assessment can be applied. Owing to the lack of existing FTs and ETs or a system failure analysis, a test case was examined in this research. For example, the 'power supply distributed' notification was assessed. The FT was constructed based on static data and information. The implementation of the power supply monitoring system differs for every location in the Netherlands; therefore a general FT was constructed within the scope of the research. Components were systematically inventoried and assessed according several manuals, drawings and FMECAs. This process resulted in several observed side effects when certain components fail. Based on those side effects, questions are formulated that can



result in identifying the root cause. All input was combined, and an ET was constructed based on the assessment. The constructed ET was, where possible, tested with several historical cases. Overall, the method could help in identifying the right mechanics. For several cases, a very specific component could be designated, which caused the notification to be generated. When additional location information of the failing component is communicated to the PCA, they could bring a spare part and drive directly to the right location.

*5. How can a qualitative risk assessment be implemented in the disruption process, to use its full potential?*

In order to use the approach to its full potential, several adaptations to the current process are needed. The first step is to assess (all) failure notifications by the proposed method. Based on the outcomes, individual implementation plans need to be made. For different failure possibilities, other information is needed, and therefore they require another approach.

For the test case, implementation has less impact. When the dispatcher informs the OBI operator of the 'power supply disturbed' notification on the operating screen, the side effects must also be specifically mentioned. The OBI operator needs to be sure whether the notification was short or is still present; whether the whole or partial control area of the dispatcher is effected; whether signals are fallen or switches are locked for operation; whether there are T.O.B.S. notifications in the control area; and whether signals are extinguished or there is flashing power or switches are out of control. The OBI operator also has to check whether the dispatcher has given the command to clear the switches or that there is a large 3kV power supply failure known by the OBI. When the OBI operator has all the answers, they need to be reported in the RVO and SAP. When no side effects are present, that must also be mentioned as well. When OBI operators allocate an element to a SAP item, they need to be sure the right mechanic is linked to the element. When the operator is not able to select the right object or discipline, this selection needs to be adapted. All chain partners (PCA, ProRail, training companies) need to be informed about the results and how they can react. The PCA can inform their personnel and send the right mechanic to the right location with the right spare element. ProRail can check whether the PCA uses all information, and in the case of a high-impact disruption, they can use the ET themselves to support the PCA in its process to fix the problem. Training companies can better train mechanics, so they know better what this failure notification effectively means. If all these recommendations are implemented, it needs to be checked how the method is performing, and it should be adapted if needed.

### 5.1.2. Answer Main Question

*How can the use of more and better information contribute to the identification and isolation of the nature, cause and location of a failure of an infrastructure element based on a PRL failure notification in order to achieve a reduction in downtime and a higher availability?*

For at least one failure notification, it has been shown that the failure cause could be identified faster, and if the PCA is better informed they could send the right mechanic to the right location, by which a reduction in downtime could be achieved. By retrospectively analysing a failure notification and using a system approach instead of a component-based approach, the notification can be assessed more effectively. When an FT is constructed, it can be made visible which components are linked and, if they fail, can trigger a specific failure message. If, subsequently, the individual components are assessed to see what other effects a component failure has, the side effects of the initial failure notification are revealed. By combining and reformulating the side effects

into binary questions, an ET can be constructed, and when followed the appropriate mechanic can be assigned. In specific instances of the test case, it is also possible to identify the specific cause and thereby the location of the failure. By answering the proposed questions, additional information is added to the RVO. To gain the extra information, the dispatcher and the OBI operator should communicate clearly and all questions should always be answered. All codings and names of specific components must be listed correctly. Only then is it possible for the PCA or ProRail to act thoroughly, and additional information can provide added value. When the PCA receives a more specific RVO, it can act in a more effective way by sending the right mechanic immediately, to bring the right spare part and to drive directly to the right location. This sort of targeted response allows the downtime to be reduced for specific cases, up to 1 hour and 45 minutes (ProRail AM Infrabeschikbaarheid, 2016a).

## 5.2. Scientific Implications

This section covers the reflection on the scientific and practical contributions of the study and discusses its methods, results, usability and limitations. Finally, a personal reflection on the research is given.

### 5.2.1. Scientific Contribution

As mentioned, the use of FTs and ETs is not new. Several sectors have been using these methods for years. FTs are mainly used very early in design development to identify safety issues early in the design process (Ericson, 2005). ETs are very powerful to identify and evaluate the system-consequence paths possible after an initiating event occurs. The ET can show the probability of the system design resulting in a safe, degraded or unsafe operational path. For this research, both methods are used in a slightly different and more pragmatic way. For this purpose, previously disclosed (operational) information sources were used to feed the model. Application of this model to the field of railway failure-recovery process presents new study in an unexploited area of research and therefore contributes to the scientific knowledge of the application of the above-mentioned systems.

### 5.2.2. Practical Contribution

Besides its scientific contribution, the research contributes to the practical failure recovery process of ProRail and their PCAs. A better understanding of the 'power supply disturbed' notification is gained by this research. It is shown that the method of FTs and ETs can be used to better assess a failure notification, by which better insight into the root cause of the notification can be gained and the quality of an RVO can be enhanced. By reporting a better specified failure, the PCA can be more thorough in solving the problem. Research-time can be shortened and potential spare parts can be brought by the mechanics. The 'power supply disturbed' notification is generated around 2,000 times per year, of which 35 result in a train service disruption. In total 1,318 trains were effected in 2015, leading to 54,000 train delay minutes. In the past year two disruptions were indicated as very large and were researched by ProRail. Potentially, the impact can be substantial. Given the large size of the network and its elements, a reduction in travel time for the mechanic can also be achieved if the real location of the failing component can be indicated faster. All this will lead to faster failure recovery and greater availability of the tracks, contributing to both the PCAs and ProRail's PIs and to minimising hindrance for TOCs and their clients.

## 5.3. Recommendations

Resulting from the research conclusions and discussion, several recommendations have been formulated. A distinction is made between recommendations for further scientific research in a broader perspective and for ProRail as a company.

### 5.3.1. Recommendations For Further Research

To continue the path of this research, some future directions can be investigated. First, other FTs and ETs can be constructed, and usage with other master stations and sub-stations can be tested by which, the use can be expanded. In addition other useful, now unknown information can be considered, and possibilities can be studied regarding how that information can be obtained: for example, by means of the internet of things applied to the existing system of the Dutch railway network. Also the possibilities and required resources for an automatic failure-assessment based on pre-defined settings can be researched. This research can help to create faster, better and more error-free failure assessments. The automatic failure-assessment can be combined with a xD BIM for the railway system of the Netherlands, applied to failure analysis.

### 5.3.2. Recommendations For ProRail

Aside from further research on the approach for other kinds of master stations, sub-stations and other safety systems, further research can be done on other applications of the proposed approach, such as for example: T.O.B.S., 'switch out of control' and '(multiple) level-crossing failure(s)' notifications. ProRail needs to evaluate the approach with all PCAs. After the evaluation, the approach should be implemented on all levels of ProRail's organisation, by educating all stakeholders—dispatchers, OBI operators, directors, inspectors and higher-level management—of the use and added value of the approach. After implementation, the approach must be secured to see whether it is used and works as it should. When it falters, the approach or education should be adapted so that it continues to add value. To validate the results statistically, the SAP database could be more useful for data analysis, and SAP database elements should be checked to see whether they are linked to the right mechanical discipline.

In addition, ProRail can research the impact of the removal of the 'power supply disturbed' notification in the dispatcher's operating screen on the situational awareness of the dispatcher and railway safety in general. A further study can indicate how the 'power supply disturbed' notification can be split, so that the value of it increases for all stakeholders.

Another avenue of inquiry is to develop a smart failure intake by the MKS with a safeguarded system, whether or not implemented in 'Sporweb', and further digitalisation and combination of technical drawings on a system-based approach.

When this latter area of future research has been sufficiently addressed, the area of failure assessment and the failure-recovery process has the basis to take significant steps forward.

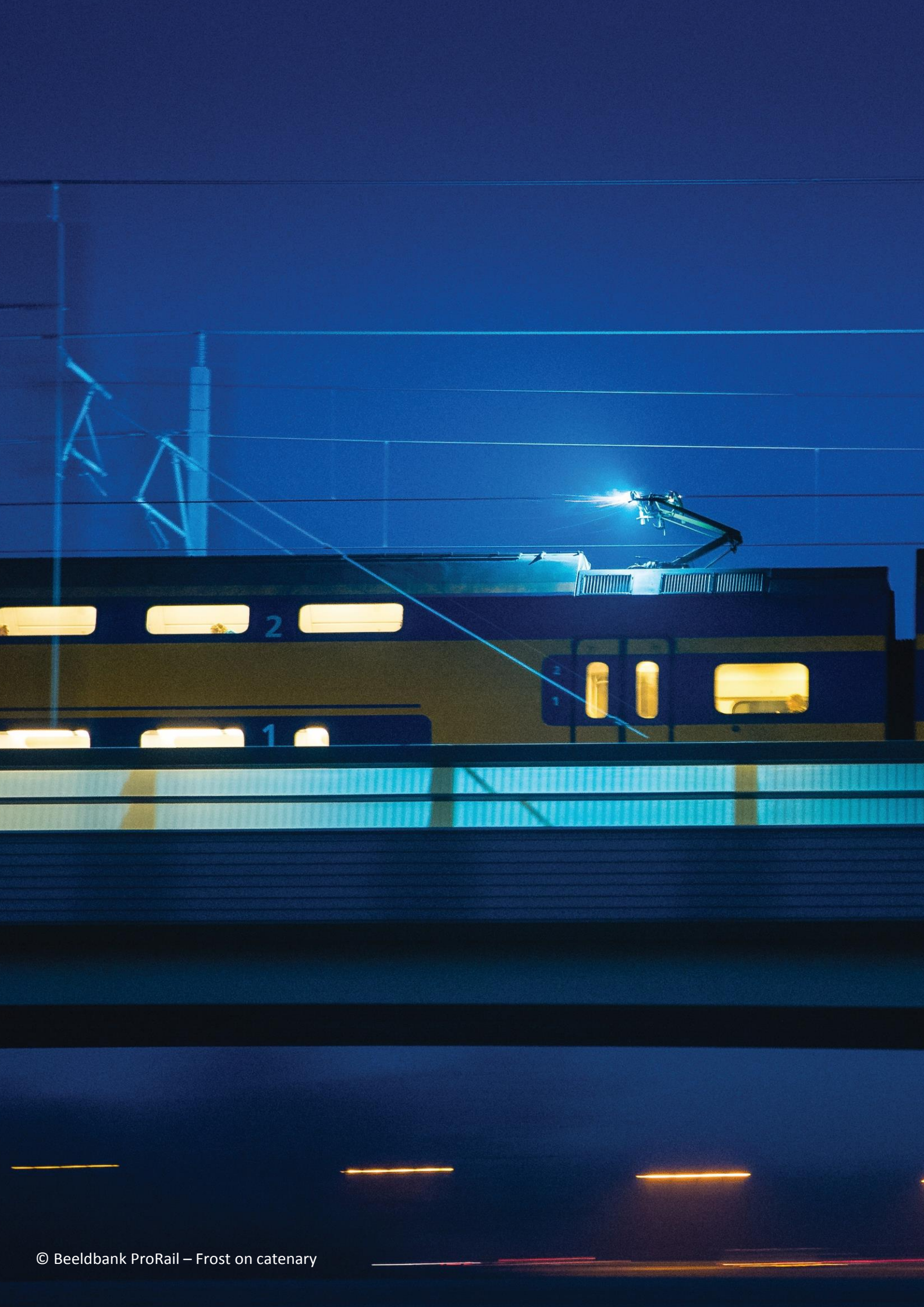
## 5.4. Personal Reflection

When I started this research, the scope was more focussed on automatic assessment of real-time data and failure notification combined with (digital) knowledge on how the system was built-up. To access all data and information sources combined with the experience of the responsible ProRail employees, I chose to work full time at the ProRail office within the OCCR. Partially, this proved to be the right decision; all the failure intakes are performed within the OCCR, but all system knowledge is present at the headquarters. But both are in Utrecht, so I managed to switch between locations quite often.

The first part of the research consisted of a literature review and background research on failure assessment and how it is performed by ProRail for the Dutch railway network. This was more difficult than expected, certainly in the practical and conservative environment of the ProRail office. The state of the digital technology was not as progressive as I thought. ProRail is working on enhancing the digital and data structures within the company, but unfortunately, the current state was not sufficient to base my research on. Also not much in the literature, or present within ProRail, seemed to be applicable for my research topic, so my research was delayed a while. Thanks to my external supervisor, I managed to speak to many different and interesting people, after which I took a step back and reinvestigated what I would like to achieve with this research. Enriched by those conversations, I dug into the cases that were the reason for this research for ProRail. The moment I realised, based on technical drawing, failure notifications and incident reports, what the real problem was, the roller coaster came in motion. Based on several sources, I managed to develop an approach to handle a 'power supply disturbed' notification. It was difficult to check the approach because of the fragmented responsibilities of notification within ProRail. No one seemed to be an expert on the 'power supply disturbed' notification, and many knew a little about it. Also, statistical evidence of the approach could not be calculated due to the lack of data or the poor quality of the data. This was a significant setback during the process. I know that the approach will help, but I could not manage to deliver proof for it. Scientifically, this does not need be a problem, but personally it gives not a complete sense of satisfaction.

Since the realisation a switch was needed, from the new 'big data' to a more 'old-fashion' method, the time flew by. Almost every day I progressed with something new and I became more and more enthusiastic about the approach. Almost half a year went by, and it did not feel that way. It was helpful to know the different deadlines and work towards them; the closer the deadline, the more came to paper. Also, the realisation that I had become 'the' expert on this specific notification was a good motivation. At the same time, it was a setback: why was I the expert instead of someone within ProRail? I realise that it has historically grown in this way and that the PCA is the system expert, while ProRail is in lead of managing it. Therefore, this study could and maybe should be performed from a PCA perspective, because they are (contractually) in the lead. At the same time, they do not know what ProRail has to offer in terms of data and additional information. Therefore, I am very satisfied with the result and, I think, I have contributed in this way to the greater availability of the Dutch rail network.







# References

- Bai, H. (2010). *A generic fault detection and diagnosis approach for pneumatic and electric driven railway assets* (Master thesis). The University of Birmingham.
- Boston Consulting Groep. (2015). *The 2015 european railway performance index*.
- Brinkman, P. (2009). *Valuing rail infrastructure performance in a multi actor context* (Master thesis). Delft University of Technology.
- Ericson, C. A. (2005). *Hazard analysis techniques for system safety*. John Wiley & Sons Inc., Hoboken, New Jersey.
- Ghaemi, N., & Goverde, R. (2015). Review of railway disruption management practice and literature. In *6th international conference on railway operations modelling and analysis, railtokyo2015, narashimo, japan, march 23-26, 2015; authors version*.
- Hansen, I., Wiggenraad, P., & Wolff, J. W. (2012). *Inrichting, gebruik en onderhoud nederlands spoorsysteem internationale vergelijking*. (Letter of government: Kamerstuk 32707 nr. 12)
- Hardin, B., & McCool, D. (2015). *Bim and construction management: proven tools, methods, and workflows*. John Wiley & Sons.
- Infrasite.nl. (2016). *Definities*. Retrieved 2016-12-02, from <http://www.infrasite.nl/definitions/definition.php>
- InTraffic. (2015). *Interface design document - care meldingen*. (Internal product specification)
- InTraffic. (2016). *Software version description procesleiding rijwegen prl 41.2 oplevering v41.2c*. (Internal product specification)
- Isermann, R. (1984). Process fault detection based on modeling and estimation methods—a survey. *Automatica*, 20(4), 387–404.
- Kamardeen, I. (2010). 8d bim modelling tool for accident prevention through design. In *26th annual arcom conference, leeds, association of researchers in construction management* (Vol. 1, pp. 281–289).
- Ministerie van Infrastructuur en Milieu. (2014). *Netwerk nederland, ov op het goede spoor, lange termijn spooragenda deel 2*.
- NS Groep N.V. (2016a). *Geschiedenis van de nederlandse spoorwegen*. Retrieved 2016-08-04, from <http://www.ns.nl/over-ns/geschiedenis-van-ns>
- NS Groep N.V. (2016b). *Jaarverslag 2015*.
- ProRail. (2005). *Instandhoudingsdocument - voeding tbb - deel 1 centrale voeding 3kv* (1st ed.) (No. IHD00008-1). (Internal document)
- ProRail. (2008). *Factsheet: Kenmerkende verschillen opc - pgo*. (Internal document)
- ProRail. (2012a). *Ontwerpvoorschrift - voeding tbb - deel 1 algemeen* (4th ed.) (No. OVS00017-1-V004). (Internal document)
- ProRail. (2012b). *Ontwerpvoorschrift - voeding tbb - deel 2 centrale voeding* (4th ed.) (No. OVS00017-2-V004). (Internal document)

- ProRail. (2012c). *Ontwerpvoorschrift - voeding tbb - deel 3 lokale voeding* (4th ed.) (No. OVS00017-3-V004). (Internal document)
- ProRail. (2012d). *Ontwerpvoorschrift - voeding tbb - deel 4 ontwerphandleiding* (4th ed.) (No. OVS00017-4-V004). (Internal document)
- ProRail. (2013). *Interface design description - trots* (6th ed.) (No. TROTS-AAP-(AAP2.1)-IDD). (Internal document)
- ProRail. (2015a). *Beheerplan 2016*.
- ProRail. (2015b). *Ketenplaat post21 be en bijsturing*.
- ProRail. (2016a). *Instandhoudingsconcept - b-relais ixl* (1st ed.) (No. IHC60201-V001). (Internal document)
- ProRail. (2016b). *Instandhoudingsconcept - laagfrequent spoorstroomlopen (grs)* (3rd ed.) (No. IHC60111-V003). (Internal document)
- ProRail. (2016c). *Instandhoudingsconcept - voeding tbb - centrale voeding* (1st ed.) (No. IHC00011-V001). (Internal document)
- ProRail. (2016d). *Instandhoudingsconcept - voeding tbb - lokale voeding* (No. P1268053). (Internal document)
- ProRail. (2016e). *Instandhoudingsrisico analyse - b-relais ixl* (1st ed.) (No. IRA60201-V001). (Internal document)
- ProRail. (2016f). *Instandhoudingsrisico analyse - laagfrequent spoorstroomlopen (grs)* (3rd ed.) (No. IRA60111-V003). (Internal document)
- ProRail. (2016g). *Instandhoudingsrisico analyse - voeding tbb - centrale voeding* (1st ed.) (No. IRA00011-V001). (Internal document)
- ProRail. (2016h). *Instandhoudingsrisico analyse - voeding tbb - lokale voeding* (No. P1268053). (Internal document)
- ProRail. (2016i). *Jaarverslag 2015*.
- ProRail AM Infrabeschikbaarheid. (2016a). *Gouda stroomstoring 18 februari 2016*. (CONFIDENTIAL)
- ProRail AM Infrabeschikbaarheid. (2016b). *Handboek storingsmanagement 2016*. (Internal document)
- ProRail Assetmanagement. (2010). *Technisch beleid - energievoorzieningsstelsel railinfra-voedingen* (3rd ed.) (No. BLD00400-2). (Internal document)
- ProRail Assetmanagement. (2012). *Bedrijfsvoeringshandboek - energievoorziening, niet-tractievoeding, voeding tbb* (3rd ed.) (No. HDB00003-3). (Internal document)
- Railinfra Opleidingen. (2011). *B-relais stationsbeveiliging - nx-systeem '68* (No. Riab B0009). Railinfra Opleidingen.
- Ramaekers, P., de Wit, T., & Pauwel, M. (2009). *Hoe druk is het nu werkelijk op het nederlandse spoor? het nederlandse spoorgebruik in vergelijking met de rest van de eu-27*. CBS, Den Haag.
- Schell, C. (1992). *The value of the case study as a research strategy*. (Manchester Business School)
- Verhaeghe, R. (2007). *Data, modeling & decision making*. Delft University of Technology. (Course reader CT4831)

- Voermans, T. (2016, 10 18). 'Pier, hoe ze over ons praten... Doe wat!'. *Algemeen Dagblad*. Retrieved 2016-11-28, from <http://www.ad.nl/nieuws/pier-hoe-ze-over-ons-praten-doe-wat~aab3d59a/>
- Yin, R. K. (1994). *Case study research: Design and methods*. SAGE Publications, New Delhi. (Second edition)











# **Appendices**

# List of Figures

1	Main tasks of ProRail. . . . .	iv
2	Bathtub model. . . . .	iv
3	Fault tree symbols. . . . .	vi
4	Fault tree (FT) ‘power supply disturbed’ notification. . . . .	viii
5	Event tree (ET) ‘power supply disturbed’ notification. . . . .	viii
6	Method implementation process. . . . .	ix
7	Kerntaken van ProRail. . . . .	x
8	Badkuipmodel storingsherstel. . . . .	xi
9	Foutenboom Boolean logica operatoren. . . . .	xiii
10	Foutenboom ‘stroomvoorziening gestoord’ melding. . . . .	xv
11	Gebeurtenissenboom ‘stroomvoorziening gestoord’ melding. . . . .	xv
12	Proces implementatie. . . . .	xvi
1.1	Main tasks ProRail. . . . .	2
1.2	Passenger-and-freight-train kilometres per kilometre of train track in the EU (2006) (Ramaekers et al., 2009). . . . .	4
1.3	Passengers per kilometre train track in the EU (2006) (Ramaekers et al., 2009). . . . .	4
1.4	Punctuality (<5 min) versus crowdedness in different countries (NS Groep N.V., 2016b). . . . .	4
1.5	2015 Railway performance index rating to public cost (Boston Consulting Groep, 2015). . . . .	5
1.6	ProRail and the surrounding stakeholders (Brinkman, 2009). . . . .	6
1.7	Bathtub Model by Ghaemi & Goverde (2015). . . . .	7
1.8	Report structure. . . . .	11
2.1	fault tree (FT) symbols. . . . .	14
2.2	fault tree (FT) ‘Car will not start’ example. . . . .	15
2.3	event tree (ET) ‘Car will not start’ example. . . . .	16
2.4	fault tree (FT)-event tree (ET) combination ‘Car will not start’ example. . . . .	17
2.5	Adapted pivotal events, event tree (ET) ‘Car will not start’ example. . . . .	18
2.6	Main actors failure recovery process ProRail (simplified). . . . .	20
2.7	Failure-recovery time line ProRail (ProRail AM Infrabeschikbaarheid, 2016b). . . . .	21
2.8	Post21 configuration adopted from InTraffic (2016). . . . .	24
2.9	Time-varying faults by Bai (2010). . . . .	26
2.10	Current information stream between ProRail and PCA. . . . .	27
2.11	Proposed information stream between ProRail and <i>procescontractaannemer</i> [contractor] (PCA). . . . .	27
3.1	Overview local power supply (Railinfra Opleidingen, 2011). . . . .	31
3.2	Overview central power supply (Railinfra Opleidingen, 2011). . . . .	31
3.3	Railway control structure. . . . .	32
3.4	‘Power supply disturbed’ notification linked series Gouda. . . . .	34
3.5	Underlying power off repeater relay (POPR) A11/12/3/4/6/8 circuit Gouda. . . . .	35
3.6	Power supply B/N-12/110V RK16 Gouda. . . . .	35
3.7	OR-scheme zoom part I RK16 Gouda. . . . .	36
3.8	OR-scheme zoom part II RK16 Gouda. . . . .	36
3.9	System to lock switches for operation in Gouda. . . . .	37
3.10	Fault Tree (FT): ‘Power Supply Disturbed’ notification causes. . . . .	38

---

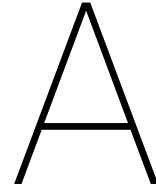
3.11 Event tree (ET): ‘Power supply disturbed’ notification diagnosis by side effects. . . . .	40
4.1 Proposed information stream between ProRail and PCA. . . . .	50
B.1 ICT-O current configuration (ProRail, 2015b) . . . . .	74
B.2 ICT-O future configuration (ProRail, 2015b) . . . . .	75
B.3 ICT-O configuration acronym explanation (ProRail, 2015b) . . . . .	76
D.1 FMECA example . . . . .	79
E.1 Power Supply Monitoring RH10 Gouda . . . . .	81
E.2 Current information stream between ProRail and PCA . . . . .	82
E.3 Zoom OR-scheme Gouda . . . . .	83
E.4 Current information stream between ProRail and PCA . . . . .	84





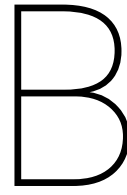
# List of Tables

1.1	Operational performance of ProRail (ProRail, 2016i).	3
1.2	TAO causes (ProRail, 2016i).	5
2.1	fault tree analysis (FTA) process steps obtained from Ericson (2005).	14
2.2	event tree analysis (ETA) process steps obtained from Ericson (2005).	16
2.3	Failure priority classifications (ProRail AM Infrabeschikbaarheid, 2016b).	22
2.4	Function recovery classes (ProRail AM Infrabeschikbaarheid, 2016b).	22
3.1	Notification cause - Side effect - Mechanic expertise.	39
3.2	Absolute results by mechanical issue from Event Tree (ET) prediction relative to observed SAP data.	41
3.3	Absolute results by location from Event Tree (ET) prediction relative to observed SAP data.	41
3.4	Absolute results by cause from Event Tree (ET) prediction relative to observed SAP data.	42
3.5	Mechanical issue test based on Table F2.	43
3.6	Location test based on Table F2.	43
3.7	Cause test based on Table F2.	43
3.8	Pearson's Chi-squared test 'power supply disturbed' notification diagnosis.	44
F1	Percentage of point of the Chi-square distribution	85
F2	Results SAP - approach results test	86
G.1	Toestand storing stroomvoorziening samenvatting	87



## SAP Report Content

- |                                    |                                  |
|------------------------------------|----------------------------------|
| 1. RVO-number                      | 23. $T_3$                        |
| 2. Contract area                   | 24. Fully restored (J/N)         |
| 3. Element                         | 25. $T_4$                        |
| 4. Location (km)                   | 26. Failure cause (code)         |
| 5. Element failure notification    | 27. Disturbed part               |
| 6. Short notice                    | 28. Repair actions               |
| 7. Elaborated notice               | 29. Causer code                  |
| 8. Priority                        | 30. Disturbed part SAP ID        |
| 9. Specialisation                  | 31. Disturbed part geo-code      |
| 10. Location                       | 32. Disturbed part description   |
| 11. Location (geo-code)            | 33. Disturbed part location (km) |
| 12. Test location geo-code         | 34. Repaired message reported by |
| 13. $T_0$                          | 35. Name                         |
| 14. Reported by                    | 36. Address                      |
| 15. Phone number                   | 37. Place                        |
| 16. WBI Number                     | 38. Billable                     |
| 17. $T_2$                          | 39. Phone number                 |
| 18. $T_{prognosis}$                | 40. Estimated labor costs        |
| 19. Prognosis validity (hard/soft) | 41. Estimated material costs     |
| 20. Short failure cause            | 42. Estimated machine costs      |
| 21. Elaborated failure cause       | 43. Estimated costs              |
| 22. –                              |                                  |



## ICT-O Components

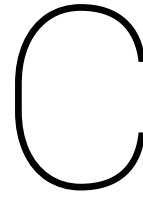
On the following pages all ICT-O components which are used for control and adjustments by traffic control (Post21 inside dashed section) et al. are shown, as constructed and operated by ProRail (2015b). The configuration is under construction, Figure B.1 shows the configuration which this study is based on, Figure B.2 shows the future configuration and Figure B.3 is added as explanation (Dutch) for all acronyms.

**CLASSIFIED**



**CLASSIFIED**

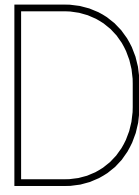
**CLASSIFIED**



## Asset Failure Causes

Several asset failure causes are described by ProRail AM Infrabeschikbaarheid (2016b), these causes are shown below.

1. Burr “Braamvorming”
2. Golf wear “Golfslijtage”
3. Wear “Slijtage”
4. Wear of rail by rolling action of train wheels “Uitwalsing”
5. Grooving “Groefvorming”
6. Drive into “Inrijden”
7. Incorrect geometry / situation / blind suspension “Onjuiste geometrie/ligging/blinde vering”
8. Local lowering of the track “Klapper”
9. RCF (headcheck)
10. Manufacturing fault
11. System failure
12. Adjustment improper/expired “Afstelling onjuist/verlopen”
13. Assembly Error “Montagefout”
14. Component failure of unknown cause “Onderdeel defect door onbekende oorzaak”
15. After examination ok / no cause found “Bij onderzoek in orde/geen oorzaak gevonden”
16. Insufficient maintenance “Onvoldoende onderhoud”
17. Overload “Overbelasting”
18. Other technical
19. Burned / burning “Inbranden van contacten, verbranden van motoren of dwars/wisselligger die in brand staat c.q. smeult.”
20. Insulation “Insulation”
21. Overvoltage “Overspanning”
22. Burn through “Doorbranden”
23. Corrosion / degradation “Corrosie/aantasting”
24. Breakage / cracking / crumbling “Breuk/scheurvorming/ afbrokkeling”
25. Vibrations “Trillingen”
26. Jammed “Vastgelopen”
27. Aging “Veroudering”
28. Rotten “Verrot”
29. Bending tongues or point rails due to internal tensions “Katterug”
30. Leakage “lekkage”
31. Buckled / deformed “Verbogen/vervormd”
32. Shifted parts “Omhoog werken/verschuiven”
33. Short circuited “Kortsluiten”
34. Pollution (technical) “Vervuiling (technisch)”
35. insufficient lubrication “Onvoldoende smering”
36. Obstructing vegetation “Belemmerende vegetatie”
37. Application / software error “Applicatie/softwarefout”
38. No examination “Geen onderzoek”
39. Not reported by Trdl “Niet door trdl gemeld.”



## FMECA ProRail

For all critical elements ProRail constructed an failure mode effect and criticality analysis (FMECA). The FMECA is part of the contract with the PCA. The FMECA is secured in three documents *informatie levering specificatie* [information supply specification] (ILS), *instandhouding risico analyse* [conservation risk analysis] (IRA), *instandhoudingsconcept* [conservation concept] (IHC). An example of an IHC is given in Figure D.1.



**CLASSIFIED**

E

# Technical Drawings Power Supply Monitoring Architecture

Technical drawings power supply used for capture monitoring architecture.

**CLASSIFIED**

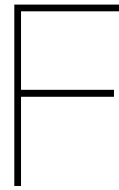
**CLASSIFIED**

**CLASSIFIED**

**CLASSIFIED**



**CLASSIFIED**



# Test Case Performance Check

Table F1: Percentage of point of the Chi-square distribution.

Degrees of Freedom	Probability of a larger value of $\chi^2$					
	0.99	0.95	0.90	0.10	0.05	0.01
1	0.00	0.00	0.02	2.71	3.84	6.63
2	0.02	0.10	0.21	4.61	5.99	9.21
3	0.11	0.35	0.58	6.25	7.81	11.34
4	0.30	0.71	1.06	7.78	9.49	13.28
5	0.55	1.15	1.61	9.24	11.07	15.09
6	0.87	1.64	2.20	10.64	12.59	16.81
7	1.24	2.17	2.83	12.02	14.07	18.48
8	1.65	2.73	3.49	13.36	15.51	20.09
9	2.09	3.33	4.17	14.68	16.92	21.67
10	2.56	3.94	4.87	15.99	18.31	23.21
11	3.05	4.57	5.58	17.28	19.68	24.72
12	3.57	5.23	6.30	18.55	21.03	26.22
13	4.11	5.89	7.04	19.81	22.36	27.69
14	4.66	6.57	7.79	21.06	23.68	29.14
15	5.23	7.26	8.55	22.31	25.00	30.58
16	5.81	7.96	9.31	23.54	26.30	32.00
17	6.41	8.67	10.09	24.77	27.59	33.41
18	7.01	9.39	10.86	25.99	28.87	34.81
19	7.63	10.12	11.65	27.20	30.14	36.19
20	8.26	10.85	12.44	28.41	31.41	37.57

Table E2: Results SAP - approach results test.

Case	ID / RVO number	SAP mechanic	SAP location	SAP cause	ET mechanic	ET location	ET cause
1	80811396	SW	RK	X5	SW	RK	X5
2	80812203	EV	Other	Z1	EV	RH	Z2
3	80812273	SW	RK	Z1	SW	RK	X5
4	80812727	EV	Other	Z2	EV	RH	Z2
5	80812736	EV	Other	Z2	EV	RH	Z2
6	70079686	EV	RK	X8	EV	RK	Z2
7	80813377	EV	RH	Z2	EV	RH	Z2
8	80813892	EV	RH	Z2	EV	RH	Z2
9	70080565	EV	RH	Z2	EV	RH	Z2
10	80814558	EV	RH	Z2	EV	RH	Z2
11	80814657	SW	RK	Z1	SW	RK	X2
12	80815037	EV	RH	Z2	EV	RH	Z2
13	80815288	EV	RH	Z2	EV	RH	Z2
14	80816566	EV	RH	Z2	EV	RH	Z2
15	70082656	EV	RH	Z2	EV	RH	Z2
16	80817710	EV	Other	Z2	EV	RH	Z2
17	80817909	SW	RH	X2	EV	RH	X2
18	80818121	EV	RH	Z2	EV	RH	Z2
19	80818149	EV	RH	Z2	EV	RH	Z2
20	80818253	EV	RH	Z2	EV	RH	Z2
21	80819080	SW	Other	X8	SW	RK	X8
22	70085574	EV	Other	Z2	EV	RH	Z2
23	80820047	EV	RH	X8	EV	RH	Z2
24	80820888	SW	RK	Z1	SW	RK	X5
25	80821417	EV	Other	Z2	EV	RH	Z2
26	70087486	EV	Other	Z2	EV	RH	Z2
27	80822572	EV	Other	Z2	EV	RH	Z2
28	70088000	EV	RH	Z2	EV	RH	Z2
29	70088300	SW	Other	X5	EV	RH	X5
30	80824870	EV	RH	Z2	EV	RH	Z2
31	80824921	EV	RH	Z2	EV	RH	Z2
32	80825072	EV	Other	Z2	EV	RH	Z2
33	80826598	SW	RH	G2	EV	RH	X2
34	80826702	SW	RK	Z1	SW	RK	X2
35	80826717	EV	RH	Z2	EV	RH	Z2
36	80826777	EV	RH	Z2	EV	RH	Z2
37	80827412	SW	RK	X5	SW	RK	X5
38	80827527	EV	RH	Z2	EV	RH	Z2
39	80827548	EV	RH	Z2	EV	RH	Z2
40	80827909	EV	Other	Z2	EV	RH	Z2
41	80828568	EV	Other	Z2	EV	RH	Z2
42	80831836	EV	Other	Z2	EV	RH	Z2
43	80832369	EV	RH	Z2	EV	RH	Z2
44	80832738	EV	Other	Z2	EV	RH	Z2
45	80833471	EV	RH	Z2	EV	RH	Z2
46	80833669	EV	RH	Z2	EV	RH	Z2
47	80833893	EV	Other	Z2	EV	RH	Z2
48	80834246	EV	RH	Z2	EV	RH	Z2
49	80834627	EV	RH	Z2	EV	RH	Z2
50	80834654	EV	RH	Z2	EV	RH	Z2
51	80834768	EV	RH	Z2	EV	RH	Z2
52	80835188	EV	Other	Z2	EV	RH	Z2
53	80835664	SW	RH	Z2	SW	RK	X5
54	80835815	SW	RK	X6	SW	RK	X6
55	80836688	SW	RK	X6	SW	RK	X6
56	80837160	EV	Other	Z2	EV	RH	Z2
57	80837916	EV	RH	Z2	EV	RH	Z2
58	80837946	SW	RK	Z1	SW	RK	X5
59	80838134	SW	RK	X6	SW	RK	X6
60	80838387	EV	RH	Z2	EV	RH	Z2
61	80838569	EV	RH	Z2	EV	RH	Z2
62	80840469	SW	RK	X6	SW	RK	X6
63	80840818	EV	Other	Z2	EV	RH	Z2
64	80842844	SW	RK	X5	SW	RK	X5
65	80844341	EV	RH	Z2	EV	RH	Z2
66	80844405	EV	Other	Z2	EV	RH	Z2
67	80845864	EV	Other	Z2	EV	RH	Z2
68	80846327	EV	RH	Z2	EV	RH	Z2
69	80846849	EV	Other	Z2	EV	RH	Z2
70	80849490	EV	RH	Z3	EV	RH	Z2
71	80849766	EV	RH	Z2	EV	RH	Z2
72	80849771	EV	RH	Z2	EV	RH	Z2
73	80851307	EV	Other	Z2	EV	RH	Z2
74	80851365	EV	Other	Z2	EV	RH	Z2

G

Werkwijze ProRail:  
Stroomvoorziening Gestoord  
Melding

**CLASSIFIED**

**CLASSIFIED**



**CLASSIFIED**

**CLASSIFIED**