Consolidation of Requirements for Railway Mobile Access Router System and Conceptualisation of Data Usage for Preventive Maintenance

JOHAN LANDERHOLM, HUGO KURTSON

KTH Industrial Engineering
and Management

Master of Science Thesis
Stockholm, Sweden January 2015

KTH Industriell teknik
och management

Consolidation of Requirements for Railway Mobile Access Router System and Conceptualisation of Data Usage for Preventive Maintenance

HUGO KURTSON
JOHAN LANDERHOLM

Master of Science Thesis MMK 2014:92 MDA 495
KTH Industrial Engineering and Management
Machine Design
SE-100 44 STOCKHOLM

KTH Industrial Engineering and Management

Master of Science Thesis MMK 2014:92 MDA 495

Consolidation of Requirements for Railway Mobile Access Router System and Conceptualisation of Data Usage for Preventive Maintenance

Hugo Kurtson
Johan Landerholm

Approved 2015-01-11	Examiner Martin Grimheden	Supervisor De-Jiu Chen
	Commissioner Tritech Technology AB	Contact person Ulf Almqvist

Abstract

This thesis has been carried out at a technology company outside of Stockholm, Sweden. The study has two major purposes: (1) to investigate how the safety aspect and railway standards affect the development of a data gathering unit for railway applications and (2) to demonstrate how reliability depend on maintenance and how gathering data could improve the maintenance planning and reliability of a train. The work is divided in three different parts.

Frame of reference, an initial study of relevant work including areas such as standards and regulations, designing software for safety-critical systems, proactive maintenance and an insight of the prototype system built by the consultant firm.

Identification of requirements for the data gathering unit, this part cover relevant standards and regulations, general system concept and risk analysis.

Dynamic effects of train maintenance with focus on reliability. Subjects discussed in this chapter are proactive and preventive maintenance, perfect and imperfect preventive maintenance and its effects on system reliability.

The results suggest that the gathering unit should not be seen as a safety critical system, still railway standards and regulations must be followed during the development process of such a product. It is also established that it can be concluded that reliability depends on the maintenance interval and the components characteristic wear parameters. Gathering data enable higher accuracy of wear parameters and makes maintenance decisions more reliable and cost effective.

KTH Industriell teknik
och management

Examensarbete MMK 2014:92 MDA 495

Konsoldering av krav för en ombordenhet på tåg samt konceptualisering av dataanvändning vid förebyggande underhåll

Hugo Kurtson
Johan Landerholm

Godkänt 2015-01-11	Examinator Martin Grimheden	Handledare De-Jiu Chen
	Uppdragsgivare Tritech Technology AB	Kontaktperson Ulf Almqvist

Sammanfattning

Detta examensarbete har utförts i samarbete med en konsultfirma i Sundbyberg. Studien har två huvudsyften: (1) att undersöka hur olika säkerhetsaspekter och järnvägsstandarder påverkar utveckling av en ombordenhet avsedd att samla in tågspecifik data samt (2) att visa hur underhåll påverkar systemets tillförlitlighet och hur datainsamling kan förbättra planering av underhåll, och därigenom tågsystemets tillförlitlighet. Arbetet är uppdelat i tre huvuddelar:

Litteraturstudie, där en inledande studie av relevant forskning har utförts. Denna del täcker relevanta standarder och direktiv, utveckling av säkerhetskritiska system, proaktivt underhåll samt en överblick av relevanta system till prototypen utvecklad av konsultbolaget.

Utveckling och kravställning av en datainsamlande ombordenhet. Denna del täcker hur standarder och lagar påverkar denna utveckling, genomgång av systemkonceptet och tillhörande riskanalys.

Förebyggande underhålls påverkan på tågsystemet med fokus på tillförlitlighet. I denna del diskuteras proaktivt och förebyggande underhåll i form av modeller för perfekt och imperfekt underhåll och dess påverkan på systemets tillförlitlighet.

Resultatet från de första delarna bekräftar att ombordenheten ej behöver anses vara en säkerhetskritisk enhet men att utvecklingsprocessen ändå bör följa järnvägsstandarder och lagar för att påvisa en tillförlitlig produkt.

Utifrån arbetet i denna avhandling kan det slås fast hur tillförlitlighet beror av hur ofta komponenterna underhålls samt dess karakteristiska förslitningsparametrar. Insamling av data över tid förbättrar förmågan att öka noggrannheten på tågsystemets förslitningsparametrar och därigenom möjliggör mer kostnadseffektiva beslut inom underhåll baserat på komponenters tillförlitlighet.

Acknowledgments

The authors would like to express their gratitude to their supervisor Ulf Almqvist at Tritech Technology and their supervisor De-Jiu Chen at the Royal Institute of Technology in Stockholm, for help and support during the entire thesis.

Work division

In this thesis the work has been divided in the following manner:

Johan: Has researched and written section 2.3 Railway industry related standards and regulations, 2.4 Concerns in the design of safety critical systems and section 2.6 Reliability models for maintenance. In chapter 3 he has concluded what is relevant from the standards and written section 3.1 Life cycle phases and guidance from standards and regulations, written subsections 3.2.5 Working environment and 3.2.7 General RAMS implications as well as written subsection 3.3.1 Risk acceptance. In chapter 4 he has written subsection 4.1.2 Improving Weibull parameters and section 4.3 Data related to preventive maintenance. In chapter 5 Final results Johan has written the general introduction to section 5.2 Verification as well as the entire section 5.3 Results on dynamic effects of preventive maintenance. In chapter 6 Conclusions and future work he has written all sections with the exception of the third paragraph in subsection 6.1 Discussion on requirements. Johan has done the all the Matlab coding.

Hugo: In chapter 2 Hugo has researched and written sections 2.1 Relevant systems of the train, 2.2 Technology behind MAR and 2.5 Proactive Maintenance. In chapter 3 he has written section 3.2 System concept with the exceptions stated above. He has written and listed the subsections 3.3.2 Hazard log and 3.3.3 Hazard analysis and the section 3.4 System requirements. In chapter 4 Hugo has written sections 4.1 Safety critical components and 4.2 Reliability dependencies. Hugo has derived how reliability dependencies between different components of the bogie can be modelled. In chapter 5 Final results Hugo has written and listed requirements in section 5.1 List of system requirements as well as written subsections 5.2.1 Verification of the hardware requirements and 5.2.2 Verification of the functional and non-functional requirements.

Nomenclature and abbreviations

Abbreviations

ADD	Pantograph Automatic Dropping Device
ALARP	As Low As Reasonably Practicable
ASIL	Automotive Safety Integrity Level
ATP	Automatic Train Protection
AWS	Automatic Warning System
COTS	Commercial off the shelf
DRA	Driver Reminder Appliance
DSD	Drivers Safety Device
ER	Train Event Recorder
ERTMS	European Rail Traffic Management System
FMECA	Failure Mode, Effects and Criticality Analysis
FTA	Fault Tree Analysis
GAMAB	Globalement Au Moins Aussi Bon
GUI	Graphical User Interface
HAZOP	Hazard and Operability Analysis
IETF	Internet Engineering Task Force
IKIWISI	I’ll know it when I see it
IPM	Imperfect Preventive Maintenance
MAR	Mobile Access Router system
MBD	Model Based Development

MEM	Minimum Endogenous Mortality
MTBM	Mean Time Between Maintenance
MTTM	Mean Time To Maintain
MTTR	Mean Time to Repair
PES	Programmable Electronic Systems
PM	Preventive Maintenance
PPM	Perfect Preventive Maintenance
PTS	Post- och telestyrelsen
RAMS	Reliability, Availability, Maintainability and Safety
RCM	Reliability Centred Maintenance
RSML	Requirements State Machine Language
RTOS	Real Time Operating System
STM	Specific Transmission Module
THR	Tolerable Hazard Rate
TPWS	Train Protection and Warning Systems
TSI	Technical Specifications for Interoperability

Nomenclature

β	Weibull parameter for shape	[1]
γ	Weibull parameter for location	[1]
μ	Mean time to repair	[−]
μ_m	Mean time for minimal repair	[−]
τ	Useful lifetime of component	[−]
θ	Weibull parameter for scale	[1]
A	Technical availability	[1]
C_c	Cost of component	[−]
C_{ci}	IPM total cost for component	[−]
C_{mri}	Cost of minimal repair for component	[−]

C_{pc}	Total cost for component	$[-]$
C_{pmi}	Cost of performing IPM on each PM stage	$[-]$
C_{ppm}	Cost of performing PPM on component	$[-]$
f	Improvement factor	[1]
n	Number of PM stages	[1]
$R(t)$	Reliability	[1]
t	Time	$[-]$
T_p	Periodic maintenance interval time	$[-]$
t_r	Component age reduction	$[-]$
U	Unavailability	[1]
W^+	Effective age	$[-]$

List of Figures

List of Tables

Contents

Chapter 1

Introduction

1.1 Background

During 2013 a consultancy firm located in Sundbyberg developed a prototype system that extracts data from trains' Automatic Train Protection system (ATP). The developed system contains a mobile gateway, a communication over cellular network, a centralised gathering unit, a database and an IT system. The possibility of extracting data more or less continuously from trains' on-board systems for analysis and processing in a central database is something several leading suppliers in the train industry is working with today. The difficulty lies within creating a general system that is compliant with trains from a multitude of different suppliers and from different ages. This requires communication with several different on-board systems and over a number of interfaces. To develop and specify a general system that gathers data from many different on-board systems on a train is not a simple process.

This general type of system is in the railway business commonly referred to as "Mobile Access Router System" (MAR). It can be described by figure 1.1 where information from several train systems are transferred to a server which the user can access through a web interface.

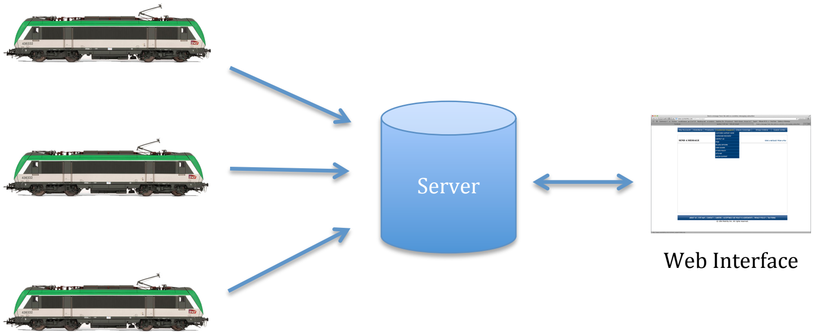


Figure 1.1: Illustrated view of the MAR system.

On the train there is a mobile gateway, alternatively a simple computer that gathers data from arbitrary many on-board systems and can communicate through public communication networks such as 3G, LTE or Tetra to a central server that handles and stores the data. The big suppliers of train equipment and industrial-communication as well as many train operators have requests and ideas about such a general gathering system. There are no available commercial off the shelves (COTS) products for this type of systems but large development projects are on-going at several suppliers.

The consultant firm has together with a global supplier of train equipment developed one of the first commercially available systems of this kind. This system, which can be seen as a prototype or just limited in functionality, is built of commercial available hardware to minimise development time and cost. They deem it is possible to further develop this system in an easy and cost effective way such that it can handle interoperability over different interfaces and communication techniques.

1.2 Motivation

In this context the purpose of this thesis is to examine how railway industry related standards influence the specification and requirements of the client or on-board unit on the train and how these should be formulated. Furthermore the purpose is to explore availability of train data and how it could be used, including which data could be used for new features such as live-tracking.

1.3 Research question

This thesis is to explore how system requirements for a train on-board data gathering unit, that is further described in section 3.2, should be specified, taking in account for how standards and regulations affects the development process. It should also lead to a greater understanding of how increased accessibility to train data could affect the usage of said data.

1.4 Hypothesis

The authors of this thesis believe that railway industry standards provides a rich set of instructions and suggestions for requirements that will make it possible to specify a on-board data-gathering unit as non-safety critical. Thus the standards will not impose requirements that will make it impossible to develop using COTS hardware. Regarding having increased accessibility to train data over time the authors believe that it will make it possible to monitor and improve the reliability for an entire system through methods for preventive maintenance.

1.5 Delimitations

To narrow down the project and fit it in the scope and time frame of a master thesis, the authors chose to concentrate on specification of the client side of the system, i.e. the on-board gathering unit. They have omitted to look deeper into the centralised server, database and web system. Specification of requirements for the unit have been done at system level and independent of what protocols and interfaces used by the devices on-board, all in order to make it as general as possible. The thesis will not explore further into the MAR functionality of network handovers and connectivity. When looking at available data on trains the authors have focused on data types that can be used for maintenance purposes.

1.6 Methods

An initial study of relevant work was performed, this included areas like standards and regulations, designing software for safety critical systems, proactive maintenance and getting an insight of the prototype system built by the consultant firm. To find possible live tracking features data models were designed and classified upon the available data. Requirements were formulated with guidance of railway specific standards. This included an investigation of which data that is possible to access in today's train-system as well as an analysis of desirable data. Models for reliability, availability and cost were modelled in Matlab and evaluated on how they are affected on a system perspective.

1.7 Report outline

This report is structured with different chapters that covers most relevant aspects of the development of this thesis. It is structured as follows:

Chapter 1 Introduction. This chapter introduces the background and purpose of this thesis, the research question and hypothesis as well as delimitations and methods used to finalise the thesis.

Chapter 2 Frame of reference. This chapter provides the reader with an overview of relevant topics regarding this thesis.

Chapter 3 Identification of requirements for the data gathering unit. This chapter presents how standards and regulations influences the product development as well as the system concept and a risk analysis. A set of requirement is presented as an outcome of the concept and risk analysis. The chapter wraps up with verification tasks for the requirements.

Chapter 4 Analysis of preventive maintenance effects on system reliability. This chapter discusses reliability and maintenance and for a system and presents a reliability model for the system as well as shows how the reliability is effected by maintenance.

Chapter 5 Conclusions and further work. This chapter discusses the work done during this thesis as well as draws relevant conclusions from performed work as well as from theory and describes an idea for further work.

Chapter 2

Frame of reference

This chapter includes a summery of related standards and technologies. The areas covered are first related to the train and the systems of the locomotive and how wireless communication typically is performed. It describe some of the relevant standards and regulations within the railway industry and a few things to consider when developing safety critical systems. The chapter ends with a description of proactive maintenance.

2.1 Relevant systems of the train

A number of computers in the locomotive keep track of information from the whole train, including information from control and safety systems, information from installed equipment and other train functionality information. This section describes different systems available in the locomotive that is relevant for this thesis.

2.1.1 Train event recorder

Railway and transport regulations today demand that locomotives for trains running faster than a certain speeds are obliged to have a Train Event Recorder (ER), usually referred to as black box, installed. Each country or region may have their own rules regarding ER but the main requirements stays the same. The ER must have a documented and proofed crashworthiness, shock, fire and fluid resistance and a hardened memory module meeting specified criterias. The ER is essentially a rugged data logger for retrospective diagnosis primarily used for investigating accidents and determining their probable cause. The required list of logged data is extensive and necessary to prevent future accidents of same origin. Data being logged cover information e.g. about how the train behaves in terms of movement, signalling and braking actions but also how the train driver acts and responds while driving the train. (Transports, 2002)

2.1.2 Automatic train protection

In order to eliminate the human factors while driving a train, there are several different security systems installed on the train. Automatic train protection, ATP is a system that among other things keeps track of the speed limits and rail section access rights. The idea in the future is for this system to fully replace the optical communication between trackside signs and traffic lights with the train driver. Through wireless transmission of data from either beacons mounted on the rail or the GSM-R network, the train gets information on upcoming rail section. Besides stop commands and speed limits this also includes other information that may affect the operation of the train. By using the already known train parameters combined with information of the upcoming track, braking curves are calculated in the train control system. When the train is approaching a speed transition or stop command, the train will automatically slow down to the maximum allowed speed if the driver of some reason missed the information or braked too weak or late. In this type of safety system there is a lot of data available describing the trains characteristics as numbers of cars, locomotive type, the design of the braking system and availability of emergency brakes, braking pipe pressure and also the information about upcoming rail sections in the form of speed limits and predicted braking curves. A lot of this data is saved for later analysis in the ATP Recorder (Banverket, 2009).

2.2 Technology behind MAR

Vehicles of today carry a great number of embedded on-board systems. In order to remotely monitor and get the information available in real time, a high performance and wide-area wireless Internet connection is needed. With today's deployed cellular network together with WLAN and Wimax in urban areas and cities it is now possible to create a network-in-motion inside a vehicle. A Mobile Access Router combines these technologies and uses multiple different wireless and cellular networks to ensure an continuously stable Internet connection without disconnection and loss of data package. The small size and ability to maintaining Internet connectivity during movement makes a Mobile Access Router suitable for handling Internet connections on-board a bus, train or other moving vehicles (Sun et al., 2008). Since a Mobile Access Router is supposed to work in motion it is necessary to use mobile cellular networks with a wide geographical coverage. The most widely deployed networks today are UMTS, GSM, GPRS, Edge, 3G and LTE. The old GPRS and EDGE technology does not provide high transfer rates compared to the newer wireless networks such as 3G and LTE. When the need to transfer bigger sets of data e.g. images and video, HSPA+, LTE, Wimax or WiFi is highly preferred over GPRS and EDGE (3GPP, 2007). The theoretical transfer rates for the most common network technologies are shown in table 2.1. The higher transfer rates is also associated with being the most short ranged technology.

Table 2.1: Theoretical transfer rates for different network technologies (3GPP, 2007).

Network	Downstream [Mbit/s]	Upstream [kb/s]
GPRS	0.040	0.014
EDGE	0.384	0.384
HSPA	14.4	5.76
HSPA+ v.7	28	11
HSPA+ v.8	42	11
HSPA+ v.9	84	23
HSPA+ v.10	168	23
LTE	150	75
Wimax 802.16m	365	376
WiFi 802.11n	450	450

2.2.1 Network topology and data routing

For handling data traffic routing Mobile IP is used. Mobile IP is a mobile communication protocol developed by Internet Engineering Task Force (IETF), an open community dedicated to research and development of Internet architecture and operation of the Internet (IET, 2014). IETF designed Mobile IP to allow mobile devices to move from one network to another while maintaining a permanent IP address. An ideal Mobile Access Router using Mobile IP would be able to change seamless between networks and different communication technologies without connected devices are affected by the change. The Mobile IP network includes three main components: Mobile Node, Home Agent and Foreign Agent. As in figure 2.1 the Home Agent is a router or server in the home network that keeps track of the IP addresses for the Mobile Node and acts like an anchor point. All traffic to the Mobile Node routes through this router. By establish a tunnel between the Home Agent and Mobile Node the devices connected to the Mobile Access Router will function as connected directly to the Home Agent. While roaming other networks, the Foreign Agent will function as the point of attachment for the Mobile Node, routing traffic from the Home Agent to the Mobile Node. While connected to other networks the Mobile Node is assigned a so-called care-of address from the Foreign Agents, this is a dynamic IP address for each new network or location. The Home Agent associates the new dynamic IP address with the care-of address to maintain the connection to the Mobile Node. (Cisco Systems, 2004)

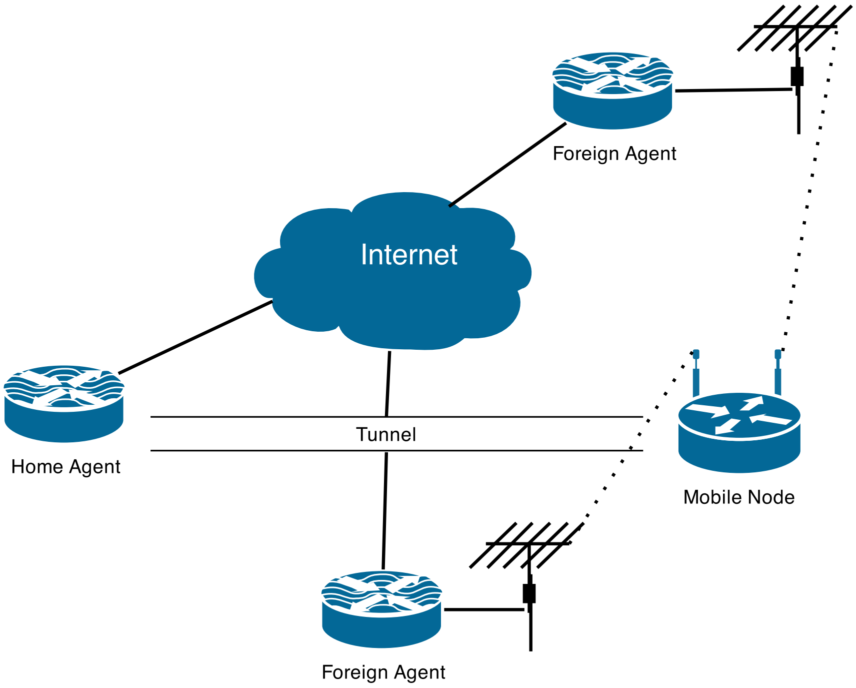


Figure 2.1: Network topology using Mobile IP.

2.2.2 Mobile access router hardware

The hardware design for the Mobile Access Router in figure 2.2, is a combination of several cellular- and wireless-network modules connected to an internal router. The internal router decides which network or technology to use based on different algorithms. The algorithms for deciding network take in account predefined priority, signal quality, latency, cost etc. depend on area of use for the Mobile Access Router. (Chan and Lu, 2003) There are Mobile Access Routers on the market offering satellite data connection but as the technology have a high latency and is far more expensive compared to 3G and growing LTE network the usage of satellite connections is limited to certain applications.

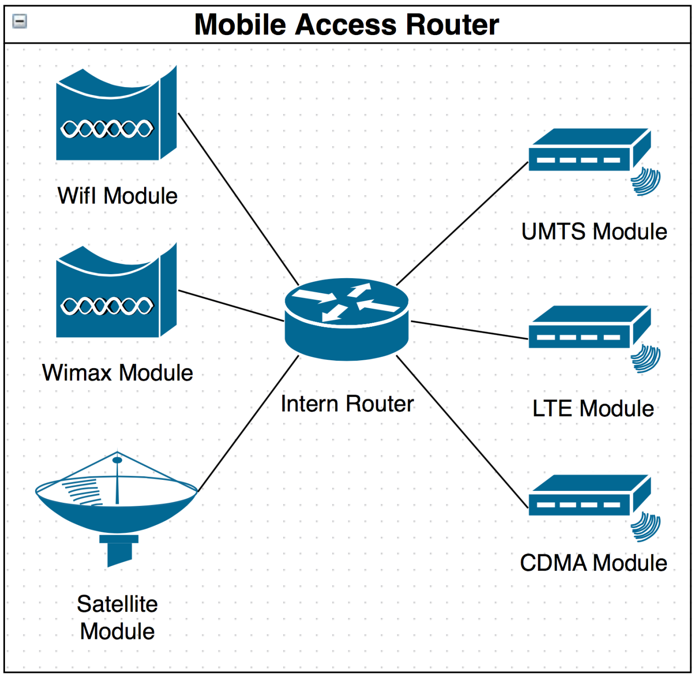


Figure 2.2: MAR hardware design.

2.3 Railway industry related standards and regulations

This section is a brief introduction to relevant standards related to product development and safety in the railway industry. In the field of railway technology there are also heavy regulations from national governments where interpretations of EU-directives can differ between countries.

2.3.1 Railway standards

Related to this thesis are the standards that specifies how the development process should go about. There is the general IEC 61508 titled: Functional Safety of Electrical/Electronic /Programmable Electronic Safety-related Systems, which many more specific standards builds upon such as the more specific railway standards:

- EN 50126:1999, Railway applications - The specification and demonstration of reliability, availability, maintainability and safety (RAMS).
- EN 50128:2001, Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems.
- EN 50129:2003, Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling.
- EN 50155:2007, Railway applications - Electronic equipment used on rolling stock.

The most relevant standard for this thesis is the EN 50126 which addresses system issues regarding reliability, availability, maintainability and safety on a large scale. It specifies how the process of handling RAMS (Reliability, Accessibility, Maintainability and Safety) should be managed. The main focus of EN 50126 is the RAMS life cycle which specifies how to handle RAMS when going from concept to decommissioning and disposal. EN 50128 comes in when choosing methods to be used in order to provide software which meets the demands for safety integrity addressed on higher levels in the design. This is described by a software life cycle with requirements for documentation, requirements specification, architecture, design and implementation, verification and testing, software/hardware integration, validation, assessment, quality assurance and maintenance among other things. These standards also refer to the general ISO 9000 suite: Quality systems - Model for quality assurance in design, development, production, installation and servicing. ISO 9000 can be seen as a basis for documentation.

As a comparison in another field than the railway industry there is the vehicle industry safety standard ISO 26262 titled: Road vehicles – Functional safety. This standard is divided into 10 different parts covering most aspects of vehicle development, it is divided into:

- Management of functional safety
- Concept phase
- Product development at the system level
- Product development at the hardware level
- Product development at the software level
- Production and operation
- Supporting processes and ASIL-oriented and safety-oriented analyses

The ISO 26262 is in some aspects quite similar to the EN 50126 in it is concepts for safety.

2.3.2 European and Swedish regulations

Within the European Union a venture to build a unified railway system started as early as 1990s. The purpose is to increase the efficiency of railway transportation as well as to be a competitive alternative to other types of transportation. The European Union has put together a number of directives with the purpose to unify the regulations of the member states. Currently there is the directive 2008/57/EG (EUROPEAN PARLIAMENT AND THE COUNCIL, 2008) for railway interoperability within the community and as can be found on the Swedish government agency Transportstyrelsen website (Banverket, 2014) there are a number of guidelines of how this should be applied in Sweden.

2.4 Concerns in the design of safety critical systems

As for all safety related products special care is needed in the design process, often especially so in the railway industry. When designing for safety one has to think about what safety is. Also embedded systems are more frequently used close to human lives, i.e. humans interacts closely with embedded devices, so one has to free humans from hazard. In other words: "safety is a system problem" (Lutz, 2000). This section describes some aspects of software engineering regarding safety and addresses issues that are related to system and requirement engineering.

In (Lutz, 1993) she addresses that when designing systems one should "focus on the interfaces between the software and the system in analysing the problem domain, since these interfaces are a major source of safety-related software errors." She also addresses that system issues like operational environment, the hardware and communication interfaces as well as timing has to be addressed in software requirements to avoid errors (Lutz, 1993).

2.4.1 Specifying requirements

Often when designing systems, as well as subsystems, one wants to have an abstraction layer towards other systems and especially if the entire system is large and very complex. There is a need to allocate sub-level requirements that fulfills higher level requirements as well as there can be environmental requirements from subsystems that flows up in the architecture as an example from the use of COTS hardware. This preferred hierarchical view, where the system development does not follow the orderly fashion of first designing top-level requirements then translate them to lower levels makes it possible to co-evolve requirements as well as architectural design. Starting out with an architecture used in similar systems adds restrictions on the set of achievable requirements but may be beneficial since designers and software engineers are used to it, as well as it is often a cheaper investment using an architecture that have been refined in several systems, e.g. product families. Thus expanding the complete set architectural models and requirements step by step gives us a tool to better handle uncertainties such as commercial off the shelves (COTS) products and their restrictions (Whalen et al., 2012). This view on how requirements and architecture interacts can be seen in figure 2.3 which shows the flow of requirements between systems and subsystems.

How are one supposed to develop products then? The standard way to do it historically was to first write the requirements and then go about to do the design, cost estimation, planning etc. This is not simple and requirements needed to cover things like completeness (describe all elements and most of all, don't miss any), consistency (the elements have to match each other), traceability (track the requirements back to system level) and testability (to make sure the end product is correct). Doing requirements this way takes time but was the only way to make sure that the software delivered matched the original specifications (Whalen et al., 2012).

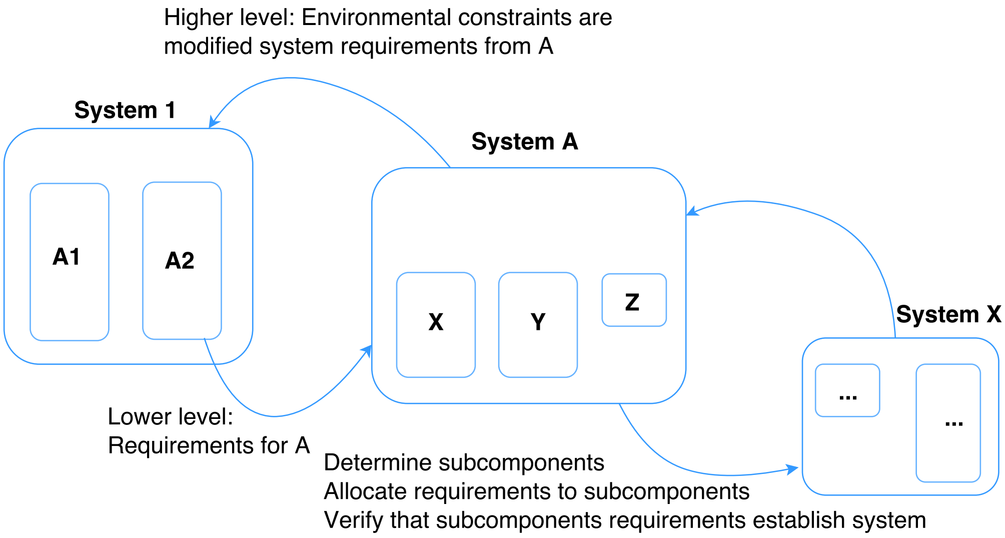

Higher level: Environmental constraints are modified system requirements from A
System 1
A1
A2
System A
X
Y
Z
System X
...
...
Lower level: Requirements for A
Determine subcomponents
Allocate requirements to subcomponents
Verify that subcomponents requirements establish system

Figure 2.3: How system architecture and requirements interacts. Requirements can flow both downwards and upwards, due to system allocation or the use of COTS components.

2.4.2 IKIWISI, COTS

Sometimes there is a need to change the requirements during design and implementation phases but this can relatively easy be handled with some change control procedure. However, the IKIWISI (I'll know it when I see it) procedure, COTS software and rapid change in information technology (eq. making a product obsolete even before it is released) have combined to disturb the traditional way of doing requirements. This is more and more frequently occurring when there is a race to reach the market before someone else (Boehm, 2000).

How are you then supposed to handle IKIWISI when you ask the users to specify requirements? First of all, users often get a better understanding for the product when they see a prototype or demo and thus their needs and wishes changes when they start using the product and get to know how it works. With the example of designing a GUI one can handle this by not being too pre-specified and rather agree upon the framework which the GUI will be built upon.

With the use of COTS one might be able to develop a product more rapidly and cheaper but it also ads restrictions on the possible performance. If you can't afford to build your own version that will outperform that COTS item you'll hopefully recognise that it is not a feasible requirement to have.

2.4.3 COTS RTOS

Using Linux as real time operating system (RTOS) in embedded systems has become more and more popular and how to handle safety with a COTS operating system has among others been researched by (Zhou et al., 2013) and one thing to take account for is that safety and reliability is not the same thing. As Linux operate on top of the hardware layer and your application on top of that you have to think about how you design safety. For example Linux does not provide accurate watchdog timers so such measures have to be done in the application layer (R H Pierce, 2011). Despite this, Linux seems to be more and more common in embedded systems.

2.4.4 Model based development

Over the last decade model based development (MBD) tools have begun to be more frequently used in the industry. Also progress in automated testing and verification has reduced the number of coding errors that escapes detection during testing (Heimdahl, 2007).

Even though safety critical systems is a well researched domain it is still difficult to specify requirements that covers all the aspects of a system. In work done by (Whalen et al., 2013) they identify the challenges with requirement verification in MBD. It was found in the study that errors were as likely found in the requirements as well as the models representing the system. For instance they show an example of inconsistencies between two requirements:

- When button X is pressed, the mode shall be A.
- When button Y is pressed, the mode shall be B.

These requirements are inconsistent if X and Y can be pressed at the same time and the system cannot be in both mode A and B at the same time. Using MBD techniques and having a formal language for the requirements can help you detect such problems, and can especially be helpful with a more complex set of requirements.

2.4.5 Transitions between perspectives on architectures

To acquire desired level of safety, standard (ISO 26262) suggest that one should have multiple views on the concepts for safety and that they should be separated between functional and technical. This introduces an issue regarding how one should define the transitions between different views or perspectives. (Ellen et al., 2012) has presented a list of objectives to make sure that such a transition is consistent. The goal is: to make sure that all allocations constraints are satisfied, to preserve each connection in different perspectives, that allocated elements must fulfil their communication needs, to take in account resource capacity and that each transition has to be optimised given their goal.

2.4.6 Validating requirements through formal methods

One of the formal languages used for requirements are RSML^{-e}. which is based on the Requirements State Machine Language (RSML) developed by (Leveson et al., 1994). This has been used to describe the requirements for the mode logic of a flight guidance system. Going from requirements on "shall" form written in English, Miller et al. found that: "The process of creating the RSML^{-e} model improved the informal requirements, and the process of providing the formal properties found errors in both the original requirements and the RSML^{-e} model" (Miller et al., 2006). The RSML^{-e} language can be useful to help achieve a more complete set of requirements and help with providing a clear reachability between states and therefore help detecting ambiguous statements.

Another tool that is academically available is UPPAAL which can be used as an integrated tool for modelling, simulation and verification. It is described as: "appropriate for systems that can be modeled as a collection of non-deterministic processes with finite control structure and real-valued clocks, communicating through channels or shared variables" and that "Uppaal consists of three main parts: a description language, a simulator and a model-checker. The description language is a non-deterministic guarded command language with data types (e.g. bounded integers, arrays, etc.). It serves as a modeling or design language to describe system behaviour as networks of automata extended with clock and data variables. The simulator is a validation tool which enables examination of possible dynamic executions of a system during early design (or modeling) stages and thus provides an inexpensive mean of fault detection prior to verification by the model-checker which covers the exhaustive dynamic behaviour of the system. The model-checker can check invariant and reachability properties by exploring the state-space of a system, i.e. reachability analysis in terms of symbolic states represented by constraints" (UPP, 2014).

This tool could be useful in a more complex development project and have been used in work done by (Ali and Sulyman, 2012) where a similar process is described. The tool is based on a free academic licence, has an easy to use GUI and there exist many examples of how to use the tool.

2.5 Proactive Maintenance

As maintenance has been recognised as a major part of the total life-cycle cost of industries, equipment and mechanical products, strategies for maintenance has become necessary. This section is about different maintenance strategies, proactive maintenance is one of these strategies for product and plant maintenance. As James C. Fitch states, "Proactive maintenance commissions corrective actions aimed at failure root causes, not just symptoms." (?).

2.5.1 Preventive and reactive maintenance

To explain preventive maintenance, it is easier to start with the opposite, reactive maintenance. RM is a failure-triggered action, components are not repaired before they break or if the condition is under the performance threshold. A characteristic for reactive maintenance is that the system needs instant repair when faults are detected, often with unplanned downtime as a result. It is never desirable with unplanned downtime since it often comes with large financial losses and service delays. Usual problems are high labour cost due to the need of hiring service personnel, urge of expensive express shipping for spare parts or large spare part inventory, all with unpredictable expenses. Common for companies using this approach is low reliability and availability because of the unpredictable failures and as a result of the unplanned downtime, compared to companies adopting a proactive maintenance plan. With a preventive maintenance plan, the company does not wait until components fail or wear out before taking action. The concept with preventive maintenance is acting before the failure occurs. Such actions could be e.g. a change of sealing or spring, lubricating, cleaning components or change a consumable part, a smaller maintenance that prolongs the lifetime of the components and system as a whole, less costly compared to change or repair the same components (Nggada, 2012). This kind of maintenance is scheduled to take action during planned stoppages, with a minimum of unnecessary downtime as possible. The benefits of using such approach are many, high personnel efficiency, minimal unplanned downtime with high availability as a result, better control of system condition, lower life time cost etc.

2.5.2 Predictive maintenance

Predictive maintenance is a process to analyse a system or equipment and develop a maintenance plan. This plan includes schedule for how and when the preventive maintenance should be carried out in the most cost-efficient way and also keep a high degree of availability and reliability. The difficulties have been to cost-optimise this maintenance schedule to match a lot of different components with different needs for maintenance both in time and labour (UPP, 2014). One approach adopted by industries that handles safety critical systems is reliability-centred maintenance (Douglas C. Brauer, 1997).

2.5.3 Reliability-centred maintenance

A predictive maintenance process, reliability-centred maintenance or RCM, was developed by Maintenance Steering Group during the 1970s. This process was later adopted by several large industries including airline companies, power plants and military applications. The main reason was to adapt a cost-effective and reliable process, "RCM process provides the desired or specified levels of operational safety and reliability at the lowest possible overall cost" (Douglas C. Brauer, 1997). The RCM process is achieved by first addressing the basic cause of system failure and then set up a maintenance plan to prevent those failures. This can be done with help of and by answering "The seven basic questions" of reliability centred maintenance for the target system. (Paul J. R. Lanthier, 1998)

The seven basic questions of reliability centred maintenance

- What are the functions and associated performance standards of the asset in its present operation context?

- In what ways does it fail to fulfil its functions?
- What causes each functional failure?
- What happens when each failure occurs?
- In what way does each failure matter?
- What can be done to predict or prevent each failure?
- What should be done if a suitable proactive task cannot be found?

This could also be done for each and every electric and mechanical component in the system. The target product or system is in that case divided into two groups of components with different maintenance requirements depending on the safety critically of the components.

Non-safety critical components

This could be any component in the system not direct related to safety functionality. Maintenance task on these components shall only be scheduled and performed if it reduces the total life-cycle cost of the system. This includes preventive maintenance tasks, which prolongs the lifetime of the components.

Safety critical components

Maintenance shall be scheduled such that the task prevent the components condition from degrading to unacceptable reliability and safety levels or as for non-safety critical components, when the total life-cycle cost reduces as a result of the maintenance task preformed.

Outcome from the seven questions

The outcome from answering these questions properly should be a cost-effective maintenance plan, component and system failure modes, failure mode effects and their corresponding risk level. To help answer these questions, different tools are used, fault-tree analysis for example is one tool recommended for use in RCM for finding safety critical components.

2.6 Reliability models for maintenance

As a tool to make maintenance decisions there are reliability models. How much of an improvement one gets from maintenance depends on several factors and there are different concepts for how large improvements it is possible to get. If a component after maintenance is returned to a state as-good-as-new it is called perfect preventive maintenance (PPM), but if the improvement lies between the condition before maintenance and when as new, maintenance is called imperfect preventive maintenance (IPM).

The state of components is often measured in performance parameters such as age, and the effectiveness of maintenance is often measured in the ability to reduce age. Life cycle parameters which maintenance effects are things as reliability, (un)availability and cost (Nggada, 2012). This section establishes models for these life cycle parameters under different conditions.

2.6.1 Reliability model under Weibull distribution

Maintenance in order to improve reliability is performed to keep the component being able to perform its required functions for a specified period of time. The model for reliability under Weibull distribution with no Preventive Maintenance is modelled as equation 2.1 (Nggada, 2012)

$$R(t) = exp\left[-\left(\frac{t-\gamma}{\theta}\right)^{\beta}\right] \tag{2.1}$$

where γ, θ and β are the Weibull parameters for location, scale and shape respectively, t represents time or calendar age. The Weibull distribution is a common model for wear on mechanical components and an estimation of the Weibull parameters for different components have been taken from the handbook (Nav, 2011). All further equations for reliability, (un)availability and cost in this section are described more in depth and are also verified in work done by Shawulu Hunira Nggada (Nggada, 2012).

2.6.2 Perfect preventive maintenance model

When the improvement factor of maintenance equals one and thus the new effective age is $W^{+} = 0$ after a maintenance procedure the maintenance is called perfect preventive maintenance. The component reliability under perfect preventive maintenance consists of two parts, the probability of survive until PM time, nT_p and the probability of surviving the remaining time, $t - nT_p; nT_p \leq t \leq \tau$. Where n is the number of PM stages since $t = 0$, and τ is the useful life of the component. The component reliability is seen in equation 2.2.

$$R_{pc}(t) = exp\left[-n\left(\frac{T_p}{\theta}\right)^{\beta}\right] exp\left[-\left(\frac{t-nT_p}{\theta}\right)^{\beta}\right]; nT_p \leq t \leq (n+1)T_p \tag{2.2}$$

When looking at unavailability under perfect preventive maintenance it can be seen as that there is no repair and PM is giving overhand of repair and therefore the unavaliability of the component becomes as equation 2.3.

$$U_{pc} = 1 - R_{pc}(t) \tag{2.3}$$

The cost for perfect preventive maintenance under the assumption that there is no repair is a simple one and varies with the total number of PM stages for a component. For the $i - th$ component the cost becomes as in equation 2.4.

$$C_{pci} = n_i C_{ppmi} + C_{ci} \tag{2.4}$$

Where C_{pci} is the total cost of the i-th component under PPM, C_{ppmi} is the cost of performing PPM for the i-th component, C_{ct} is the unit cost of the i-th component and n_i is the total number of PM stages for the i-th component.

2.6.3 Imperfect preventive maintenance model

Under maintenance called Imperfect preventive maintenance the maintenance action is presumed to improve the state of the component to a degree between as before the maintenance action and when the component was as good as new. This implies that the new effective age of the component depends on the improvement factor f that is less than 1, i.e. $0 \leq f < 1$ and assumed that both PM interval T_p and the improvement factor are constants the new effective age for a component is calculated as in equation 2.5.

$$W_n^+ = (1-f)nT_p \tag{2.5}$$

Together with equation 2.6 that describes how much the maintenance action rejuvenates the component age and with the Weibull parameters we get the equation for reliability under IPM.

$$t_r = (1-f)T_p \tag{2.6}$$

$$\begin{aligned} R_{ic}(t) = \prod_{j=1}^{n} &\left(1 - exp\left[-\left(\frac{(j-1)t_r - \gamma}{\theta}\right)^{\beta}\right] + exp\left[-\left(\frac{((j-1)t_r + T_p) - \gamma}{\theta}\right)^{\beta}\right]\right) \\ &\left(1 - exp\left[-\left(\frac{nt_r - \gamma}{\theta}\right)^{\beta}\right] + exp\left[-\left(\frac{(nt_r + (t - nT_p)) - \gamma}{\theta}\right)^{\beta}\right]\right) \end{aligned} \tag{2.7}$$

Equation 2.7 gives the component reliability under IPM and is an iterative evaluation of the probability of surviving until the n-th PM stage.

Availability under IPM

One concept of IPM is that you have repair of the component and often the objective is to improve availability through speedy but effective repair or to reduce the occurrences of failures that will lead to corrective maintenance. In these models for availability minimal repair is considered. Minimal repair is often things such as replacing a seal, spring, bearing etc. The availability of a component depends on the reliability and maintenance and can be modelled with dependency on up time of the component and down time of the component as seen in equation 2.8.

$$A_{ic} = \frac{\sum_{j=1}^{n}\left(T_p - \frac{\mu_m}{\theta^\beta}|t^\beta|_{W_{j-1}^+}^{W_j}\right)}{\sum_{j=1}^{n}\left[\left(T_p - \frac{\mu_m}{\theta^\beta}|t^\beta|_{W_{j-1}^+}^{W_j}\right) + \left(\mu - \frac{\mu_m}{\theta^\beta}|t^\beta|_{W_{j-1}^+}^{W_j}\right)\right]} \tag{2.8}$$

Where μ_m represents the mean time for minimal repair of the component and μ represents mean time to repair of the component and j represents the $j-th$ PM stage.

The equation for unavaliability becomes as in equation 2.9.

$$U_{ic} = 1 - A_{ic} \tag{2.9}$$

Cost under IPM

There are no standardised ways to perform maintenance as well as there are no standardised ways to calculate the maintenance cost. Without being specific on the type of preventive maintenance to perform, this model is established to allow evaluation of PM schedules in a generic way. The cost model under IPM is according to equation 2.10,

$$C_{ci} = C_{mri} \sum_{j=1}^{n} \left(\frac{1}{\theta^{\beta}} |t^{\beta}|_{W_{j-1}^{+}}^{W_j} \right) + n_i C_{pmi} + C_i \tag{2.10}$$

where C_{ci} is the IPM total cost for the i-th component, C_{mri} is the cost of minimal repair for the i-th component, C_i is the unit cost of the i-th component and C_{pmi} is the cost of performing IPM for the i-th component at each PM stage. As mentioned earlier the models in equation 2.1 to 2.10 in this section are derived and verified by Shawulu Hunira Nggada (Nggada, 2012).

Chapter 3

Identification of requirements for the data gathering unit

To be able to design system requirements there are a lot of basic prerequisites that need to be considered. To be able to present the system requirements this chapter covers the product life cycle phases, the system concept and the risk analysis and finally presenting system requirements.

3.1 Life cycle phases and guidance from standards and regulations

This section covers issues that needs to be considered during system development and the what guidance the standard EN 50126 gives. Focus is on how the RAMS life cycle phases effects the system development. The RAMS life cycle phases starts with concept and ends with decommissioning and disposal. In the scope of this thesis the phases concept to system requirements are covered. There are also examples of system requirements following Swedish regulations.

3.1.1 Phase 1. Concept

During the concept phase the goal is to develop understanding for the system and to build a basis for subsequent life cycle phases. Here is presented some very brief examples from the system examined in this thesis and the different topics one has to consider in the concept phase.

The scope, context and purpose of the system

First of all, one have to define the system/product in question. Attention is needed in defining the scope, the context and purpose of the system. This is an extensive feat that sets the direction for further steps in the life cycle. The full conceptual description of the system in focus is presented in section 3.2.

The environment of the system

Furthermore the environment the system operates in needs to be considered and can be divided into subcategories as

- Physical issues
- Potential system interface issues
- Social issues
- Political issues
- Legislative issues
- Economical issues.

A number of issues are identified from these categories, the following list is arranged according to these categories and are examples of things that need to be considered.

> Vibrations, the unit is exposed to temperature variations, size of the unit, the possibility to place antennas on the outside of the train, limitations in the possibility to install new hardware.
>
> Electromagnetic interference from other system as well as this system, loss of power, limited cable length allowed for RS232, data transmission rates on RS232, varying wireless reception over geographic areas, GPS signal strength over different geographic areas.
>
> Demands from different stakeholders regarding development.
>
> None political issues.
>
> Safety standard required for train systems, different train regulations in different countries.
>
> Use of COTS hardware to keep costs down.

And of course there are more issues that needs consideration.

Sources of hazards which could affect the system RAMS performance

To be able to handle hazards one has to know the sources of them. To help with that one should start to examine sources of hazards which here are classified into several different categories and this list can be used as a tool to identify more sources.

General

- Interaction with other systems

Systematic failure

- Errors in requirements
- Design & realisation inadequacies
- Manufacturing deficiencies
- Inherent weaknesses
- Software errors
- Operation instruction deficiencies
- Human errors

Random failure

- Operating modes
- Environment
- Stress degradation
- Wear out
- over stress
- Etc.

External disturbances

Human errors

Diagnostics

- Manual
- Automatic

Logistics

Human factors

- Interaction with humans

Maintenance procedures

- Preventive maintenance
- Corrective maintenance

Once more the list of hazards gets extensive and the feat is to fully cover all aspects of the systems. A handful of example hazards could be: The system disturbs or gets disturbed by the system which it is connected to, the system is not fully understood by system engineer, engineer lacks ability to develop system, lack of specifications, lack of control, depends on the reliability of other system, software bugs, design errors, lack of proper manual and instructions for scheduled maintenance, conditional maintenance diagnostics internal and external etc.

3.1.2 Phase 2. System definition and application conditions

The second phase of the RAMS life cycle is about defining and setting up the operational context of the system in the aspects of how it influences the RAMS performance of the system. The main objectives are to: define the system and its mission profile, define the boundary of the system, establish application conditions, define the scope of system hazard analysis and to establish the RAMS policy as well as a safety plan for the system.

To state how the system is defined one should give a description of the system with its long term operating- and maintenance-strategy and conditions on that. It should also include system life-time considerations as well as logistic considerations. The system boundary needs to address interfaces with a number of things, such as interfaces with: the physical environment, other technological systems, humans; other railway duty holders as well as with existing infrastructure. This will be a guide to define constraints imposed by existing infrastructure and to define the system operating and maintenance conditions. One should also review past experiences for similar systems.

A RAM plan that describes the RAMS policy and strategy to be applied in the later steps of the life cycle shall be established. This RAM plan includes details about the scope of the plan and the planning of RAM activities and the plan should be agreed by the railway duty holder and the railway supplier for the system. The RAM plan includes among other things analysis, related RAM tasks and testing for: system management, reliability, maintainability and availability. This document as well as the safety plan should be considered a living document and be updated continuously through the life cycle phases.

3.1.3 Phase 3. Risk analysis and evaluation

The objectives of the third phase are to: identify hazards associated with the system, identify the events leading to the hazards, determine the risk associated with the hazards and establish a process for on-going, or continuous, risk management. At the early stages and particularly in this life cycle phase the risk analysis is performed with the aim to form a foundation for risk based RAMS requirements. The risk analysis is also performed in later steps of the RAMS life cycle in order to make sure the system meets its safety requirements and to be a part of on-going risk management.

How to handle identified hazards

Items identified as hazards should be recorded in an hazard log. A plan for handling hazards should be developed, the comprehensiveness of the plan is depending on the scope and complexity of the system and also how severe the identified hazards are. This is an example of an identified hazard related to proactive maintenance.

H 4: Corrupted data from ATP recorder to client.

Even though it could have existed for some time the possibility to discover corrupted or damaged data is when it is processed to be used, for example in the parser. The state the system is in when this happens is when the unit is in its operational state, i.e. in its running state. The cause could be due to environmental issues such as problems with the physical connection to the event recorder or something internals such as faulty hardware. Corrupted data is only an issue when used for analysis, it will not affect the system performance. Consequences regarding the railway system are more severe, for example if the data is used as basis for proactive maintenance the data need to be correct to make correct decisions. These decisions are based on statistics so a single element of erroneous data will not have as hazardous effects as having a systematic error in values.

For the risk level one has to argue about the frequency of occurrence for this hazardous event. In the risk analysis section of EN 50126 there are different categories for the frequency. This hazard fits in the description of the category of occurrences called remotely or lower. It is described as its likely to occur sometime in the life cycle. The hazardous event is probably not going to happen several times a day and it is not safe to say it is never going to happen. To classify the severity level, consequences for persons or the environment has to be studied. In this case, the usage of erroneous data for planning maintenance on the brake system could lead to faulty brakes. But, there are still other tools to prevent breakdown of the braking system today. Since this is used as a tool for planning maintenance and does not directly effect person safety the severity level can be categorised as insignificant according to EN 50126. To decide the final risk level a frequency-consequence matrix is used and for that risk acceptance should be based on a generally accepted principle such as "As Low As Reasonably Practicable (ALARP principle as practised in UK) or Minimum Endogenous Mortality (MEM principle as practised in Germany). In EN 50126 a typical risk evaluation and acceptance matrix is exemplified. Following that matrix this identified hazard is evaluated as Negligible and can be acceptable without any agreement from Railway Authority and therefore no further action in risk reduction/control is needed. Regarding Safety Integrity, this is often interpreted as that this type of functionality is on SIL0 level.

On the other hand, if a predicted risk needs action, it should be considered to introduce the following types of risk reduction measures:

- introduction of a safety or monitoring system
- introduction of design measures
- computational evidence and/or representative testing
- operational measures
- maintenance measures

3.1.4 Phase 4. System requirements

As stated in the standard, the fourth phase of the life cycle has the main objective to specify the overall RAMS requirements for the system under consideration. One shall also establish a RAM program that shall be agreed by the Railway Authority. The RAM program should include details about: Management of the RAM requirements and the policy and strategy for achieving those, reliability analysis and prediction as well as how to handle reliability planning and testing, handling of maintainability- analysis, prediction, planning and data acquisition for analysis of maintainability improvements, and finally availability analysis and demonstration of early operation. The RAM program for the system examined in this thesis is not presented here.

One alternative of how to achieve suitable levels on the RAMS requirements is to look at similar systems. In this case, with the system under consideration in the thesis, the device reads information from the ATC recorder which allows for direct connection to the information bus that the Swedish Specific Transmission Module or STM device is also connected to. The RAMS system requirements for this device is regulated by the Swedish government agency Transportstyrelsen.

In short, the requirements for the STM are (Banverket, 2008):

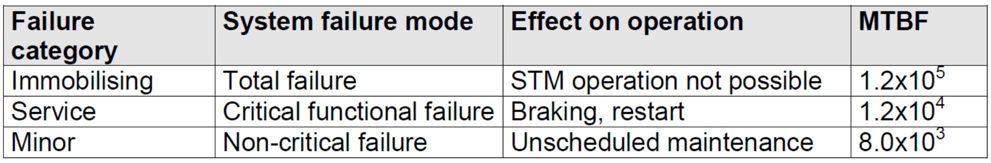
Applicable Standards

R1 In the design and construction of the STM, the following standards shall apply: EN 50126:1999, EN 50128:2001 and EN 50129:2003.

Reliability requirement

R3 The applicable MTBF values for different failure categories shall be as in table 3.1.

Table 3.1: The applicable MTBF values for different failure categories.



Failure category	System failure mode	Effect on operation	MTBF
Immobilising	Total failure	STM operation not possible	$1.2\text{x}10^5$
Service	Critical functional failure	Braking, restart	$1.2\text{x}10^4$
Minor	Non-critical failure	Unscheduled maintenance	$8.0\text{x}10^3$

Availability requirement

The availability of the STM is specified as the time in which STM is in a state to perform its mission.

R5 The technical availability (A_a) of the STM module shall be at least 0.9999885. A_a is defined as

$$A_a = \frac{MTBM}{MTBM + MTTM}, \tag{3.1}$$

where
MTBM = Mean Time Between Maintenance (hours)
MTTM = Mean Time To Maintain (hours)
In this case the MTTM takes into account the mean time required to maintain rolling stock both for preventive and corrective maintenance but not including logistical and administrative delays.

Maintainability requirement

R6 Unless otherwise agreed, the STM shall be designed so as not to require regular periodic maintenance. In case of this kind of maintenance, the manufacturer shall specify any necessary or prohibited maintenance procedures and the Mean Time between (Planned) Maintenance (MTBM).

R7 If maintenance is needed, the Mean Time to Repair (MTTR) shall be less than 2 h. MTTR = Operational Standstill time for the vehicle caused by fault on STM including fault diagnosis time and check out time, but not including logistic delay nor administrative delay.

Safety requirement

Top hazards affecting the ATC on-board system include:
-overspeed

R8 The Tolerable Hazard Rate (THR) shall not exceed $1.0 * 10^{-10}$ f/h for the STM in the intended applications.

The RAMS requirements for the STM-device is set very high due to the fact that it is used to interpret the desired speed of the train as well as when the train is supposed to brake. The requirements for the system described in this thesis is user for out of the loop analysis and warnings and it is therefore not suitable or desirable to adopt the STM requirements as they are.

3.2 System concept

3.2.1 Client: scope, context and purpose

The client device is installed in the locomotive of the train. Main function is to read out data from the train's ATP recorder. Read out data is then saved and linked with GPS coordinates for tracking events to geographical areas. Data types relevant for live tracking function are analysed in real-time while most of the data is sent to a central server for later analysis. Warning and information messages from live-tracking analysis are sent either by email or SMS. The goal with this type of system is to increase availability of maintenance data and the possibility to make analyses over time as well as over an entire fleet of locomotives.

3.2.2 Main functionality

ATP recorder read out

This function reads out data from the memory banks of the ATP recorder. The procedure is as follows, a read out request is sent from the client to the ATP recorder using a serial interface, RS-232, ATP recorder sends back requested data and the client saves it as raw data in a file on the internal memory. See figure 3.1.

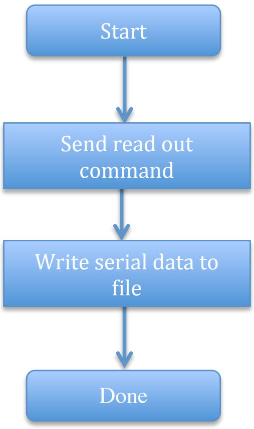


Figure 3.1: Read-out function.

Log GPS coordinates

GPS coordinates are provided by the internal GPS module. If GPS coordinates are on the right format, the client saves the coordinates together with a time stamp to a text file. If not, the client will try to receive new coordinates for up to 10 minutes before restarting the module and repeat the procedure. See figure 3.2.

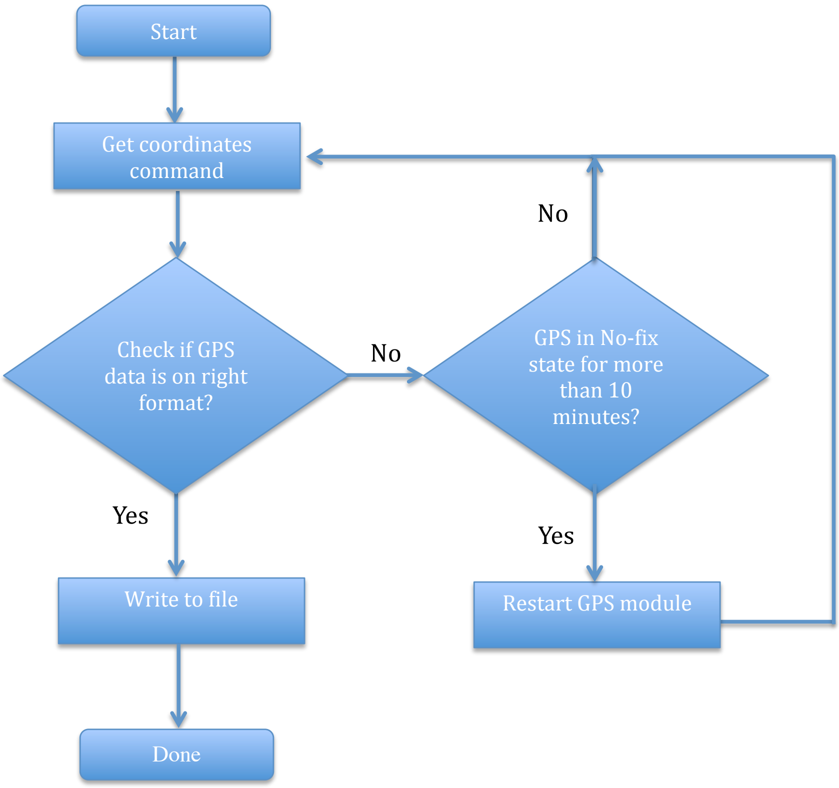

Start
Get coordinates command
Check if GPS data is on right format?
No
GPS in No-fix state for more than 10 minutes?
No
Yes
Yes
Write to file
Restart GPS module
Done

Figure 3.2: GPS coordinates.

Send data to server

Gathered data is being compressed and sent to the central server at regular intervals. The client uses HTTPS protocol for safe file transfer. If file transfer is interrupted or if no network connection is available, the client will try to send the file again until successful transfer is accomplished, this is illustrated in figure 3.3.

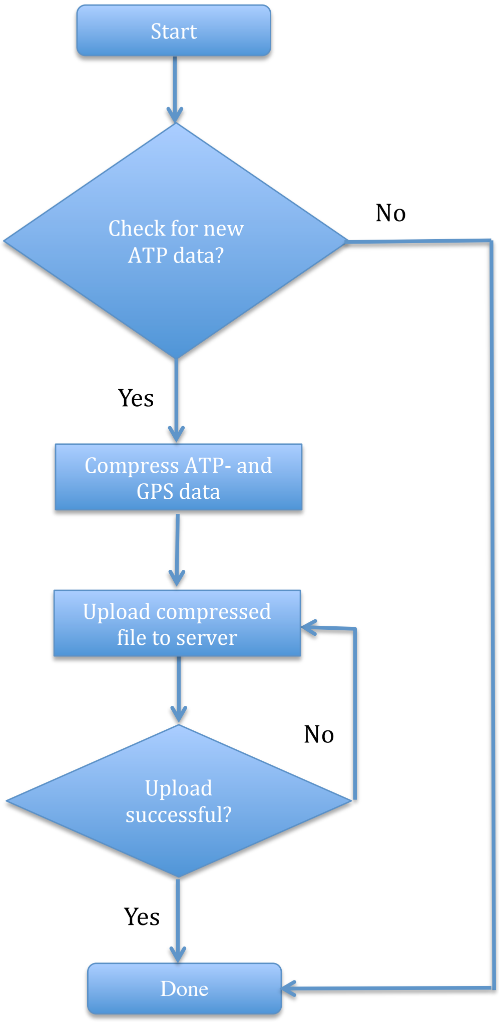


Figure 3.3: Client to server data transfer.

Live-tracking

This function uses models for different live tracking use-cases. Data relevant for each use-case is analysed and checked against the models for detecting errors and faulty conditions. Depending on the outcome of the model checking, SMS and email messages are sent as warning or notification. Gathered data that does not require real-time analysis can advantageously be sent to a central server for processing. Embedded computer power and storage space are costly and should therefore be kept as low as reasonable possible. Moving the analysis process to a central server should be the first choice when time is not crucial. Other benefits of using a central server are the possibility to collect data from a whole fleet of trains. With data from different trains, analysis and statistics can easily be made available online through a web interface. Despite the advantages of a central analysis, there are some cases when data needs to be processed directly on the train in order to do instant actions, this is referred to as live tracking in the railway industry. Live tracking is a way to use available train data for detecting errors and faulty conditions of both the train and trackside equipment. After an error or faulty condition has been detected, a suitable message or notification is sent to the responsible in the corresponding area.

3.2.3 Live tracking use cases

Balise read error

When a train passes a balis, data is transferred wireless from the node to the train. A quick analysis on the train shows if the data is corrupted, this could tell if the node for example is damaged or if something is covering the node. The GPS coordinates together with the node id tells the operator which node to look up and repair.

Railway track conditions

A common problem referred to as slippery rail is when moist leaves end up on the rails. The combination of moist and leaves is a huge problem because the trains wheels slip on the surface and reduce the braking ability, which could lead to dangerous situations. By measuring the wheel spin its possible to draw conclusions about the railway track conditions and alert the railway maintenance and warn the locomotive driver.

High power consumptions

Disproportionately high power consumptions could reveal problems with the train like a broken or worn wheel bearing or a stuck brake. Such detection of faulty components could save money in waste of electric power and prevent further damage to the train and rails.

Brake performance

A model for braking could tell if the brake performance, in terms of retardation not corresponds to the pressure in the brake pipe. This could help detect faulty brakes or worn out wheels.

Shock values

If the system detects high shock values, assumption can be made that the train has been in a collision or other accident and an emergency message can be sent out automatically. The GPS position and information about the train can help emergency services act faster and more prepared.

Predicted brake curve

For each speed limit change or stop signal, trains have calculated predicted braking curves. These braking curves depend on several different aspects as train parameters, track conditions and rail gradient. Information about how actual braking curves match predicted curves could be useful for operators.

3.2.4 System boundaries and interfaces

The client is interfaced with the ATP recorder which it should be able to read information from. The client it self should be able to communicate with GPS satellites through a GPS module as well as send data, via wireless terrestrial networks, to the server for storing and analysing data from clients on multiple locomotives. The system boundary should be defined as in figure 3.4.

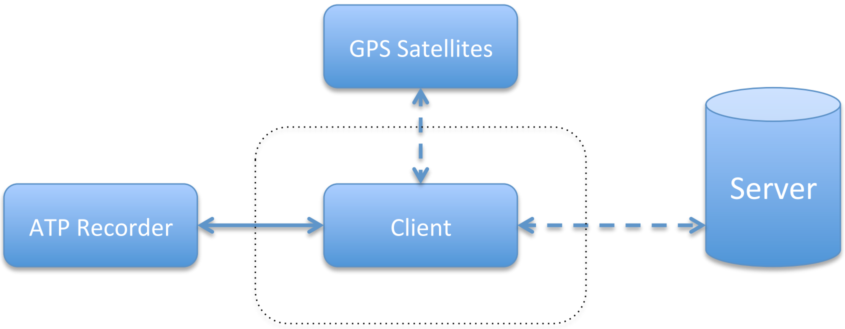


Figure 3.4: Client interface boundaries, solid arrow represent wired connection and dashed represents wireless.

3.2.5 Working environment

Physical issues

The client should be able to withstand the operational conditions imposed by being installed in the locomotive, including pressure differences, temperature changes, high air humidity, shocks and vibrations. It should be no larger than to fit inside a 19-inch rack with a maximum height of 2 units and be possible for service personnel to access for maintenance purposes. Otherwise the client is not intended to be accessible for passengers and the public. Antennas for cellular network and GPS position should be able to be placed outside of the train to achieve sufficient signal reception. The client should not affect the performance of other devices installed on the train.

Potential system interface issues

To make the client general it should be able to connect to a number of devices, protocols for communication should include RS232 since it is one of the most common. The software architecture should allow for configuring of other protocols. The client should have the possibility to connect external antennas to increase wireless functionality.

Social issues

One issue to consider is what the public opinion is about the fact that the internal data types of a train is being logged and sent wirelessly in the air with the possibility that someone could hack the communication. The client should not be able to influence other system and the possibility that someone taps into the wireless communication is not seemed as a threat. Gathered data is not seen as secret or safety related. Without knowing the exact sequence of data, identify the different data types from the transferred raw data would be very difficult. With this background, the data communication does not need to have any further encryption besides whats included in HTTPS communication protocol.

Political issues

There are no direct regulations of how one should specify this type of new system.

Legislative issues

The system should conform to EU directive 2008/57/EG and the Swedish interpretations set up by Transportstyrelsen (Banverket, 2014).

Economical issues

Developing a system of this kind is a complex task. Development according to standard EN 50126 will cost more than to not do so, one have to weigh the benefits of reaching the market with a certified product compared to not doing so.

3.2.6 Data classification

The different systems and subsystems of the train holds all sort of information about the train. Data types listed in figure 3.5 are not a complete set of data available, this is an selection of data types that by regulations need to be recorded in the train event recorder. Decisions whether a certain data type is analysed locally on the client or on the central server are based on the time constrains for the given function. Live tracking features have a natural stricter time constrain compared to maintenance analysis.

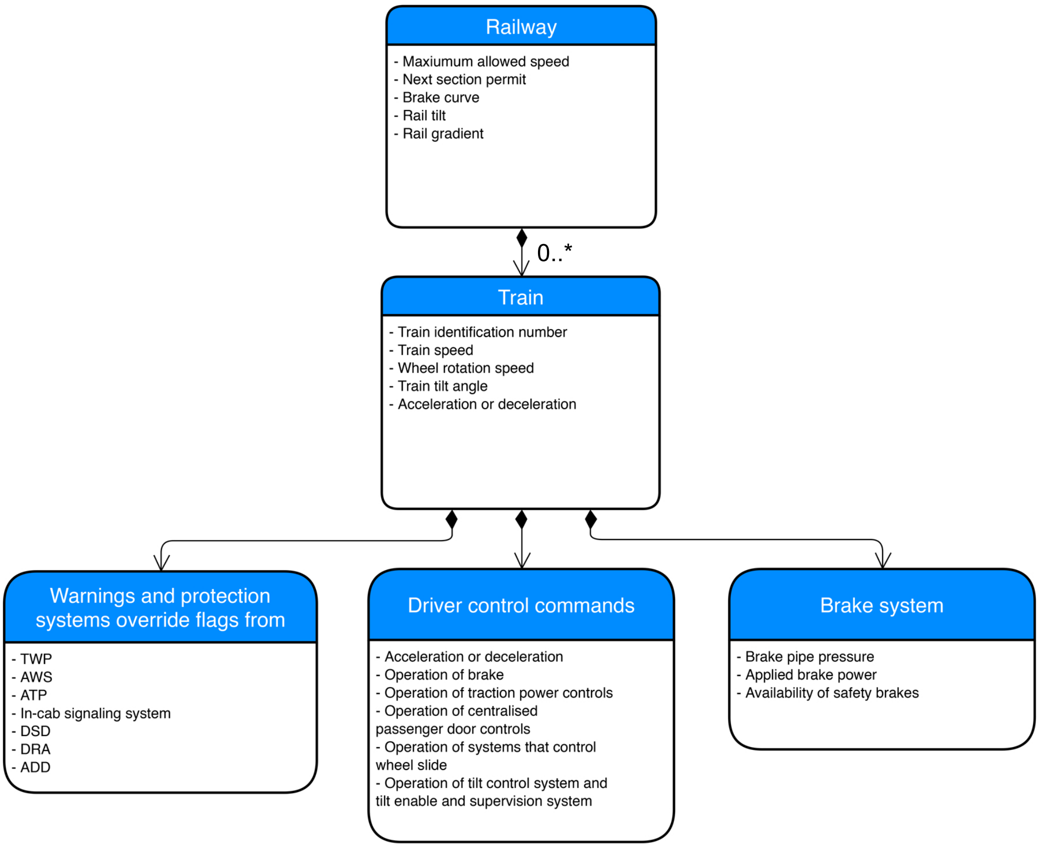

Railway
- Maxiumum allowed speed
- Next section permit
- Brake curve
- Rail tilt
- Rail gradient
0..*
Train
- Train identification number
- Train speed
- Wheel rotation speed
- Train tilt angle
- Acceleration or deceleration
Warnings and protection systems override flags from
- TWP
- AWS
- ATP
- In-cab signaling system
- DSD
- DRA
- ADD
Driver control commands
- Acceleration or deceleration
- Operation of brake
- Operation of traction power controls
- Operation of centralised passenger door controls
- Operation of systems that control wheel slide
- Operation of tilt control system and tilt enable and supervision system
Brake system
- Brake pipe pressure
- Applied brake power
- Availability of safety brakes

Figure 3.5: An overview of the data taxonomy

3.2.7 General RAMS implications

According to the standard EN 50126 railway RAMS is a major contributor to the Quality of Service and to set suitable RAMS requirements one has to identify the factors influencing the system and particularly the human factors. To achieve a dependable system one has to find the optimum combination of RAMS elements for that particular system while at the same time the RAMS elements are interlinked in the sense that a mismanagement or conflict in the RAMS requirements may be hindering in achieving a dependable system. The complexity of the RAMS requirements should reflect the complexity of the system and how much the system under construction influences factors as people, environment, economics and so on.

Reliability

Looking at reliability in the specified application and environment, different failure modes for the system can be looked upon.

Total failure

Partial failure of specific functionality

Minor failure, e. g. reading error

Without expanding on the specific failure modes the worst operation that could occur is that the system does not respond in any way. Since this is seen as a tool for collecting data and no data will be lost from the ATC recorder, all train data is still available to collect anew, there are no consequences with just resetting the system to an operational state. Since this system does not affect the general railway system and how it operates the reliability of this system has no need to be specified with a more strict MTBF than the STM.

Availability

Since this device is in no manner time critical the availability does not need to be set as high as the STM device.

Maintainability

It is reasonable that the device is designed not to require regular periodic maintenance. If maintenance procedures are needed the most effective way would be to simply replace the hardware/software.

Safety

Relating to the THR for the STM device it is deemed that the gathering unit is allowed to have a significant lower safety level as well as the identified hazards is not deemed to affect people or environmental safety.

3.3 Risk analysis

Risk analysis is a systematic process of evaluating all available information to identify sources of hazards and the assessing risk. It is often recommended that the risk analysis is performed with methods such as Hazard and Operability Analysis (HAZOP), Failure Mode, Effects and Criticality Analysis (FMECA) or Fault Tree Analysis (FTA).

3.3.1 Risk acceptance

The Swedish government agency has divided risk acceptance into three different categories.

Accepted praxis

Reference system

Qualitative and quantitative risk acceptance principles

Accepted praxis can be used if there is a common and known practice in the railway industry, if it is relevant for management of potential hazards. Hazards that are controlled according to this praxis is acceptable and do not need further analysis. Examples of accepted praxes are TSIs (Technical specifications for interoperability), notified national rules and EN-standards.

The principle of using a reference system can be used if you can find a reference system that is tested with an approval safety level, that has similar functionality and interface, that is used under similar operation conditions as well as under similar environmental conditions. Hazards that are present in the reference system is then accepted as hazards in the system under analysis and the safety requirements for the reference system should be implemented and fulfilled for the system under analysis.

With the qualitative and quantitative risk acceptance principles the hazards are evaluated against criteria for risk acceptance. Examples of principles for risk assessment are ALARP (As Low As Reasonably Practicable), MEM (Minimum Endogenous Mortality) and GAMAB (Globalement Au Moins Aussi Bon). These principles are common for designing new systems and the criteria can be both qualitative or quantitative or both at the same time, as with the examples of THR and SIL. Criteria are set on each level of the design all the way to the highest or top level.

Transportstyrelsen has a specific criteria for risk acceptance that governs risk sources in technical systems: If there is a erroneous function has a direct potential for catastrophic consequences there is no need to further reduce the risk if the occurrences of the error are lower than 10^{-9} per hour (Robert Bylander).

3.3.2 Hazard log

Provided in EN 50126-2 are checklists for hazard identification in railway systems. These checklists are divided in six different areas, functional, mechanical, construction, electrical, operation and support and occupational health. With support from these checklists a number of hazards have been identified for the new system.

Warnings and alarms

H 1: Failure to deliver warning messages when live tracking hazards has been identified.
H 2: Failure to identify potential hazards that should be detected by live tracking and there after send a warning message.

Maintenance and support

H 3: Risk of electric shock when installing or replacing client unit.

Software malfunction

H 4: Corrupted data from ATP recorder to client.
H 5: Corrupted data from GPS module.
H 6: Data transmission error from client to server.

H 7: GPS coordinates not accurate.
H 8: GPS coordinates does not match ATP data timestamp.

Software crash

H 9: System reboots as result of software crash.
H 10: System freezes as result of software crash.

Recovery from failure

H 11: Time and date settings lost after downtime or reboot.
H 12: Information lost due to system freeze.
H 13: Information lost after downtime or reboot.

Environment influences

H 14: System freezes due to high temperatures.
H 15: System reboots or freezes due to voltage spikes.
H 16: Client hacked.

Mechanical hazard identified

H 17: Electric failure due to corrosion on client circuit.
H 18: Smoke or fire due to overheated client.

Insect, rodent or mould damage

H 19: Electric failure due to shorts in client caused by insects.

Ventilation

H 20: Client overheating as a result of insufficient ventilation in the rack compartment.

Shock and vibration

H 21: Antenna cables disconnected due do large vibrations or shock.
H 22: Lost communication with ATP-recorder due to loose serial cables after exposed to large vibrations or shock.

Humidity

H 23: Electric error due to circuit corrosion after high humidity.

Foreign bodies and dust

H 24: Overheating due to dust in client ventilation
H 25: Fan break down causing overheating.

Overheating

H 26: System shut down due to overheating.
H 27: System freezes due to overheating.

Electromagnetic interference and compatibility

H 28: Clients cellular network module interference with railway cellular network, GSM-R.

Loss of power

H 29: System shutdown and reboot after loss of power.

3.3.3 Hazard analysis

This section gives a few examples of how hazards are treated and analysed.

Functionality failures

The client is passive in the sense that it does not have any influence on the train control system. Data is only gathered and analysed, the client lacks the actual physical connection and possibility to feed back commands and information to the train control system. This system architecture is the main reason why the functional requirement for the client is not as strict as for the STM and European Rail Traffic Management System, ERTMS. Hazards identified regarding system functionality failures as data read error, system crash and freeze do not have any harmful consequence due to the inability of the client to actually control the train functions.

H 18: Smoke or fire due to overheated client

One identified hazard is fire or smoke as a result of high temperatures in the client. During operational state, the client unit produces heat. If the electric cooling fan fails, the client unit could end up overheated. The most common reason for electric cooling fans to fail is due to large amounts of dust or foreign objects stuck in the fan. The consequences of a overheated client could be severe. At high temperatures smoke and eventually fire could occur which are direct hazards for the locomotive operator and other nearby electronic equipment. Assumption made by looking at similar products leads to the conclusion that this hazard is remotely likely to happen. After the following risk reduction measures the risk level is seen as negligible.

- Filter protecting the fan and client from dust and foreign objects. Included in IP classification.

- Flameproof coating or materials.

- Software and/or hardware overheating protection.

H 28: Clients cellular network module interference with railway cellular network, GSM- R

Included in the client is a module for cellular data transmission. The ERTMS on the train utilises the cellular network, GSM-R, for data transfer between rail-side equipment and the train. Interference between the module and this network could lead to hazardous events. Lost or not delivered information about the upcoming rail sections could lead to collision with a stationary train or rail maintenance personnel. According to Trafikverket the interference level is acceptable if regulations from Swedish government agency Post- och telestyrelsen, PTS are followed for transmitting on the cellular network. Modules approved for the Swedish market follows these regulations.

These two hazards described handles the top identified hazards that can influence the train system. Further on the thesis discusses the advantage of utilising a gathering system, and how that can be done, before returning to presenting the resulting requirements derived from the safety analysis.

3.4 System requirements

These requirements are the result of the system concept in section 3.2 and the risk analysis in section 3.3. The first list of requirements relate to one or more hazards identified during the risk analysis process. This list of requirements is neither complete nor comprehensive but rather seen as an example of requirements essential for the safety aspect. The second list relate to the functions described in the system concept section. Other hardware requirements not specified should comply with the standard EN 50155 "Railway applications - Electronic equipment used on rolling stock".

3.4.1 Hardware requirements

The first requirement, R1.1 in table 3.2 is identified to minimise the hazard H3 from hazard log in section 3.3. Hazard H3, "Risk of electric shock when installing or replacing client unit.", is identified as a hazard under category "Maintenance and support" from the hazard checklist in standard EN 50126-2. The requirement R1.1, "The electric connection for the power supply shall follow the standard IEC 60320 and shall also comply with the isolation requirements of standard EN 50155.", ensures that the power connection is protected against insertion of fingers and therefore lowers the risk of electric shock during installing or replacement of the unit. The rest of the of the hardware requirements in table 3.2, R1.2 - R1.9, are identified using the same procedure for other hazards identified under different categories from the checklist.

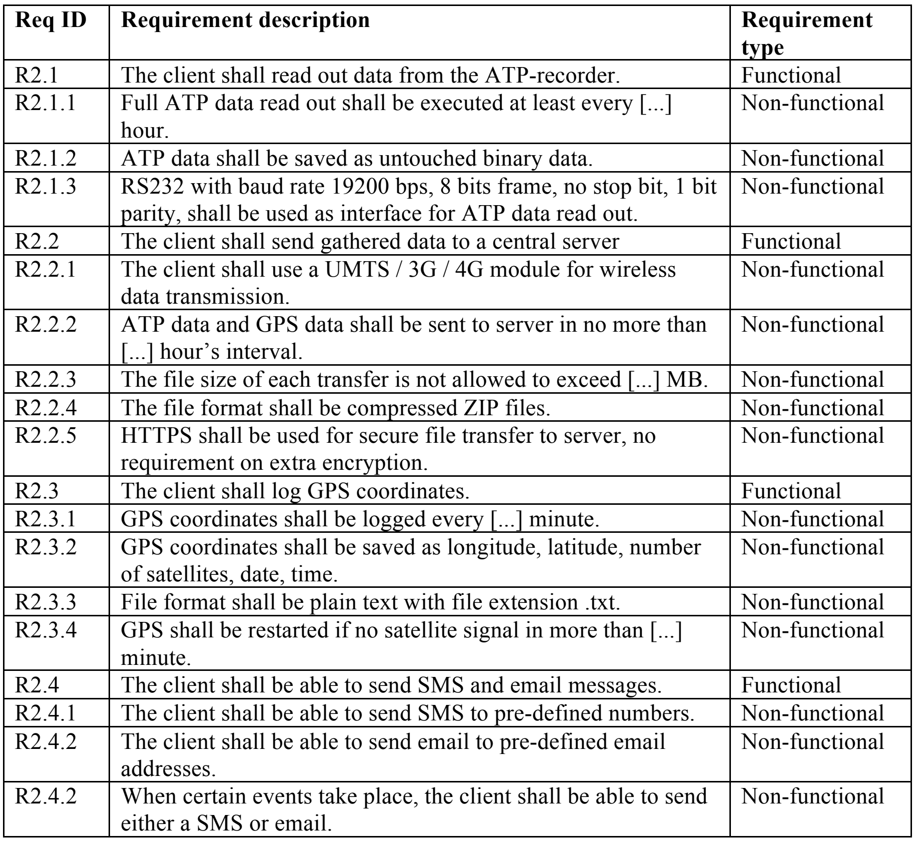
Table 3.2: Hardware requirements and their corresponding hazards.

Req ID	**Requirement description**	**Corresponding hazard ID**
R1.1	The electric connection for the power supply shall follow the standard IEC 60320 and shall also comply with the isolation requirements of standard EN 50155.	H3
R1.2	The client shall have backup battery for time and date. This battery shall have a minimal lifetime of [...] years.	H11, H12, H13
R1.3	The client shall withstand and be able to fully operate at an internal cabinet temperature range of -40 to +70 °C following standard EN 50155	H14
R1.4	The power supply of the client shall be able to handle voltage spike levels defined in train standard EN 50155	H15
R1.5	The client shall comply with the humidity requirements of standard EN 50155.	H17, H23
R1.6	The client shall be made of fire resistant materials.	H18
R1.7	The client and connectors must pass the shock and vibration tests described in standard EN 61373.	H21, H22
R1.8	The client shall follow standard IP 5x on dust and foreign objects protection.	H19, H24, H25
R1.9	Client must comply with requirements on EMI and EMC described in standard EN 50155	H28

3.4.2 Functional and non-functional requirements

In table 3.3 and table 3.4 are functional and non-functional requirements. The functional requirements as R2.1, R2.2 and R2.3 are main functions identified in the concept phase in section 3.2.2. The non-functional requirements as R2.1.x, R2.2.x and R2.3.x are needed to specify and define the functional requirements further. The non-functional requirement describes how good the system is supposed to behave rather than describing what the system is supposed to do.

Table 3.3: Functional and non-functional requirements.



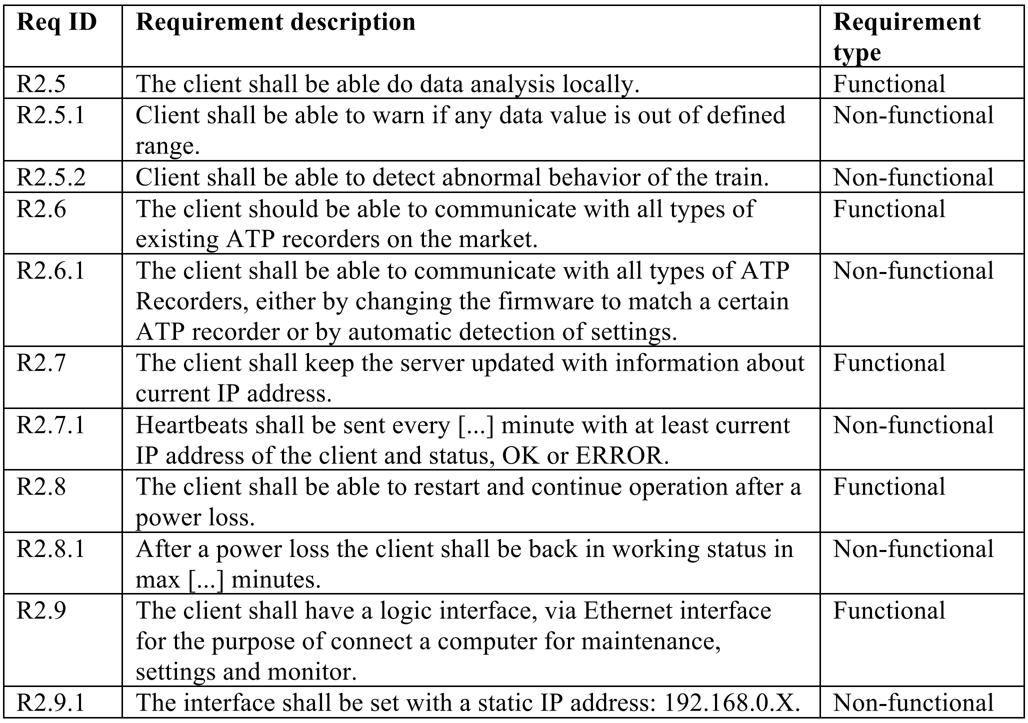
Req ID	Requirement description	Requirement type
R2.1	The client shall read out data from the ATP-recorder.	Functional
R2.1.1	Full ATP data read out shall be executed at least every [...] hour.	Non-functional
R2.1.2	ATP data shall be saved as untouched binary data.	Non-functional
R2.1.3	RS232 with baud rate 19200 bps, 8 bits frame, no stop bit, 1 bit parity, shall be used as interface for ATP data read out.	Non-functional
R2.2	The client shall send gathered data to a central server	Functional
R2.2.1	The client shall use a UMTS / 3G / 4G module for wireless data transmission.	Non-functional
R2.2.2	ATP data and GPS data shall be sent to server in no more than [...] hour's interval.	Non-functional
R2.2.3	The file size of each transfer is not allowed to exceed [...] MB.	Non-functional
R2.2.4	The file format shall be compressed ZIP files.	Non-functional
R2.2.5	HTTPS shall be used for secure file transfer to server, no requirement on extra encryption.	Non-functional
R2.3	The client shall log GPS coordinates.	Functional
R2.3.1	GPS coordinates shall be logged every [...] minute.	Non-functional
R2.3.2	GPS coordinates shall be saved as longitude, latitude, number of satellites, date, time.	Non-functional
R2.3.3	File format shall be plain text with file extension .txt.	Non-functional
R2.3.4	GPS shall be restarted if no satellite signal in more than [...] minute.	Non-functional
R2.4	The client shall be able to send SMS and email messages.	Functional
R2.4.1	The client shall be able to send SMS to pre-defined numbers.	Non-functional
R2.4.2	The client shall be able to send email to pre-defined email addresses.	Non-functional
R2.4.2	When certain events take place, the client shall be able to send either a SMS or email.	Non-functional

3.5 Verification

The standard EN 50126 states that there are no specific verification tasks to be done for the system requirements other than more generic verification that is performed at several levels of the development. One shall evaluate the correctness and adequacy of the safety analysis, do a verification of compliance with specified deliverables in the current life cycle phase as well as to deliverables of former phases and finally do a evaluation of the correctness, consistency and adequacy of test cases and executed tests. How this is performed is presented in the safety plan.

The scope of the safety plan is established early in the life cycle and is done by the means of defining the system as well as its safety functions, their integrity and the process to implement these functions. The functionality of the system described in this theses is concluded non-safety critical and a more detailed safety plan is therefore left out according to the principle: "There is no sense in producing large documents for small and simple products only to satisfy the standard" (EN 50126-2).

Table 3.4: Functional and non-functional requirements.



Req ID	Requirement description	Requirement type
R2.5	The client shall be able do data analysis locally.	Functional
R2.5.1	Client shall be able to warn if any data value is out of defined range.	Non-functional
R2.5.2	Client shall be able to detect abnormal behavior of the train.	Non-functional
R2.6	The client should be able to communicate with all types of existing ATP recorders on the market.	Functional
R2.6.1	The client shall be able to communicate with all types of ATP Recorders, either by changing the firmware to match a certain ATP recorder or by automatic detection of settings.	Non-functional
R2.7	The client shall keep the server updated with information about current IP address.	Functional
R2.7.1	Heartbeats shall be sent every [...] minute with at least current IP address of the client and status, OK or ERROR.	Non-functional
R2.8	The client shall be able to restart and continue operation after a power loss.	Functional
R2.8.1	After a power loss the client shall be back in working status in max [...] minutes.	Non-functional
R2.9	The client shall have a logic interface, via Ethernet interface for the purpose of connect a computer for maintenance, settings and monitor.	Functional
R2.9.1	The interface shall be set with a static IP address: 192.168.0.X.	Non-functional

3.5.1 Verification of the hardware requirements

Regarding the requirements identified in this thesis, requirement R1.1, R1.3, R1.4, R1.5 and R1.9 should be verified by the responsible group for hardware design according to tests described in standard EN 50155 "Railway applications - Electronic equipment used on rolling stock". The requirement R1.2 for battery backup should be verified by measuring the power consumption and calculate estimated need of battery capacity. To verify requirement R1.6, material compliance from standard EN 13501-2 must be fulfilled. Test described in standard EN 61373 verifies requirement R1.7 and specification of IP standard for requirement R1.8 is found in IEC standard 60529.

3.5.2 Verification of the functional and non-functional requirements

As a part of the software development, test for functional and non-functional requirements are designed. It is highly recommended in standard EN 50129 that “reviews should be carried out to demonstrate that the specified characteristics and safety requirements have been achieved” (EN 50129, 2003) . Due to the non-safety criticality of this system, it is up to the product owner to decide what is seen as adequate testing and test documentation.

Chapter 4

Analysis of preventive maintenance effects on system reliability

One advantage with logging data over time is that it enables a possibility to plan maintenance based on historical data. This chapter establishes a reliability model for a bogie system that shows how different maintenance parameters effects the reliability of the system.

The system reliability depends on the reliability of the individual components included in the system. These components have different wear characteristics and thus will wear out differently depending on the maintenance time interval and wear characteristics. Maintenance is performed on a system's components with the goal to improve either the components reliability or the system as a whole.

4.1 Safety critical components

A railway train have different number or types of cars depending on the assignment for a specific route. This results in different mileage and usage time between cars. The wear on the components of a car will not be the same as on the whole train. One example is the wear on the wheels. The wheels on a car in middle section of the train does not have as high stress as for a car in the front or back section of the train. To enable optimisation of maintenance, reliability for each car must be calculated. In this analysis, components taken into account when calculating the reliability for each car has been identified as parts of the powertrain. These components are located on the train bogie, or for bogie-less trains, same components as on the bogie except these components are mounted directly on the cars mainframe. These are not the only safety critical components, rather an example of a few selected safety critical components available on each car, and are therefore the components chosen for this analysis.

Wheel

Support the weight of the car, lateral guidance from railway track to car and transfer brake and traction power from train to rail. There are usually four wheels attached on each bogie.

Disc brake

Create the braking torque required to slow down and stop the train. Usually four disc brakes on each bogie.

Axle box

Contains the bearings for the wheel axle and handle forces from car weight and lateral movement. One bogie have four axle boxes mounted.

Reduction gearbox

Transfer torque and reduce the speed from traction motor to a speed matching the efficiency curve of the motor.

Motor clutch

Transmission of power from traction motor to the reduction gearbox. Disengage power transmission when braking or moving passive car.

Spring suspension

The suspension function is to give the car stability, keep the wheel in contact with the rail at all time and reduce vibrations and movement both in lateral and axial directions.

Traction motor

Electric traction motors, usually asynchronous but in some cases synchronous AC motors.

4.1.1 Component wear characteristics

Wear characteristic parameters for identified components have been found in the mechanical handbook (Nav, 2011). These parameters are for standard machine components and may not be accurate for railway specific components. An assumption has been made that railway components have a 50% higher β-value than standard components due to better quality and higher requirements. Those higher values are used in the calculations from here on and can be seen in table 4.1. Parameters for train wheels are slightly different and makes the wheels less suitable for preventive maintenance (Wei et al., 2012a). In a real life application these parameters needs to be determined for the specific component in use.

Table 4.1: Weibull shape, β and scale, θ parameters for components.

Component	Quantity	Parameter β	Parameter θ
Wheel	4	0.45	41
Disc brake	4	2.1	11
Axle box	4	1.95	6
Reduction gearbox	2	3.0	9
Motor clutch	2	2.1	11
Spring suspension	4	1.65	3
Traction motor	2	1.8	11

4.1.2 Improving Weibull parameters

To be able to make correct maintenance decisions, all relevant data should be considered for the reliability analysis. The basic data for finding wear characteristics for components are time to failure for non-repairable components and time between failure for repairable components. Other factors that influence the reliability of components are items such as external conditions, (temperature, humidity, etc.) and how they have failed. There is also a difference if data are found in the laboratory or in the field. The advantage with field data is that it is obtained under conditions that is absolutely true for the operation of the trains. If there are no significant randomness in the data the Weibull parameters can be derived from the components mean time to failure, but if there is, another method called Weibull probability plot can be used (Barabadi, 2013).

4.1.3 Data related to preventive maintenance

In the locomotive of trains there are many on-board systems that stores log files of their operation, unfortunately different manufacturers use different log systems as well as there is a reluctance to share their information. The minimum information that is available is the one stored in the ER. The data types that are useful for providing information related to maintenance are as seen in figure 4.1.

The data from the GPS allows for tracking positioning over time as well as it is possible to calculate acceleration/deceleration. These items can be associated with the train identification number, making it possible to determine the mileage of the locomotive as well as the cars. Knowing the mileage makes it possible to analyse mean time for and between failures more precise and will improve the reliability analysis. Besides this basic data it is possible to monitor special cases such as:

Case 1: Follow up on typical speeds on different railway sections.
Data: Maximum allowed speed, train speed.

Case 2: Follow up on braking curves and how well do they fit reality.
Data: Brake curve, deceleration.

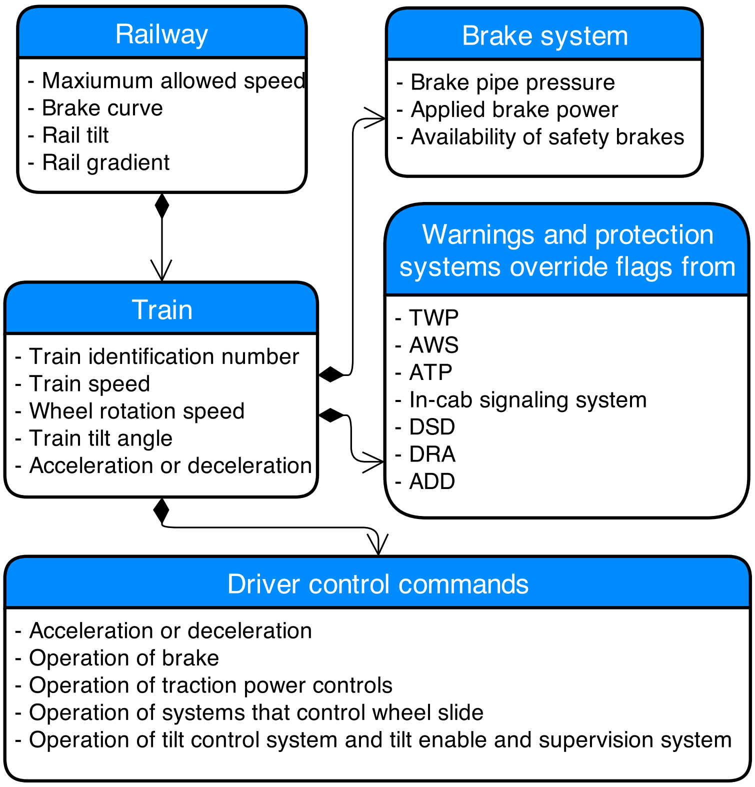

Railway
- Maxiumum allowed speed
- Brake curve
- Rail tilt
- Rail gradient
Brake system
- Brake pipe pressure
- Applied brake power
- Availability of safety brakes
Warnings and protection systems override flags from
- TWP
- AWS
- ATP
- In-cab signaling system
- DSD
- DRA
- ADD
Train
- Train identification number
- Train speed
- Wheel rotation speed
- Train tilt angle
- Acceleration or deceleration
Driver control commands
- Acceleration or deceleration
- Operation of brake
- Operation of traction power controls
- Operation of systems that control wheel slide
- Operation of tilt control system and tilt enable and supervision system

Figure 4.1: Data types useful for preventive maintenance.

Case 3: Follow up on train and rail tilt on different railway sections.
Data: Rail tilt, rail gradient, train tilt angle, operation of tilt control systems.

Case 4: Follow up on slip on railway segment.
Data: Train speed, wheel rotation speed, operation of systems that control wheel slide.

Case 5: Follow up on braking performance.
Data: Deceleration, brake pipe pressure, applied brake power, operation of brake.

Case 6: Follow up on warning system behaviour.
Data: Warnings and protection systems override flags from systems.

These cases provides added value about the operation and when deciding on maintenance.

4.2 Reliability dependencies

The components of a system have different dependencies often represented by parallel and serial behaviour. In a fault tree, dependencies of primary events are visualised mainly by logic gates AND and OR, equivalent to parallel and serial behaviour. The primary events in this case represent the reliability of the components. The figures below represent the logic gate AND and OR used in the fault tree. The use of a logic gates work as follows:

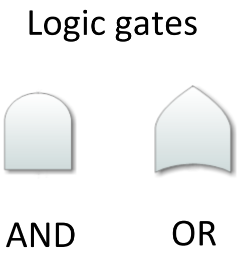


Figure 4.2: Figures for logic gates.

AND - Output event occurs if all input events occurs.
OR - Output event occurs if all any events occurs.

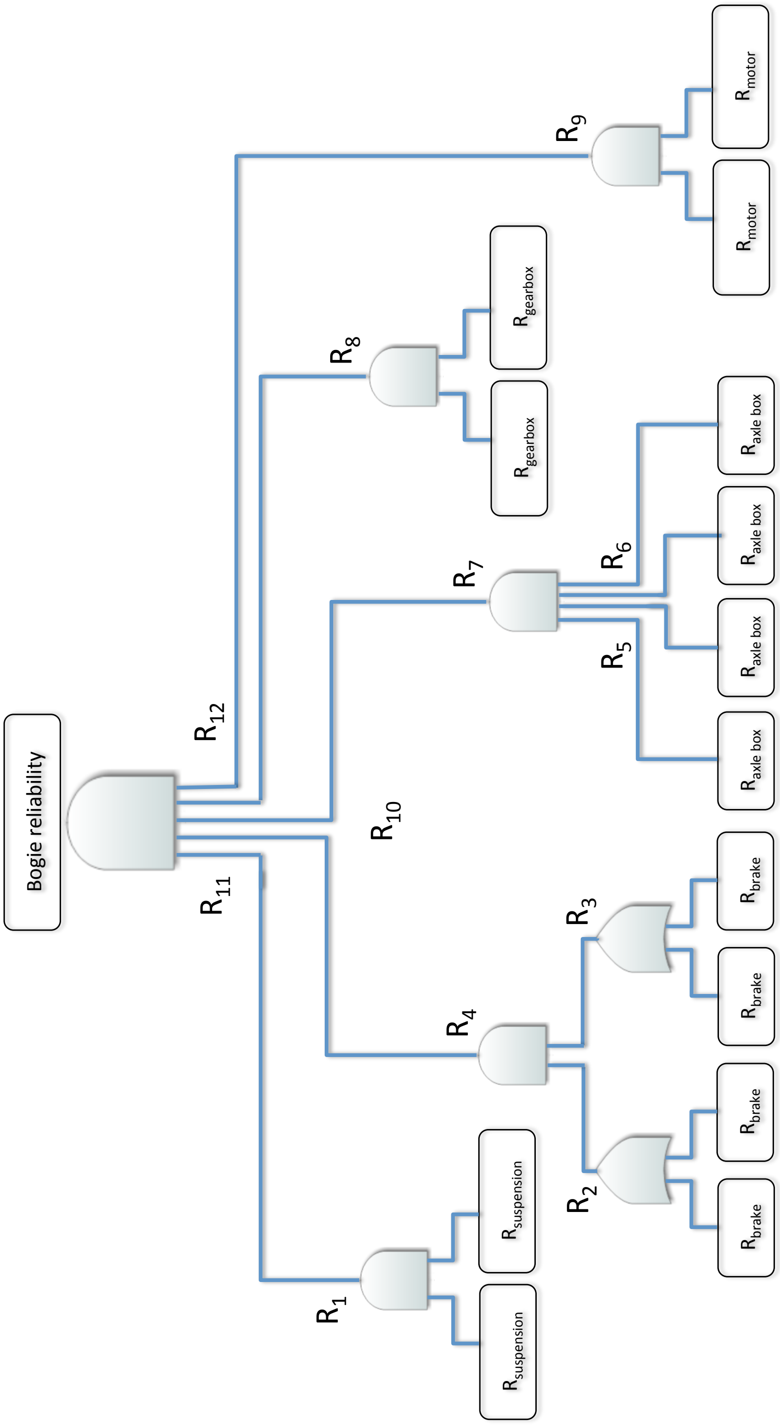


Figure 4.3: Reliability tree for one bogie.

4.2.1 Fault tree

One example of how the reliability for components of a train car bogie could depend on each other is visualised in figure 4.3. On each wheel axle there are two axle boxes, two disc brakes and two wheels attached. In this example are each one of these components allowed to fail, and still the system is considered to be in a working condition, but when a pair of any of these components on the same axle fail, the whole system fails. For the rest of the components considered, a single fail would result in system failure. An assumption has been made that three wheels on a bogie is enough to consider the bogie in a working condition, however in need of repair. Another assumption made is that there are no differences between brakes on the same axle. The wheels are not taken into account when calculating the overall reliability for the bogie, this is because of their different maintenance requirements which do not follow the same maintenance plan as for the rest of the components.

Mathematic expression for reliability

To derive a mathematic expression for the bogie's reliability as showed in the fault tree in figure 4.3, these calculations are used, equation 4.1 to 4.16.

For logic gates

$$AND = R_a * R_b \tag{4.1}$$

$$OR = R_a + R_b - R_a * R_b \tag{4.2}$$

Fault tree

$$R_1 = R^2_{suspension} \tag{4.3}$$

$$R_2 = 2 * R_{brake} - R^2_{brake} \tag{4.4}$$

$$R_3 = R_2 \tag{4.5}$$

$$R_4 = R^2_3 \tag{4.6}$$

$$R_5 = R^2_{axlebox} \tag{4.7}$$

$$R_6 = R_5 \tag{4.8}$$

$$R_7 = R^2_6 \tag{4.9}$$

$$R_8 = R^2_{gearbox} \tag{4.10}$$

$$R_9 = R^2_{motor} \tag{4.11}$$

$$R_{10} = R_4 * R_7 \tag{4.12}$$

$$R_{11} = R_1 * R_{10} \tag{4.13}$$

$$R_{12} = R_8 * R_9 \tag{4.14}$$

$$R_{bogie} = R_{11} * R_{12} \tag{4.15}$$

Reliability for a bogie

Final equation for the train bogie derived from the fault tree using logic AND and logic OR gates. This equation was used in section 4.3 for calculating reliability under different maintenance strategies.

$$R_{bogie} = R_{suspension}^2 * (2 * R_{brake} - R_{brake}^2)^2 * R_{axlebox}^4 * R_{gearbox}^2 * R_{motor}^2 \tag{4.16}$$

As seen in equation 4.16 the reliability for the bogie depends on the reliability for the individual components of the bogie system.

4.3 Results on dynamic effects of preventive maintenance

The dynamic effects of preventive maintenance were examined using the system model from chapter 4 and the reliability models presented in section 2.6 The result were visualised with Matlab. To be able to simulate the effects of preventive maintenance the process were divided into examining the effects on a single component and later on how an entire system when combined would be affected.

4.3.1 Disc break reliability

One of the components on the bogies of the train is the disc brake. It is designed to decelerate the train and is therefore a critical component. In figure 4.4 the reliability is shown for a disc brake using the Weibull parameters as described in table 4.1 and a maintenance interval T_p of 6 months.

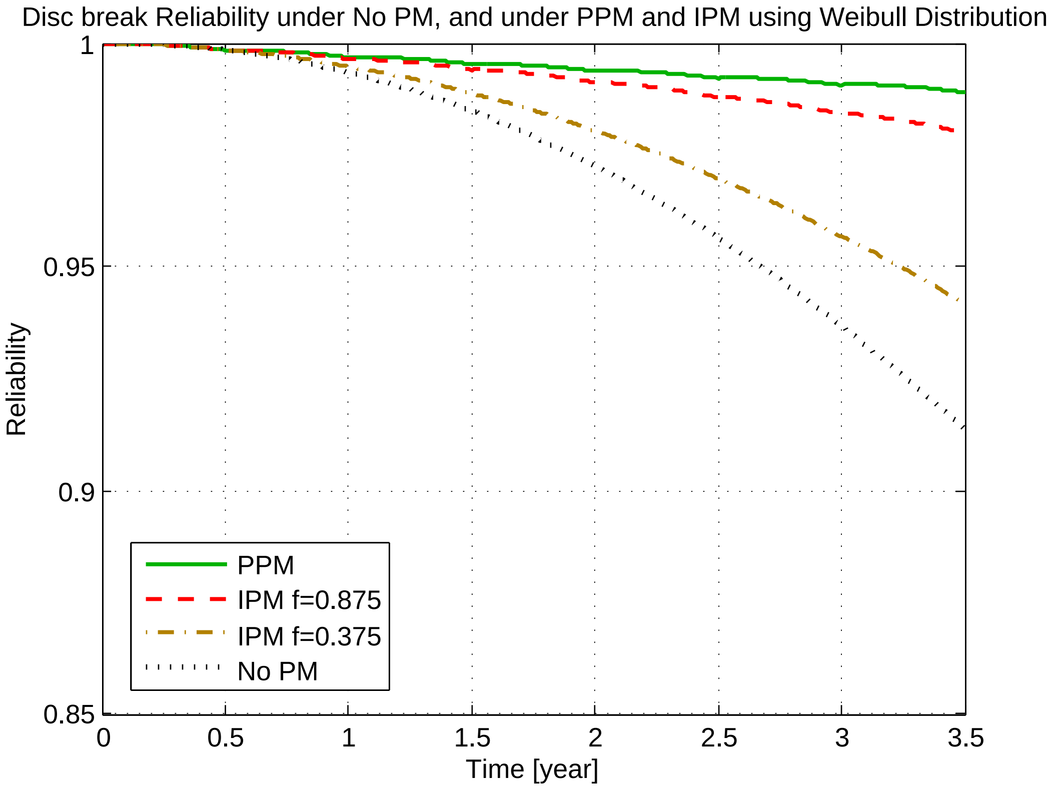


Figure 4.4: Disc brake reliability under no PM, and under PPM and IPM using Weibull distribution.

The reliability is fairly high and well over 90% after 3 years even without periodic maintenance and when using perfect preventive maintenance it keeps the condition of the component close to as good as new. When combining several components in series or parallel each component will influence the system in a higher degree.

4.3.2 System reliability, standard Weibull distribution

For the basic set up of the bogie system the Weibull parameters from table 4.1 were used and a maintenance interval $T_p = 6$ months. This yields a system reliability as shown in figure 4.5.

It is noticeable that the bogie reliability degrades over time and when there is no periodic maintenance that the reliability reaches close to zero significantly faster then when compared to PPM.

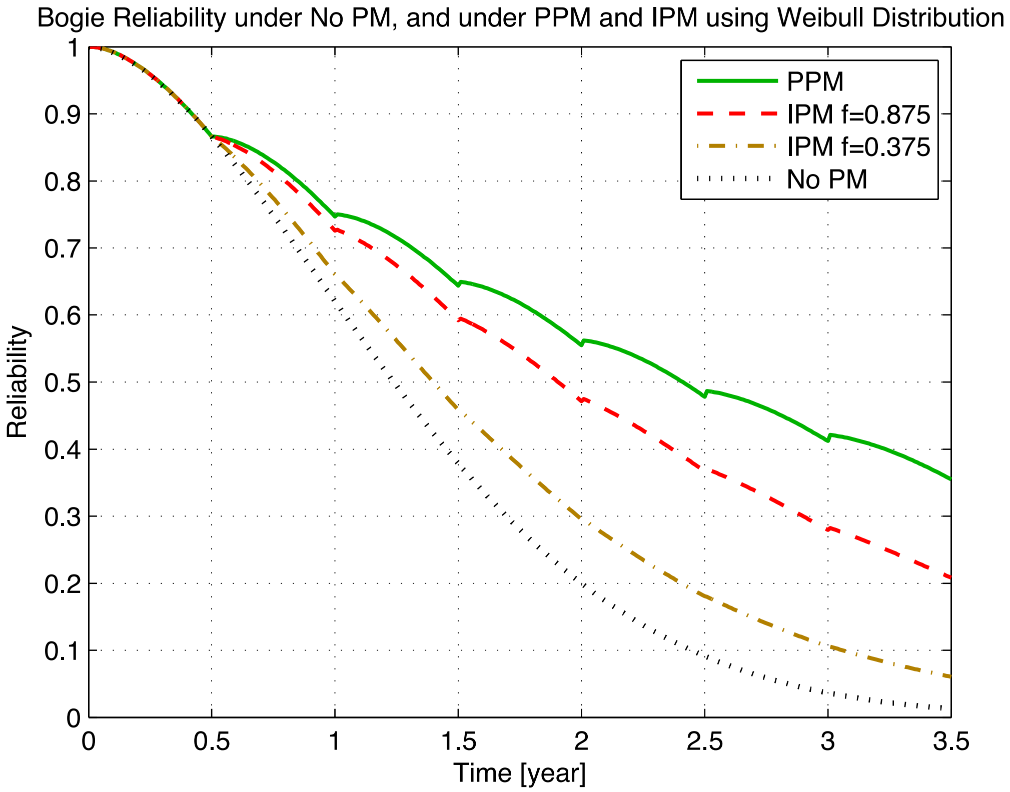


Figure 4.5: Bogie reliability under no PM, and under PPM and IPM using Weibull distribution.

4.3.3 System reliability, high maintenance model

To increase reliability, the PM time T_p can be altered to perform maintenance more often. This produces an overall higher reliability but at a larger cost. In figure 4.6 the bogie reliability is shown when $T_p = 1$ month.

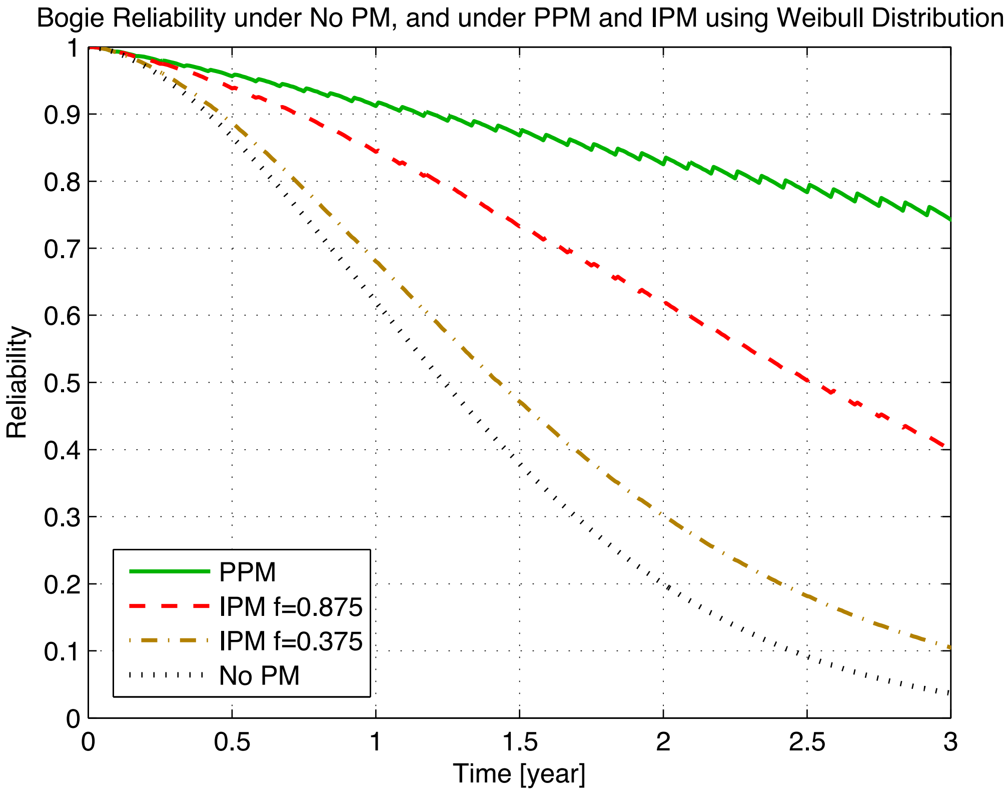


Figure 4.6: Bogie reliability under no PM, and under PPM and IPM using Weibull distribution with short PM time.

With the shorter PM time T_p in figure 4.6 the reliability is overall higher for both perfect and imperfect maintenance compared to figure 4.5 that has a longer PM time. As example the increase in reliability for IPM with $f = 0.875$ when going for the shorter PM time in figure 4.6 compared to the longer in figure 4.5 is 43% better after 3 years.

4.3.4 System reliability, low parameters distribution

Besides the PM interval the reliability is effected by the Weibull parameters which needs to be determined more specific for the components used generally in the railway industry and in the actual case. When using a $T_p = 6$ months and reducing the Weibull shape parameters β, to 25% better than standard components the reliability is negatively effected as seen in figure 4.7.

The reliability with IPM and $f = 0.875$ as seen in figure 4.7 compared to when the shape parameter is 50% higher than standard components and with the same T_p is considerable lower with 53% after 3 years.

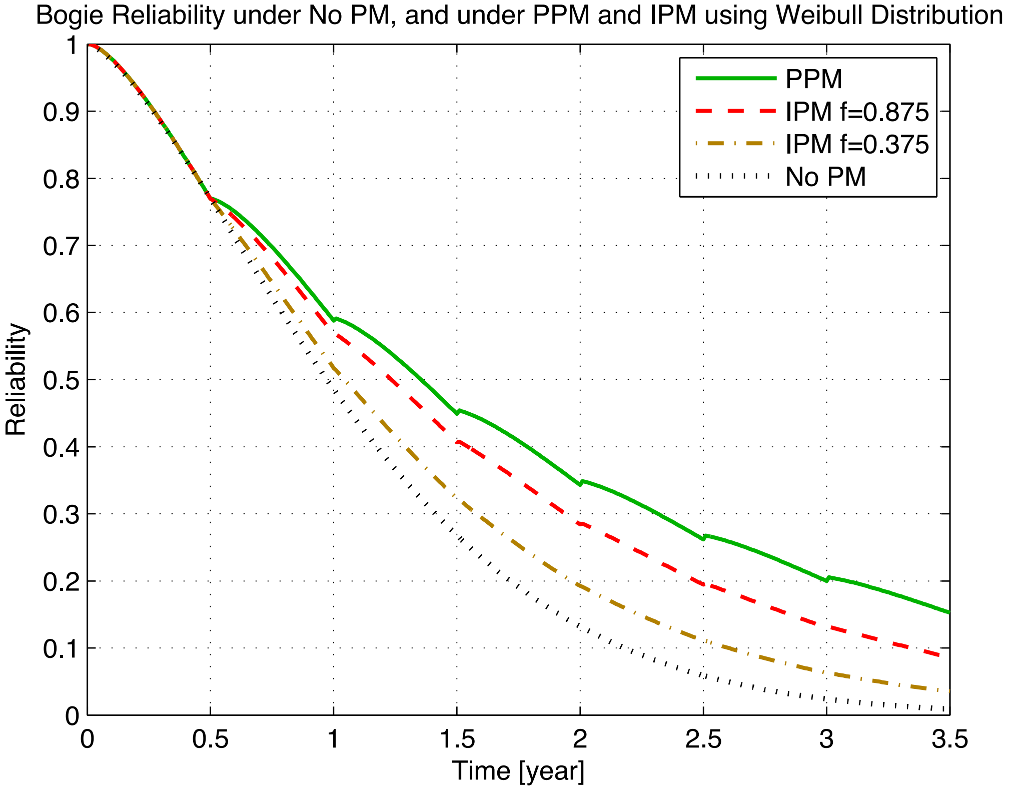


Figure 4.7: Bogie reliability under no PM, and under PPM and IPM using Weibull distribution with reduced Weibull parameters.

4.3.5 System reliability, high parameters distribution

Likewise when the Weibull shape parameter is 75% higher than for standard components an increase in reliability is seen in figure 4.8. For IPM with $f = 0.875$ there is an increase in the reliability of 60% after 3 years when comparing when the Weibull shape parameter is 75% higher than standard components as to when Weibull shape are 50% higher than standard components.

The bogie reliability depends on several item such as how the system is defined, what is seemed as a failure, how the components degrade and how often and what kind of maintenance there are. Seen here the bogie reliability is greatly affected by the varying the components Weibull parameters as well as the maintenance interval.

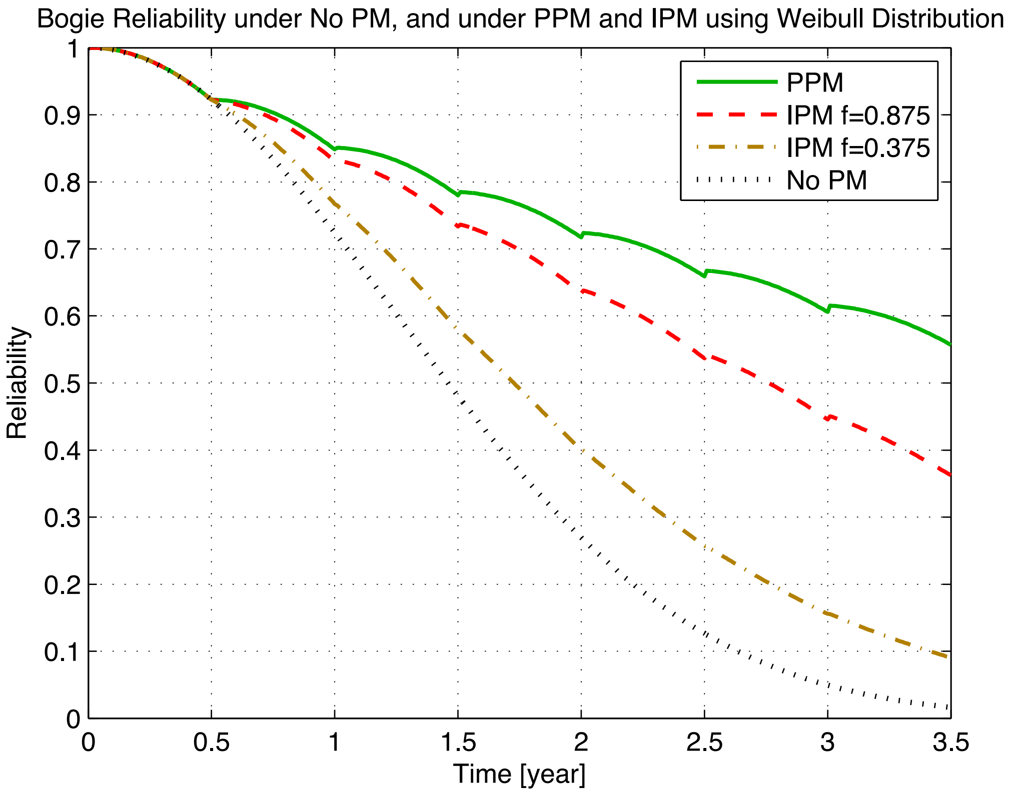


Figure 4.8: Bogie reliability under no PM, and under PPM and IPM using Weibull distribution with higher Weibull parameters.

Chapter 5

Conclusions and future work

The final chapter addresses issues regarding how to specify system requirements for the gathering unit and how this system is useful. It describes the advantages with the case of proactive maintenance and how maintenance planning can be based on system reliability and what is needed to achieve that. There is also a discussion about how this type of analysis could be useful for maintenance planning of other subsystems to the train than just the bogies.

5.1 Discussion on requirements

When designing system requirements to be presented in the thesis the aim was to form a basis for what is needed to be addressed rather than giving a complete system design. In the further steps of the RAMS life cycle, beyond the fourth step of system requirements, one of the first goals is to design the architecture and apportionment of the system requirements. Here the traceability is also addressed to track all the way down from risk analysis to requirements and to verification and validation.

The list of requirements presented in section 3.4 is a result of the initial steps of explaining the system concept, defining the environment with boundaries and doing risk analysis. These steps were performed with the guidance of the standard EN 50126. In these steps the hazards brought up as examples are the ones identified as the most critical and that needed to be examined to draw conclusions. Despite that there is still a possibility that hazards have been undiscovered.

Looking at robustness of data transfer between client and server, time is not crucial. If data transfer fails, client is able to resend data until successful transfer. To guarantee the correctness between client and server, data transfer is handled by the HTTPS protocol. A drawback is that communication between train event recorder and client uses RS232 communication with minimal error handling, the communication protocol is defined in the event recorder requirements and is not possible to change or modify. Incorrect data readings would not be a major problem because data being logged and sent to server is analysed over time and incorrect data should be identified and sorted out during the analysis.

A greater aspect of transferring train related data wirelessly could be the public opinion, can it be allowed to send the internal data types of the trains running on our railways. It is possible the wireless communication could get hacked or sniffed in some way and if that could pose a danger to persons or the train in some way. In the design of this gathering unit it has no possibility to inject data or control the train in any way, but these days it is hard to state that it is impossible it will never get hacked in some way. Many of the data types of the train can be seen as non-secret since it is regulated what should be stored in the ER for example, obviously different manufacturers for train equipment would perhaps want to store different types of data. Another factor making the possibility for communication being sniffed less of a danger is that the basis for analysis in this thesis is based on gathering data over long time as well as large geographical areas making the information less desirable to sniff.

When doing risk analysis there is a need to find an appropriate acceptance level. One method is to examine other similar systems, as example the requirements of the STM device were brought up. The STM device has a different application but is located on the same information bus as it would be appropriate to connect an information gathering unit. The STM device has very strict RAMS requirements due to its functionality so it may be an uneven comparison but they are interconnected. Another aspect of mentioning the STM is that it is one of few systems with directly specified requirements from Transportstyrelsen. In the same way as the STM should not interfere with other systems the gathering unit should not influence other systems.

In this thesis the focus has been on examining the on-board unit. This is done despite that it is only a small part of the complete information gathering system that also consists of the receiver, storage unit i.e. server, the parser as well as the application to use the data. It is only the on-board device that is directly connected to the train and can be considered online. From the hazard list and risk analysis the functionality of the device can be considered non-hazardous or SIL0 class and therefore the authors have omitted to examine other parts of the system that are more disconnected and deemed less hazardous.

One of the main advantages with this type of system, is the possibility to handle large sets of data from entire fleets of train systems. Given enough compatibility and connectivity, data from things such as doors and toilets to items like brake line oil pressure can be analysed with a new perspective, giving great advantages over existing monitoring systems that are offline and time consuming in the information retrieval. This gathering system that gathers information to a centralised server has a great advantage in fields of sustainability as well. Preventing that service technicians has to come to the train just to gather information and instead the information comes to them.

5.2 Discussion on preventive maintenance

Looking into the advantages of being able to collect data from an entire fleet of trains the focus has been on what can be done in the field of preventive maintenance. There are other interesting fields as well. Within preventive maintenance the models looked at handles reliability, availability and cost. These are interlocked and since when planning maintenance scheduling, to ensure safety, reliability has the highest priorities and has therefore been the focus in the thesis.

For the reliability analysis the purpose is the show an example of how the reliability is effected by maintenance. This is done on the components of a train car and more specifically on the bogies, since these are similar for most train systems. To set up the reliability models for the cars the focus was to separately look at all the components and from that put it together to a system.

Looking at the components of the bogie and comparing the Weibull parameters as seen in table 4.1 the Weibull shape, β and scale, θ parameters differs for the wheels as compared to the other components. In this analysis the wheels are not fit for preventive maintenance and are therefore left outside of the analysis (Wei et al., 2012b). The way the components are dependent on each other to reach a state seen as failure is here presented as an example. In a practical analysis, components dependency to reach a failure state needs to be set up by experts in train car maintenance.

The simulations in this thesis is based on general assumptions made about the characteristics of how components degrade according to a Weibull distribution. The assumption was made that the Weibull parameter β should be set higher for components in the railway industry compared to general components due to their often safety related function and thereby robust construction. When looking at the reliability of a single component it is often fairly high (well above 90% for several years) but when combining several components the system reliability is greatly effected by Weibull parameters as well as maintenance interval as shown in section 4.3. To be able to fully use this method and to take decisions based on reliability there is a need to improve the accuracy and correctness of the Weibull parameters for the specific system.

An approach to increase the accuracy of the Weibull parameters is to use historical data for how components have degraded and eventually failed. This would lead to a more accurate reliability prediction for PPM and IPM models and this could be done either as trying to fit the Weibull parameters for the entire system under consideration or for each individual component. Much work has been done in the field of improving Weibull parameters based on historical data, often in the form of MTBF, a second and refined example is (Juang and Anderson, 2004) who have established a Bayesian approach to determine and update the uncertain Weibull parameters and to find an adaptive preventive maintenance policy.

With the rolling stock of today not all systems are possible to automatically collect information about how they have degraded. However for the bogie reliability example it is possible to capture the mileage of each boogie, the power consumption of the engines, brake pipe pressure and resulting retardation as well as the demanded braking control signal, all this giving information about the condition of the components. With the ability to collect data from an entire fleet of trains operating in their natural environment the ability to increase the precision of maintenance parameters are improved and time consumption reduced compared to doing follow ups on a single or a few train systems. Connecting back to the safety aspects of the gathering unit that as such is seen as non-safety critical but in the future have potential to perhaps replace other safety systems and be more than a complement when planing maintenance it is obvious that one has to be able to trust the gathering system.

When deciding on maintenance interval all the parameters of reliability, availability and cost must be considered. In section 2.6 there are basic models for the cost of preventive maintenance under PPM as well as IPM, this can be seen as a guidance to getting an appropriate maintenance interval. As exemplified here the maintenance interval for the basic analysis were set to $T_p = 6$ months as a compromise between cost and reliability.

One more complex issue with the analysis of IPM policy is how to determine the improvement factor f in real life. As seen in figures in section 4.3 when improvement factor reaches one, IPM becomes equal to PPM. There are suggestions how to find the improvement factor done by (Lie and Chun, 1986) who has looked at a method comparing preventive maintenance cost and operation time to find a appropriate improvement factor.

5.3 Conclusion

In the hypothesis it was stated that this thesis would focus at specifying requirements for a data gathering unit under the restrictions of standards and regulations for the railway industry and with the aim of not being safety critical. The goal was also to look at the advantages of increased accessibility of train related data and how that could be used to improve preventive maintenance.

As seen in section 3.3, Risk analysis, using recommended methods as suggested by railway standards, this type of data gathering system can be seen as a non-safety critical system when formulated as in this thesis and with this type of functionality. Making it possible to develop this system from non-specific COTS hardware that meets the requirements stated.

In chapter 4 Dynamic effects of maintenance, a model for how to calculate the reliability of a car bogie is presented. The car bogie model is just the first step in modelling a whole train system. From the increased accessibility to train related data through the gathering system there are new analysis possibilities available. The model together with a deeper knowledge of how much each maintenance action restores the condition of the system and also having more accurate Weibull parameters for the components will lead to a higher accuracy in the reliability prediction as well as it will be useful for maintenance planning.

The reliability model for a bogie presented in this thesis is merely an example of how reliability can be analysed using a data gathering system such as described in this thesis. This type of analysis could be applied on most components that degrade according to a Weibull distribution, which mechanical components often does. Another valuable benefit from the gathering system is that it enables another way to perform follow up on things such as typical speeds on a railway section, conditions about the track such as rail tilt and slip and as well as warning system behaviour that gets recorded over time.

5.4 Future work

In the discussion part there are several fields that needs to be addressed to make this a complete product, in this section some of the more important things are mentioned.

Even though the on-board gathering unit is considered non-safety critical there could be winnings in being able to put out a product to the market that is complying to railway standards and specifically to EN 50126. To do so the safety plan needs to be completed by addressing the later steps of the RAMS life cycle. The life cycle phases that further needs to be addressed are: architecture and apportionment of system requirements, design and implementation, manufacture, integration, system validation, system acceptance, operation, maintenance and performance monitoring and finally decommissioning.

Furthermore it would be interesting to look into what other kinds of analyses that are possible to do on large sets of data from a multitude of trains systems, especially if one could get increased accessibility to other information storing systems other than the ER. Regarding the system reliability model developed in the thesis the model needs further validation by train experts working with train maintenance as well as expert judgement is needed to decide on improvement factors for different specific maintenance actions.

References

3GPP. Telecommunication management; Performance Management (PM); Performance measurements - GSM. TS 52.402, 3rd Generation Partnership Project (3GPP), December 2007. URL http://www.3gpp.org/ftp/Specs/html-info/52402.htm(Accessed2014-04-10).

U.S. Government Printing Office Canada Transports, 2002. URL http://www.rgsonline.co.uk/Railway_Group_Standards/Rolling20Stock/Railway20Group20Standards/GMRT247220Iss201.pdf(Accessed2014-04-22).

Banverket. Stm frs bvs 544.65001, version 5.1,, 2009. URL http://www.transportstyrelsen.se/sv/Jarnvag/Godkannande/Nationella-krav/(Accessed2014-05-03).

Yan Sun, Fangfei Chen, and T.F. La Porta. Multiple backhaul mobile access router: Design and experimentation. In *Communications, 2008. ICC '08. IEEE International Conference on*, pages 4543–4548, May 2008. doi: 10.1109/ICC.2008.852.

The internet engineering task force homepage, 2014. URL http://www.ietf.org(Accessed2014-04-20).

Cisco Systems. Mobile Access Router and Mesh Networks Design Guide. Ts, 2004. URL http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/Mobile_Access_Router_DG.html(Accessed2014-04-12).

A.Y.-M. Chan and Wen-Pai Lu. Architecture for wireless access in vehicles. In *Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th*, volume 5, pages 3336–3340 Vol.5, Oct 2003. doi: 10.1109/VETECF.2003.1286298.

EUROPEAN PARLIAMENT AND THE COUNCIL. Directive 2008/57/ec of the european parliament and of the council of 17 june 2008 on the interoperability of the rail system within the community, 2008. URL http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:191:0001:0045:EN:PDF(Accessed2014-05-15).

Banverket. Eu och järnvägssystemet, May 2014. URL `http://www.transportstyrelsen.se/sv/Regler/Regler-for-jarnvag/EG-direktiv/(Accessed2014-04-24)`.

Robyn R. Lutz. Software engineering for safety: A roadmap. In *Proceedings of the Conference on The Future of Software Engineering*, ICSE '00, pages 213–226, New York, NY, USA, 2000. ACM. ISBN 1-58113-253-0. doi: 10.1145/336512.336556. URL `http://doi.acm.org/10.1145/336512.336556(Accessed2014-04-02)`.

R.R. Lutz. Analyzing software requirements errors in safety-critical, embedded systems. In *Requirements Engineering, 1993., Proceedings of IEEE International Symposium on*, pages 126–133, Jan 1993. doi: 10.1109/ISRE.1993.324825.

M.W. Whalen, A. Murugesan, and M.P.E. Heimdahl. Your what is my how: Why requirements and architectural design should be iterative. In *Twin Peaks of Requirements and Architecture (Twin Peaks), 2012 IEEE First International Workshop on the*, pages 36–40, Sept 2012. doi: 10.1109/TwinPeaks.2012.6344559.

B. Boehm. Requirements that handle ikiwisi, cots, and rapid change. *Computer*, 33(7): 99–102, Jul 2000. ISSN 0018-9162. doi: 10.1109/2.869384.

Guo Zhou, Huibing Zhao, and Hongyu Quan. Safety assessment of cots rtos based computer platform applied in train control system. In *Intelligent Rail Transportation (ICIRT), 2013 IEEE International Conference on*, pages 60–64, Aug 2013. doi: 10.1109/ICIRT.2013.6696268.

R H Pierce, 2011. Rr11 - preliminary assessment of linux for safety related systems. URL `http://www.hse.gov.uk/research/rrhtm/rr011.htm(Accessed2014-04-10)`.

M.P.E. Heimdahl. Safety and software intensive systems: Challenges old and new. In *Future of Software Engineering, 2007. FOSE '07*, pages 137–152, May 2007. doi: 10.1109/FOSE.2007.18.

M.W. Whalen, A. Gacek, D. Cofer, A. Murugesan, M.P.E. Heimdahl, and S. Rayadurgam. Your what is my how: Iteration and hierarchy in system design. *Software, IEEE*, 30(2): 54–60, March 2013. ISSN 0740-7459. doi: 10.1109/MS.2012.173.

ISO 26262. Road vehicles – Functional safety, 2011.

C. Ellen, C. Etzien, and M. Oertel. Automatic transition between structural system views in a safety relevant embedded systems development process. In *Design, Automation Test in Europe Conference Exhibition (DATE), 2012*, pages 820–823, March 2012. doi: 10.1109/DATE.2012.6176607.

N.G. Leveson, M.P.E. Heimdahl, H. Hildreth, and J.D. Reese. Requirements specification for process-control systems. *Software Engineering, IEEE Transactions on*, 20(9):684–707, Sep 1994. ISSN 0098-5589. doi: 10.1109/32.317428.

StevenP. Miller, AlanC. Tribble, MichaelW. Whalen, and MatsP.E. Heimdahl. Proving the shalls. *International Journal on Software Tools for Technology Transfer*, 8(4-5):303–319, 2006. ISSN 1433-2779. doi: 10.1007/s10009-004-0173-6. URL http://dx.doi.org/10.1007/s10009-004-0173-6(Accessed2014-04-22).

Uppaal homepage, 2014. URL http://www.uppaal.org/(Accessed2014-04-18).

Shahid Ali and Muhammad Sulyman. Applying model checking for verifying the functional requirements of a scania's vehicle control system. Master's thesis, School of Innovation, Design and Engineering Mälardalen University Västerås, Sweden, 2012.

Shawulu Hunira Nggada. *Multi-objective system optimisation with respect to availability, maintainability and cost.* PhD thesis, University of Hull, 2012.

Greg D. Brauer Douglas C. Brauer. Maintenance-centered maintenance. *IEEE Transactions On Reliability*, 1997.

John Moubray Paul J. R. Lanthier, The Aladon Network. *Reliability-Centred Maintenance*, volume 2. Butterworth-Heinemann Ltd, United Kingdom, 1998.

Handbook of Reliability Prediction Procedures for Mechanical Equipment. Naval Surface Warfare Center Carderock Division, West Bethesda, Maryland, May 2011.

Banverket. Stm rams requirements 100200 e003, version a, 2008. URL http://www.transportstyrelsen.se/sv/Jarnvag/Godkannande/Nationella-krav/(Accessed2014-05-03).

Sektion teknik järnväg Robert Bylander. Vägledning vid tillämpning av eu-förordning om gemensam säkerhetsmetod för riskvärdering och riskbedömning. URL http://www.transportstyrelsen.se/Global/Jarnvag/Vagledning/Godkannande/v%C3%A4gledning-CSM-RA-1.0.pdf(Accessed2014-05-03).

EN 50126-2. Guide to the application of EN 50126-1 for safety, 2007.

EN 50129, 2003. Communication, signalling and processing systems — Safety related electronic systems for signalling, 2003.

Chuliang Wei, Hwa-yaw Tam Zemin Cai, and Qin Xin S.L. Ho. Reliability verification of a fbg sensors based train wheel condition monitoring system. *International Conference on Intelligent Systems Design and Engineering Application*, 2012a.

Abbas Barabadi. Reliability model selection and validation using weibull probability plot—a case study. *Electric Power Systems Research*, 101(0):96 – 101, 2013. ISSN 0378-7796. doi: http://dx.doi.org/10.1016/j.epsr.2013.03.010. URL http://www.sciencedirect.com/science/article/pii/S0378779613000813(Accessed2014-09-12).

Chuliang Wei, Zemin Cai, Hwa yaw Tam, S.L. Ho, and Qin Xin. Reliability verification of a fbg sensors based train wheel condition monitoring system. In *Intelligent System Design and Engineering Application (ISDEA), 2012 Second International Conference on*, pages 1091–1094, Jan 2012b. doi: 10.1109/ISdea.2012.434.

Muh-Guey Juang and Gary Anderson. A bayesian method on adaptive preventive maintenance problem. *European Journal of Operational Research*, 155(2): 455 – 473, 2004. ISSN 0377-2217. doi: http://dx.doi.org/10.1016/S0377-2217(02)00856-1. URL `http://www.sciencedirect.com/science/article/pii/S0377221702008561(Accessed2014-06-19)`. Financial Risk in Open Economies.

Chang Hoon Lie and Young Ho Chun. An algorithm for preventive maintenance policy. *Reliability, IEEE Transactions on*, 35(1):71–75, April 1986. ISSN 0018-9529. doi: 10.1109/TR.1986.4335352.

Appendix A

MATLAB code

```
%% Exsamensarbete 2014-06-02
%
% Johan Landerholm
%
close all; clear all; clc
%%
tic
% -------Perfect Preventive Maintenance PPM----------
t=0;                % calendar age of component
tau=0;              % useful life of componen or the scale of time
MTTF=6;             % Mean Time To Failure
Risktime=3;         % Useful system operational life, or system risk time
Q=1;                % integer quitent
PMtime=6/12;        % An interval know as PM time, PM interval

%case 1 MTTF <= RT
n1=round(MTTF/PMtime);

%case 2 MTTF > RT
maintenancesteps=round(Risktime/PMtime);


% -------- Component parameters ------------
%http://reliabilityanalyticstoolkit.appspot.com/
    mechanical_reliability_data
gamma_diskbreak=0;            % weibull parameter: location
theta_diskbreak=11;           % weibull parameter: scale
beta_diskbreak=1.4*1.5;           % weibull parameter: shape

gamma_wheel=0;            % weibull parameter: location
theta_wheel=41;           % weibull parameter: scale
beta_wheel=1*1.5; % weibull parameter: shape

gamma_axlebox=0;            % weibull parameter: location
theta_axlebox=6;            % weibull parameter: scale
beta_axlebox=1.3*1.5;           % weibull parameter: shape
```

```
gamma_reduction=0;          % weibull parameter: location
theta_reduction=9;          % weibull parameter: scale
beta_reduction=2*1.5;           % weibull parameter: shape

gamma_clutch=0;          % weibull parameter: location
theta_clutch=11;          % weibull parameter: scale
beta_clutch=1.4*1.5;           % weibull parameter: shape

gamma_suspention=0;          % weibull parameter: location
theta_suspention=3;          % weibull parameter: scale
beta_suspention=1.1*1.5;           % weibull parameter: shape

gamma_motor=0;          % weibull parameter: location
theta_motor=11;          % weibull parameter: scale
beta_motor=1.2*1.5;           % weibull parameter: shape


% Weibull Distribution Modelling of PPM

%----------plot stuff, Reliabilty without maintenance
reliability_diskbreak_noPM=ReliabilityNoPM(maintenancesteps,PMtime,
    gamma_diskbreak,theta_diskbreak,beta_diskbreak);
reliability_wheel_noPM=ReliabilityNoPM(maintenancesteps,PMtime,
    gamma_wheel,theta_wheel,beta_wheel);
reliability_axlebox_noPM=ReliabilityNoPM(maintenancesteps,PMtime,
    gamma_axlebox,theta_axlebox,beta_axlebox);
reliability_reduction_noPM=ReliabilityNoPM(maintenancesteps,PMtime,
    gamma_reduction,theta_reduction,beta_reduction);
reliability_clutch_noPM=ReliabilityNoPM(maintenancesteps,PMtime,
    gamma_clutch,theta_clutch,beta_clutch);
reliability_suspention_noPM=ReliabilityNoPM(maintenancesteps,PMtime,
    gamma_suspention,theta_suspention,beta_suspention);
reliability_motor_noPM=ReliabilityNoPM(maintenancesteps,PMtime,
    gamma_motor,theta_motor,beta_motor);

reliability_boogie_noPM=(reliability_suspention_noPM.^2).*((2.*
    reliability_diskbreak_noPM-reliability_diskbreak_noPM.^2).^2).*(
    reliability_axlebox_noPM.^4).*(reliability_reduction_noPM.^2).*(
    reliability_motor_noPM.^2);

failure_diskbreak_noPM=1-reliability_diskbreak_noPM;
failure_wheel_noPM=1-reliability_wheel_noPM;
failure_axlebox_noPM=1-reliability_axlebox_noPM;
failure_reduction_noPM=1-reliability_reduction_noPM;
failure_clutch_noPM=1-reliability_clutch_noPM;
failure_suspention_noPM=1-reliability_suspention_noPM;
failure_motor_noPM=1-reliability_motor_noPM;
%------------System reliability no PM --------
P1=failure_wheel_noPM.^2;
P2=failure_wheel_noPM.^2;
P3=0;%P1+P2-P1.*P2;
P4=2.*failure_suspention_noPM-failure_suspention_noPM.^2;
P5=failure_diskbreak_noPM.^2;
```

```
P6=P5;
P7=2.*P5-P5.^2;
P8=2.*failure_axlebox_noPM-failure_axlebox_noPM.^2;
P9=P8;
P10=2.*P8-P8.^2;
P11=2.*failure_reduction_noPM-failure_reduction_noPM.^2;
P12=2.*failure_motor_noPM-failure_motor_noPM.^2;
P13=P3+P4-P3.*P4;
P14=P7+P10-P7.*P10;
P15=P13+P14-P13.*P14;
P16=P11+P12-P11.*P12;
P_failure_boogie_noPM=P15+P16-P15.*P16;
P_failure_car_noPM=2.*P_failure_boogie_noPM-P_failure_boogie_noPM.^2;


%probability of surviving until the n-th PM stage
%n=n2; %current PM-stage
%R_Tp_n =exp(-n*u_substitution);

%----------Plot to check reliability calculation vs probability-----
% figure
% time=0:0.01:maintenancesteps*PMtime+PMtime;
% plot(time,reliability_boogie_noPM-(1-P_failure_boogie_noPM),'LineWidth
    ',2)
%------------------------------------------------------------------


%Weibull model for component reliability under PPM, where begin from
    orgin
[reliability_diskbreak_PPM,scale_k]=ReliabilityPPM(maintenancesteps,
    PMtime,theta_diskbreak,beta_diskbreak);
[reliability_wheel_PPM,scale_k]=ReliabilityPPM(maintenancesteps,PMtime,
    theta_wheel,beta_wheel);
[reliability_axlebox_PPM,scale_k]=ReliabilityPPM(maintenancesteps,PMtime,
    theta_axlebox,beta_axlebox);
[reliability_reduction_PPM,scale_k]=ReliabilityPPM(maintenancesteps,
    PMtime,theta_reduction,beta_reduction);
[reliability_clutch_PPM,scale_k]=ReliabilityPPM(maintenancesteps,PMtime,
    theta_clutch,beta_clutch);
[reliability_suspention_PPM,scale_k]=ReliabilityPPM(maintenancesteps,
    PMtime,theta_suspention,beta_suspention);
[reliability_motor_PPM,scale_k]=ReliabilityPPM(maintenancesteps,PMtime,
    theta_motor,beta_motor);

%------------System reliability PPM --------
failure_diskbreak_PPM=1-reliability_diskbreak_PPM;
failure_wheel_PPM=1-reliability_wheel_PPM;
failure_axlebox_PPM=1-reliability_axlebox_PPM;
failure_reduction_PPM=1-reliability_reduction_PPM;
failure_clutch_PPM=1-reliability_clutch_PPM;
failure_suspention_PPM=1-reliability_suspention_PPM;
failure_motor_PPM=1-reliability_motor_PPM;

P1=failure_wheel_PPM.^2;
```

```
P2=failure_wheel_PPM.^2;
P3=0;%P1+P2-P1.*P2;
P4=2.*failure_suspention_PPM-failure_suspention_PPM.^2;
P5=failure_diskbreak_PPM.^2;
P6=P5;
P7=2.*P5-P5.^2;
P8=2.*failure_axlebox_PPM-failure_axlebox_PPM.^2;
P9=P8;
P10=2.*P8-P8.^2;
P11=2.*failure_reduction_PPM-failure_reduction_PPM.^2;
P12=2.*failure_motor_PPM-failure_motor_PPM.^2;
P13=P3+P4-P3.*P4;
P14=P7+P10-P7.*P10;
P15=P13+P14-P13.*P14;
P16=P11+P12-P11.*P12;
P_failure_boogie_PPM=P15+P16-P15.*P16;
P_failure_car_PPM=2.*P_failure_boogie_PPM-P_failure_boogie_PPM.^2;


%-------Unavaliability PPM---------

unavaliability_diskbreak_PPM=1-reliability_diskbreak_PPM;
                                                     %(4.16)

%--------PPM Cost-------

C_ppmi_diskbreak=1000;        % cost of performing PPM for the i-th
    component
C_ci_diskbreak_PPM=10000;     % unit cost of the i-th component
n_i_diskbreak=10;             % total number of PM stages for the i-th
    component

C_pci_diskbreak=n_i_diskbreak*C_ppmi_diskbreak+C_ci_diskbreak_PPM;

% Total system cost = sum up C_pci for all components identified for PPM


%----------Imperfect Preventive Maintenance----------

f=0.875;              % improvement factor
n=maintenancesteps;   % current PM-stage
%PMtime=1;            % PM time interval
MTBF=8;               % Mean Time Between Faliures

%when both PM time T_pj and improvement factor f are constants
W_n_plus=(1-f)*n*PMtime;        % Component current age after n PM
    intervals

%total number of PM stages n for a given component under IPM
% n=round(MTBF/T_p);  MTBF <= RT
% n=round(RT/T_p);    MTBF > RT

%----------Weibull distrubution modelling of IPM---------
reliability_diskbreak_IPM_H_improvment = ReliabilityIPM(maintenancesteps,
    PMtime,gamma_diskbreak,theta_diskbreak,beta_diskbreak,f);
reliability_wheel_IPM_H_improvment = ReliabilityIPM(maintenancesteps,
    PMtime,gamma_wheel,theta_wheel,beta_wheel,f);
reliability_axlebox_IPM_H_improvment = ReliabilityIPM(maintenancesteps,
    PMtime,gamma_axlebox,theta_axlebox,beta_axlebox,f);
reliability_reduction_IPM_H_improvment = ReliabilityIPM(maintenancesteps,
    PMtime,gamma_reduction,theta_reduction,beta_reduction,f);
reliability_clutch_IPM_H_improvment = ReliabilityIPM(maintenancesteps,
    PMtime,gamma_clutch,theta_clutch,beta_clutch,f);
reliability_suspention_IPM_H_improvment = ReliabilityIPM(maintenancesteps
    ,PMtime,gamma_suspention,theta_suspention,beta_suspention,f);
reliability_motor_IPM_H_improvment = ReliabilityIPM(maintenancesteps,
    PMtime,gamma_motor,theta_motor,beta_motor,f);

%------------System reliability IPM f=H --------
failure_diskbreak_IPM_H=1-reliability_diskbreak_IPM_H_improvment;
failure_wheel_IPM_H=1-reliability_wheel_IPM_H_improvment;
failure_axlebox_IPM_H=1-reliability_axlebox_IPM_H_improvment;
failure_reduction_IPM_H=1-reliability_reduction_IPM_H_improvment;
failure_clutch_IPM_H=1-reliability_clutch_IPM_H_improvment;
failure_suspention_IPM_H=1-reliability_suspention_IPM_H_improvment;
failure_motor_IPM_H=1-reliability_motor_IPM_H_improvment;

P1=failure_wheel_IPM_H.^2;
P2=failure_wheel_IPM_H.^2;
P3=0;%P1+P2-P1.*P2;
P4=2.*failure_suspention_IPM_H-failure_suspention_IPM_H.^2;
P5=failure_diskbreak_IPM_H.^2;
P6=P5;
P7=2.*P5-P5.^2;
P8=2.*failure_axlebox_IPM_H-failure_axlebox_IPM_H.^2;
P9=P8;
P10=2.*P8-P8.^2;
P11=2.*failure_reduction_IPM_H-failure_reduction_IPM_H.^2;
P12=2.*failure_motor_IPM_H-failure_motor_IPM_H.^2;
P13=P3+P4-P3.*P4;
P14=P7+P10-P7.*P10;
P15=P13+P14-P13.*P14;
P16=P11+P12-P11.*P12;
P_failure_boogie_IPM_H=P15+P16-P15.*P16;
P_failure_car_IPM_H=2.*P_failure_boogie_IPM_H-P_failure_boogie_IPM_H.^2;

%---------------IPM once more with different f---------------
f=0.375;             % improvement factor
reliability_diskbreak_IPM_L_improvment = ReliabilityIPM(maintenancesteps,
    PMtime,gamma_diskbreak,theta_diskbreak,beta_diskbreak,f);
reliability_wheel_IPM_L_improvment = ReliabilityIPM(maintenancesteps,
    PMtime,gamma_wheel,theta_wheel,beta_wheel,f);
reliability_axlebox_IPM_L_improvment = ReliabilityIPM(maintenancesteps,
    PMtime,gamma_axlebox,theta_axlebox,beta_axlebox,f);
reliability_reduction_IPM_L_improvment = ReliabilityIPM(maintenancesteps,
    PMtime,gamma_reduction,theta_reduction,beta_reduction,f);
reliability_clutch_IPM_L_improvment = ReliabilityIPM(maintenancesteps,
    PMtime,gamma_clutch,theta_clutch,beta_clutch,f);
```

```
reliability_suspention_IPM_L_improvment = ReliabilityIPM(maintenancesteps
    ,PMtime,gamma_suspention,theta_suspention,beta_suspention,f);
reliability_motor_IPM_L_improvment = ReliabilityIPM(maintenancesteps,
    PMtime,gamma_motor,theta_motor,beta_motor,f);

%------------System reliability IPM f=H --------
failure_diskbreak_IPM_L=1-reliability_diskbreak_IPM_L_improvment;
failure_wheel_IPM_L=1-reliability_wheel_IPM_L_improvment;
failure_axlebox_IPM_L=1-reliability_axlebox_IPM_L_improvment;
failure_reduction_IPM_L=1-reliability_reduction_IPM_L_improvment;
failure_clutch_IPM_L=1-reliability_clutch_IPM_L_improvment;
failure_suspention_IPM_L=1-reliability_suspention_IPM_L_improvment;
failure_motor_IPM_L=1-reliability_motor_IPM_L_improvment;

P1=failure_wheel_IPM_L.^2;
P2=failure_wheel_IPM_L.^2;
P3=0;%P1+P2-P1.*P2;
P4=2.*failure_suspention_IPM_L-failure_suspention_IPM_L.^2;
P5=failure_diskbreak_IPM_L.^2;
P6=P5;
P7=2.*P5-P5.^2;
P8=2.*failure_axlebox_IPM_L-failure_axlebox_IPM_L.^2;
P9=P8;
P10=2.*P8-P8.^2;
P11=2.*failure_reduction_IPM_L-failure_reduction_IPM_L.^2;
P12=2.*failure_motor_IPM_L-failure_motor_IPM_L.^2;
P13=P3+P4-P3.*P4;
P14=P7+P10-P7.*P10;
P15=P13+P14-P13.*P14;
P16=P11+P12-P11.*P12;
P_failure_boogie_IPM_L=P15+P16-P15.*P16;
P_failure_car_IPM_L=2.*P_failure_boogie_IPM_L-P_failure_boogie_IPM_L.^2;

figure
scale=(maintenancesteps*PMtime+PMtime)/(scale_k-1);
plot(0:scale:(maintenancesteps*PMtime+PMtime),1-P_failure_boogie_PPM,'-',
    'color',[0 0.7 0],'LineWidth',1.5)
%plot(0:scale:(maintenancesteps*PMtime+PMtime),reliability_diskbreak_PPM
    ,'-','color',[0 0.7 0],'LineWidth',1.5)
hold on

plot(0:scale:(maintenancesteps*PMtime+PMtime),1-P_failure_boogie_IPM_H,'r
    --','LineWidth',1.5)
%plot(0:scale:(maintenancesteps*PMtime+PMtime),
    reliability_diskbreak_IPM_H_improvment,'r--','LineWidth',1.5)

plot(0:scale:(maintenancesteps*PMtime+PMtime),1-P_failure_boogie_IPM_L,'-
    .','color',[0.7 0.5 0],'LineWidth',1.5)
%plot(0:scale:(maintenancesteps*PMtime+PMtime),
    reliability_diskbreak_IPM_L_improvment,'-.','color',[0.7 0.5 0],'
    LineWidth',1.5)

time=0:0.01:maintenancesteps*PMtime+PMtime;
plot(time,1-P_failure_boogie_noPM,'k:','LineWidth',2)
```

```
%plot(time,reliability_diskbreak_noPM,'k:','LineWidth',2)
%---------------end IPM once more with different f-----------
legend('PPM','IPM f=0.875','IPM f=0.375','No PM')
title('Boogie Reliability under No PM, and under PPM and IPM using
    Weibull Distribution')
xlabel('Time [year]')
ylabel('Reliability')
grid
ylim([0 1])
%xlim([0 3])

%---------(un)avaliability IPM---------

my_m_diskbreak=0.002;             %mean time for minimal repair of the
    component
my_diskbreak=0.005;               %mean time to rapair of the component

unavaliability_diskbreak_IPM = unavaliabilityIPM(maintenancesteps,PMtime,
    theta_diskbreak,beta_diskbreak,f,my_diskbreak,my_m_diskbreak);

%--------------Plot Unavaliability--------- Not relevant, present in
    Table
% figure
% plot(1:(maintenancesteps*PMtime+PMtime),unavaliability_diskbreak_IPM,'-
    og')
% hold on
% step=floor(length(0:scale:(maintenancesteps*PMtime+PMtime))/
    maintenancesteps);
% x_scale=0:scale:(maintenancesteps*PMtime+PMtime);
% z=1;
% for x=1:maintenancesteps
%     for y=1:step
%         plot(x_scale(z),unavaliability_diskbreak_IPM(x),'-r')
%         z=z+1;
%     end
% end

%-----------IPM Cost-----------

C_mri_diskbreak=1000;                % cost of minimal repair for the i-
    th component
C_i_diskbreak=10000;                 % unit cost of the i-th component
C_pmi_diskbreak=2000;                % cost of performing IPM for the i-
    th component at each PM stage

N_t=[];
W_n=[0];
for k=1:maintenancesteps
    W_n=[W_n,(1-f)*k*PMtime];
end

for k=1:n
    N_t=[N_t,(1/(theta_diskbreak^beta_diskbreak))*((1/(beta_diskbreak+1))
        *(W_n(k+1)^(beta_diskbreak+1)-W_n(k)^(beta_diskbreak+1)))];
```

```
end
C_ci_diskbreak_IPM=C_mri_diskbreak*sum(N_t)+n*C_pmi_diskbreak+
    C_i_diskbreak;     %Cost of IPM one component



toc


function [reliability_vector] = ReliabilityNoPM(maintenancesteps,PMtime,
    gamma,theta,beta)
%Reliabilty without maintenance

reliability_vector=[];
array_pos=1;
    for t=0:0.01:maintenancesteps*PMtime+PMtime
        u_substitution=((t-gamma)/theta)^beta;
        reliability_vector(array_pos)=exp(-u_substitution);
        array_pos=array_pos+1;
    end

end


function [reliability_PPM,k] = ReliabilityPPM(maintenancesteps,PMtime,
    theta,beta)
%Reliabilty PPM maintenance
%Weibull model for component reliability under PPM, where begin from
    orgin
t=0;
k=1;
reliability_PPM=[1];
    for n=0:maintenancesteps
        for i=0:0.01:PMtime
            reliability_PPM(k+1)= exp(-n*((PMtime/theta)^beta))*exp(-((t-
                n*PMtime)/theta)^beta);   %(4.15)
            %; n*T_p <= t <= (n+1)*T_p
            t=t+0.01;
            k=k+1;
        end
    end
end


function [reliability_IPM] = ReliabilityIPM(maintenancesteps,PMtime,gamma
    ,theta,beta,f)
%Reliabilty IPM maintenance
t=0;
reliability_IPM=[1];
k=1;
t_r=(1-f)*PMtime;      % effective age rejuvination of component

    for n=0:maintenancesteps
```

```
        for i=0:0.01:PMtime

            % Reliability equation:
                                                        %(4.31)
            temp_array=1:n;
            for j=1:n
                exp1=exp(-((((j-1)*t_r-gamma)/theta)^beta));
                exp2=exp(-(((((j-1)*t_r+PMtime)-gamma)/theta)^beta));
                temp_array(j)=1-exp1+exp2;
            end

            product=prod(temp_array);
            exp3=exp(-(((n*t_r-gamma)/theta)^beta));
            exp4=exp(-((((n*t_r+(t-n*PMtime))-gamma)/theta)^beta));
            % R_ic_t is the weibull model for component reliability under
                 IPM for
            % surviving until the n-th PM stage.
            reliability_IPM(k+1)=product*(1-exp3+exp4);

            t=t+0.01;
            k=k+1;
        end
    end
end


function [unavaliability] = unavaliabilityIPM(maintenancesteps,PMtime,
    theta,beta,f,my,my_m)
unavaliability=[0];
for n=1:maintenancesteps
    W_n=[0];                %Effective age of component at n
    UT=[];
    DT=[];
    for k=1:n
        W_n=[W_n,(1-f)*k*PMtime];
    end

    for k=1:n
        UT=[UT,PMtime-(my_m/(theta^beta))*((1/(beta+1))*(W_n(k+1)^(beta
            +1)-W_n(k)^(beta+1)))];
    end

    for k=1:n
        DT=[DT,my+(my_m/(theta^beta))*((1/(beta+1))*(W_n(k+1)^(beta+1)-
            W_n(k)^(beta+1)))];
    end

    A_ic=sum(UT)/(sum(UT)+sum(DT));     %Avaliability
    unavaliability=[unavaliability, 1-A_ic];                        %
        Unavaliability
end
end
```