ADDIS ABABA UNIVERSITY

ADDIS ABABA INSTITUTE OF TECHNOLOGY

AFRICAN RAILWAY CENTER OF EXCELLENCE

Reliability, Availability and Safety Analysis of Addis Ababa Light Rail Transit Interlocking System

---

A Thesis in Railway Engineering (Traction and Train Control)

By:- Almaz Assire

(GSR/4911/10)

Advisor:- Yihenew Wondie (PhD)

December 2020

Addis Ababa, Ethiopia

A Thesis

Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science

The undersigned have examined the thesis entitled '**Reliability, Availability and Safety Analysis of Addis Ababa Light Rail Transit Interlocking System**' presented by **ALMAZ ASSIRE**, a candidate for the degree of **Master of Science,** and hereby certify that it is worthy of acceptance.

Yihenew Wondie (PhD)		
Advisor	Signature	Date
Celestin Nkundineza (PhD)		
Internal Examiner	Signature	Date
Yalemzewd Negash (PhD)		
External Examiner	Signature	Date
Mr Zewdie Moges		
Chairperson	Signature	Date
Ermias Tesfaye (PhD)		
Post Graduate Associate Director	Signature	Date

UNDERTAKING

I certify that research work titled “Reliability, Availability and Safety Analysis of Addis Ababa Light Rail Transit Interlocking System” is my work. The work has not been presented elsewhere for assessment. Where material has been used from other sources it has been properly acknowledged.

Signature: _____

Name: Almaz Assire

ABSTRACT

A railway interlocking system ensures safe train traffic in the railway line by monitoring and controlling its components, such as Computer Based Interlocking (CBI), signals, switches and track circuits. These components must prevent collisions and derailments of the train and their reliability directly affects the availability and safety of the railway network. This study analyzes the reliability, availability and safety of the interlocking control architectures and components by Markov and Reliability Block Diagram (RBD) methods based on the design and failure data of AA-LRT signaling systems.

The first part of this study analyzes and compares the reliability, availability and safety of the one-out-of-one (1oo1), two-out-of-two (2oo2), two-out-of-three (2oo3) and double two-out-of-two (2*2oo2) systems of interlocking control architectures. This helps to choose appropriate interlocking control architecture for AA-LRT. The results show the more advantageous of a double 2oo2 system that is the current control architectures of AA-LRT with high requirements in both safety (0.999999993) and availability (0.9999999999997). When one part of the redundant 2oo2 system is in active mode, another works in standby mode. If a failure occurs in the active mode, the process continues by the standby subsystem.

The second part of the study evaluates the reliability and availability of AA-LRT interlocking system components. This helps to give priorities for critical components and to determine technical and non-technical manpower planning. The results show that CBI has the highest reliability (0.8922) and availability (0.9999), and the axle counter has the lowest reliability (0.1059) and availability (0.9986) after 500 hours of operation. According to the analysis, 92.15% of failures are axle counters failure and this affects the normal operation of both East-West (EW) and North-South (NS) railway lines. The main reasons for axle counter failures are power system and wheel sensor failures, it requires a stable power supply and swift wheel sensor maintenance.

Key Words: *Interlocking System, Reliability, Availability, Safety, Markov*

ACKNOWLEDGMENTS

Foremost, I would like to express my deep and sincere gratitude to my advisor Yihenew Wondie (PhD) who suggested and advised me on this thesis. His guidance helped me in all the time of research and writing of this thesis. He truly exemplifies the merit of technical excellence and academic wisdom.

Also, I am thankful to the respective Ethiopian Railway Cooperation and AAiT offices for their collaboration and support, particularly for their assistance in providing me the necessary information for the input of this thesis work.

I would also like to extend my heartfelt gratitude to my family for their continuous encouragement and moral support. They have been an important and indispensable source of spiritual support throughout my years of study and through the process of researching and writing this thesis.

Finally and most importantly, I would like to thank the almighty God, for his giving me strength, patience, invaluable care, and support throughout my life and completion of this work.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND SYMBOLS

Abbreviation	Definition
A	Availability
AA-LRT	Addis Ababa Light Rail Transit
ACB	Axle Counting Board
ACS	Axle Counting Subsystem
BE	Basic Event
CASCO	Council Committee on Conformity Assessment
CBI	Computer-Based Interlocking
CENELEC	European Committee for Electro technical Standards
CPU	Central Processing Unit
DC	Direct Current
DMI	Driving Monitor Interface
EN	Europe Standard
ERC	Ethiopian Railway Corporation
EW	East-West
f	Failures
FMEA	Failure Modes and Effects Analysis
FT	Fault Tree
FTA	Fault Tree Analysis
h	Hour
HMI	Human Machine Interface
IPS	Interlocking Process Subsystem
IS	Interlocking System
LED	light-Emitting Diodes
LEU	Line Encoder Unit
M	Number of fault-free units necessary to achieve a correct result
MA	Markov Analysis
MSS	Maintenance Support System
MTBF	Mean Time Between Failures
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
N	Number of unites perform the function in parallel

NS	North-South
OCC	Operation Control Center
P	Probability matrix
PC	Personal Computer
PN	Petri Net
POSMOR	Principles of Safe Movement on Rails
$P_S(t)$	Probability of safety
P(t)	Failure-free probability
$Q_D(t)$	Probability of dangerous failure
Q(t)	Probability of failure
R	Reliability
RAMS	Reliability, Availability, Maintainability and Safety
RBD	Reliability Block Diagram
RNET	Redundant Network Subsystem
S	Safety
SCC	Safety Comparison Circuit
SDM	System Diagnose Maintenance
S_H	Disabled hazardous state
SIL	Safety Integrity Level
S_O	Operable state
S_P	Disabled protected state
S_U	Up state
T	Time unit
TBF	Time Between Failures
TCC	Train Control Center
T_D	Mean operating time to hazardous failure
TE	Top Event
TMR	Triple Modular Redundancy
TTR	Time to Repair
UPS	Uninterruptible Power Supply
V	Voter
1oo1	One-out-of-one channel configuration
2oo2	Two-out-of-two channel configuration

2oo3	Two-out-of-three channel configuration
2*2oo2	Double-two-out-of-two channel configuration
Δ	Difference operator
$\boldsymbol{\lambda}$	Failure rate
μ	Repair rate
!	Factorial notation
$\sum$	Summation operator
Π	Product operator
$\cap$	Boolean and
$\cup$	Boolean or

CHAPTER 1 INTRODUCTION

The railway network is a complex system with several technologies working together to fulfil the demands on capacity, speed and mobility to transport goods and passengers. Several equipment and devices, also called wayside or line side equipment, are used for different purposes. All this equipment and devices must be in the proper position before permitting a train movement to ensure a safe operation. The signaling system guarantees safety by locking wayside equipment with each other. This internal locking activity is called an interlocking system [1].

Interlocking is the central function to ensure that trains move safely in technical terms. To achieve this the interlocking obtains information about track occupation (by rail vehicles and other objects) and the position of movable track elements. Then it evaluates this information and permits movements via the signals. The interlocking primary focus on systems where safety is provided technically and tolerate the wrong operation from the worker: if the operator sends a track fault release command for the track circuit in the front of the train, the interlocking system can't release the track circuit [2].

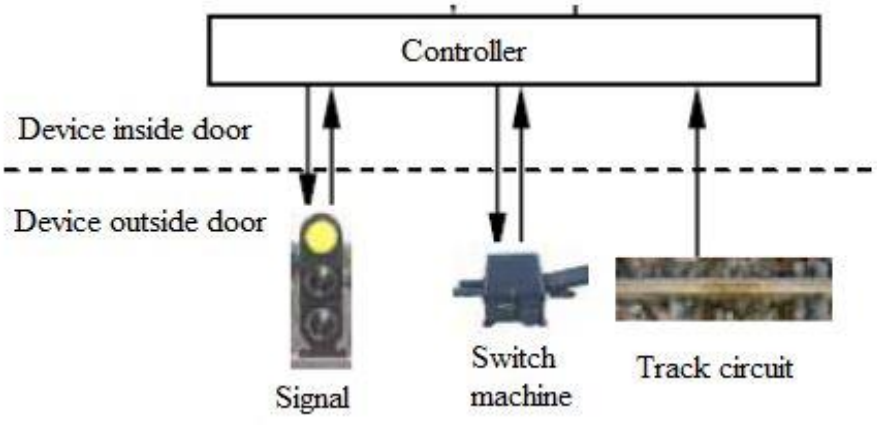

Figure 1-1: Interlocking system structure [3]

To guarantee the trains go safe in the railway track, the interlocking system needs some railway signal devices as shown in Figure 1-1. Functions of these signaling devices in the interlocking system are described as follows [3].

- Track circuit: to check train-position;
- Switch machine: to decide train-run-route;

- Signal: to determine whether the train can run;
- Controller: interlocking logic control for signals, switches and track circuits of a railway station.
  - ✓ Get state information of signals, switch position, and track circuit;
  - ✓ Control switch to change position, control signal to display permission-light or stop-light.

The controller (Computer Based Interlocking system) is centralized to a high degree, where one faulty component can spoil the whole system. The interlocking control program is executed by the Central Processing Unit (CPU) [4]. A failure occurring in the central part of the system is critical for reliability and safety. A computer-based interlocking system gains the fail-safe feature through hardware computer redundancy (for example redundant CPU of main interlocking). There are three major forms of hardware system redundancy, depending on special national requirements, in various electronic interlocking systems. The commonly used redundant structures include 2-out-of-2 architecture, 2-out-of-3 architecture, a double 2-out-of-2 architecture based on system redundancy [5].

Therefore, the key features of an interlocking system are to assure the reliability, availability and safety of railway transportation. The system should guarantee that trains do not conflict or turn over in any case, even in case the operator makes some mistakes or the system fails [6]. It must reject unsafe combinations of track- and signal-commands. In the case of railways, the stoppage of trains is, in general, the safest when the malfunction of relevant systems or any other difficulty happens. Safety is the primary goal, while availability is the second, and the performance of the system is the third main requirement [7].

Railway infrastructure managers need reliability, availability, maintainability and safety (RAMS) analysis that enables them to systematically analyze and optimize budget needs and guarantee the quality of the railway assets in the long run. The key benefits of reliability, availability, and safety analysis in railway systems include [8]:

- The result is an improved management process in case of failures
- Fewer costs for maintenance
- A safe railway operation

- Prevent derailments and collisions between trains
- Ensure system quality
- Prevent environmental hazards
- Manage the railway traffic and increase the operation capacity
- Prevent customer (passengers) dissatisfaction

1.1 Background

Addis Ababa Light Rail Transit (AA-LRT) Project consists of East-West (EW) and North-South (NS) lines, with the total length of the mainline 31.025km. These two lines operate on the same rail in the downtown area for a total length of 2.662km. The ground line mode is mostly applied in rail laying, while elevated line and underground lines are also applied in some sections. As shown in Figure 1-2, the entire line has 39 stations consisting of 9 elevated stations, 2 underground stations, 1 semi-underground, and the rest are all ground stations [9].

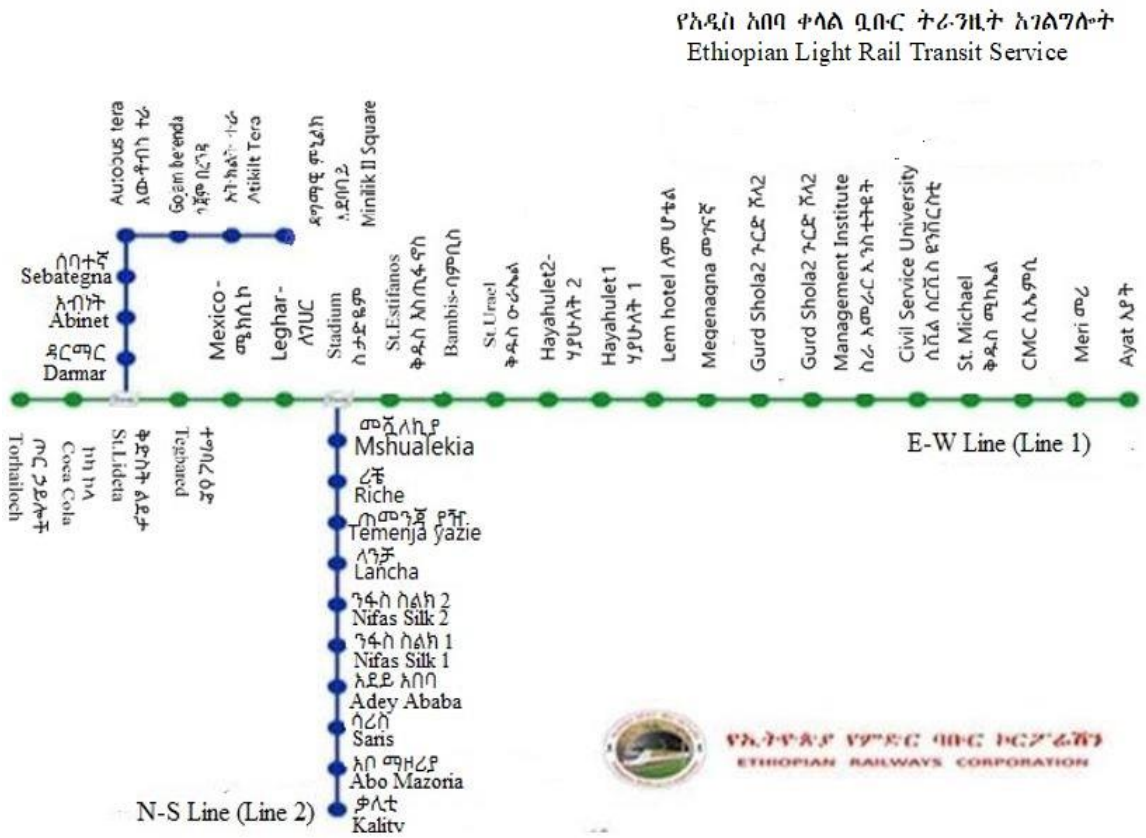

Figure 1-2: Track Layout diagram of east-west Line/south-north Line [9]

There are 12 level crossings between the line of this project and urban roads. Except the elevated stations and underground stations, the ground stations are located in the isolation belt in the middle of the streets [9].

The signaling system interlocking production building is located at the EW1, EW7, EW16, EW20, EW22, NS27, NS10, and NS6 traction substations in the mainline, and it is hereafter referred to as the 'Equipment Centralization Station'. The computer-based interlocking (CBI) subsystem is mainly composed of double two-out-of-two (2*2oo2) interlocking computer, hot-redundant network. The configuration of each main station interlocking system is a "2*2oo2" hardware redundancy structure, used to implement all the interlocking functions, which is located in the signaling equipment room of the main station [10].

The Kality Depot is located near the starting station in the South-north Line and the Ayat Depot is located near the starting station in the East-west Line. The Operation control center of this project is located inside the Kality Depot and the East-west Line and the South-north Line share the same Operation control center. The Maintenance centers are set up in the Kality Depot. The interlocking system in Ayat depot and Kality depot is the same as the ilock system in mainline. The depot interlocking system configures a "2*2oo2" hardware redundancy, it is used to implement all the interlocking functions, which is located in the signaling equipment room of the depot [10].

1.2 Problem statement

Failure of the interlocking system has a large impact on the operation of the railway transportation system, and in the worst case, it causes derailments and collisions [11].

From operation index and failure statistical data of AA-LRT, 47.5% of failures are interlocking system failures. This causes train delay, trip cancellation, speed restriction, passenger's trip interruption before arriving at their destination, and have negative economic consequences. From September 2018 to September 2019 operational statistics, interlocking equipment failures have an economic impact, costs over 7,736,244 ETB [12]. The reasons for these failures are either interlocking control system and/or components.

This thesis aims to analyze the reliability, availability and safety of AA-LRT interlocking control hardware architecture using design data, and compare the results with other architectures depending on special national requirements. This thesis also studies the reliability and availability of interlocking subsystems using failure data and identifies frequently fail interlocking equipment and causes of failure. Ensuring safety in the railway interlocking system is a guarantee of the safe and efficient operation of the whole railway. Thus dealing with the reliability, availability and safety of the interlocking system is very important to improve overall system quality, minimize and prevent system failure and reduce maintenance cost.

1.3 Objectives

1.3.1 General objective

The main objective of this study is analisis of reliability, availably and safety of AA-LRT interlocking system controllers and components, and formulate suggested solutions for identified interlocking system problems.

1.3.2 Specific objectives

Specific objectives of this thesis are:-

- Study and analyze railway interlocking control architectures and components
- Identify commonly used interlocking control architectures
- Develop the reliability block diagram (RBD) and Markov analysis model
- Analyze reliability, availability and safety of interlocking control architectures and components of AA-LRT
- Compare the reliability, availability and safety of the interlocking control architectures and identify the best for AA-LRT
- Identify frequently failed components and formulate suggested solutions

1.4 Methodology

The study approach is based on qualitative and quantitative methods to evaluate the reliability, availability and safety of AA-LRT interlocking system. The information is gathered from site visiting/observation, literature survey, unstructured interviews, discussions, and consultation with signaling and communication engineers from AA-LRT.

The general architecture and full information of the interlocking system components, which are deployed for AA-LRT are obtained from Ethiopian railway cooperation (ERC) documents.

This thesis uses the reliability block diagram (RBD) and Markov process methods to analyze the reliability, availability and safety of the interlocking system. The primary objective is analyzing the current control architecture of AA-LRT in reliability, availability and safety, and compare the result with commonly used architectures. Finally, evaluate the result for supporting the choice of the best interlocking control architecture. This thesis also analyzes the reliability and availability of four interlocking components of AA-LRT. Then evaluate the result for identifying frequently failed components to suggest appropriate solutions.

The thesis plan was performed as the following major tasks:

- Data collection: the data was collected from
  - ✓ Ethiopian Railway Corporation and Addis Ababa Light Rail Transit company
  - ✓ Interviews and documentation: a useful approach when there is a need to determine the important topics to investigate.
  - ✓ Literature: documents reviewed included conference and journal papers, researches, technical specifications, manuals and technical reports.
  - ✓ Database: design data, passenger flow data, operational index data and failure statistics data
- Model development
  - ✓ Interlocking control architecture study model: Reliability block diagram (RBD) for reliability and safety analysis and Markov process for steady-state availability analysis.
  - ✓ Interlocking subsystem/components study model: RBD and Markov process model is used to study the reliability and availability of the interlocking components.
- Data processing
  - ✓ Excel 2013
  - ✓ Matlab 2017a
- Results and conclusions

1.5 Beneficiaries

This thesis directly or indirectly will benefit the following members of the society to have a safe, efficient, reliable and sustainable railway system:

- The researcher (student)
- Ethiopian Railway Corporation (ERC)
- The Government of Ethiopia
- Railway infrastructure managers
- Train and station operators; etc.

1.6 Scope and limitations

1.6.1 Scope

The first study analyzes the reliability, availability and safety of interlocking controller system architectures using RBD and Markov's process based on the design data. Matlab and excel are used to simulate the result to identify the best interlocking control architecture.

The second study analyzes the reliability and availability of AA-LRT interlocking components using the RBD and Markov process model based on historically recorded data obtained from the signaling and maintenance section of AA-LRT. Matlab and excel are used to simulate the results.

1.6.2 Limitations

Some limitations of this thesis are:-

- The study focuses on the hardware architecture of the interlocking control system mainly on CBI central processing unit (i.e. the thesis will not consider software architecture) and the analyses were not considering the cost of the system.
- This thesis analyzes AA-LRT interlocking system components reliability and availability which is limited to one-year data of a specific interlocking area (EW16).
- This thesis studies the reliability and availability of only four components of an interlocking system namely axle counter, CBI, rail signal and switch machine.

1.7 Contribution

Reliability, availability and safety analysis of the interlocking system plays an important role to ensure the safe operation of railways. This thesis contributes to Ethiopian Railway Corporation (ERC) railway infrastructure managers and operators to manage technical and non-technical manpower planning, and reduce maintenance and spare part costs.

Other contributions of this study include: suggesting improvement of the system after analyzing, determination of quantitative aspects such as the probability of occurrence of hazards and mean operating time to hazardous failure.

1.8 Organization of the thesis

The rest of the thesis is organized as follows:

Chapter 2: Gives the description and parameters of reliability, availability and safety. Qualitative and quantitative reliability analysis techniques and comparisons of each technique are briefly discussed. Literature reviews with their contribution are discussed here.

Chapter 3: Discusses the railway interlocking system and components. The interlocking system structure of AA-LRT and its sub-systems are provided.

Chapter 4: Describes the modeling of interlocking control architectures and how the interlocking system models perform and give the reasons. Reliability, availability and safety modeling of different interlocking architectures are done using RBD and Markov process. Modeling of series configuration interlocking subsystem components using the RBD and Markov process are explained. Markov‘s transition diagram has been presented, making some assumptions. From the transition diagram, state transition linear differential equations are derived for the Markov process and then the steady-state performance of the interlocking system has been discussed.

Chapter 5: Summarizes the results of the thesis. Discusses the reliability, availability and safety simulation results**.**

Chapter 6: Summarizes the work done through this thesis and make some recommendations for future work.

CHAPTER 2 THEORETICAL BACKGROUND AND LITERATURE REVIEW

2.1 Introduction to reliability, availability and safety

Reliability, Availability, Maintainability & Safety (RAMS) is defined to indicate the quality and working performance of a system. It is a system characteristic and can be achieved by the application of some particular methods, tools and techniques performed through the whole lifecycle of the system [6], [11].

The interlocking system is mainly used to ensure the safe operation of running trains. Therefore it owns the qualities of high-accurate performance and vital responsibility. High reliability and safety levels are the two most common characteristics and requirements of the system [13]. Consequently, it is a great importance that the system's reliability, availability and safety be analyzed before putting it to use.

Achieving a high degree of safety is one of the most important objectives of a railway signaling and interlocking system. The safety of trains is dependent on the correct and prompt output of their signaling and interlocking system.

2.2 Standards for railway RAMS application

A safety standard can be achieved by assigning different safety levels to different system functions based on their level of criticality. This is determined based on the overall contribution of the function to the system behavior as defined by the European Committee for Electro technical Standardization (CENELEC) [14], [15].

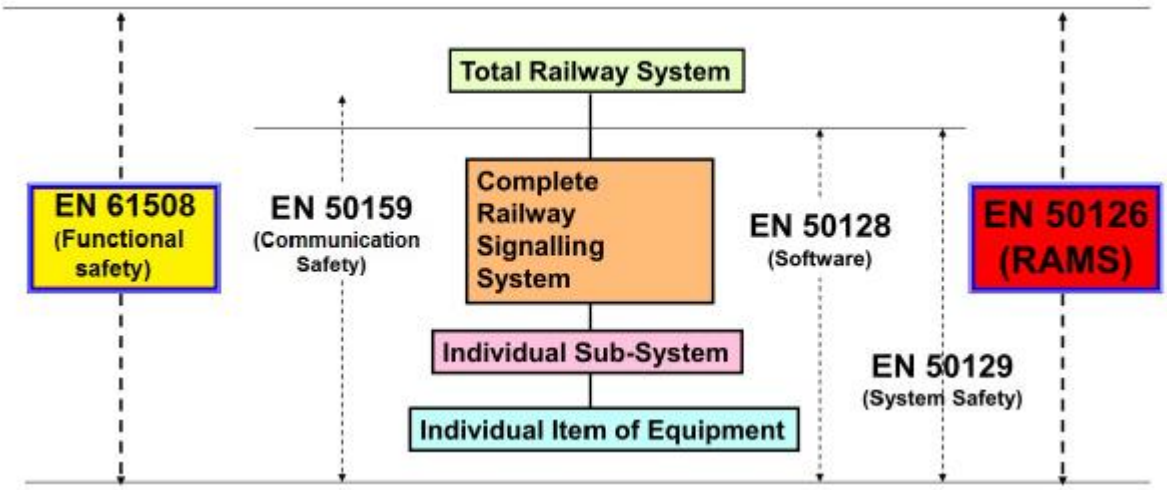

Figure 2-1: Standards for railway application RAMS [14]

Developers must follow the European Standard (EN) standards for railway applications to produce safe and reliable systems. The applicable railway applications standards are EN 50126 (The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) [16]), EN 50128 (Software for railway control and protection systems [17]), and EN 50129 (Safety related electronic systems for signaling [18]) as depicted in Figure 2-1.

All graphical system models must be verified to determine required Safety Integrity Levels (SIL) described by standards EN 50126, EN 50129, and IEC 61508 (Functional safety of electrical/electronic/programmable electronic safety-related systems). The SIL represents the probability of a system to execute specified safety functions within a specified time interval. The standard defines five critical levels where 0 is a non-safety-critical level and 4 is the highest safety-critical level. These levels are defined after an assessment of the level of risk, probability of death or injuries of people, environmental disasters, damage or loss of property, etc. In railway environments, the failure of controllers can cause train derailment or collisions which can result in the loss of human life. Subsequently, the interlocking system for railways is assigned a safety-critical level of 4 [14].

The interlocking system must satisfy safety requirements for both software and hardware. The software must be developed according to defined standards and under key fail-safe railway interlocking principles. Safety-certified components can be used to satisfy the hardware requirements for the interlocking. The hardware (i.e. signaling field equipment) is also instructed to operate in a defined manner in the event of failure.

These requirements state that route requests received by the interlocking must first proceed through a series of checks which are used to verify the behavior of the interlocking system. These checks ensure that no train can be directed into a route already occupied by another train. To avoid a collision, two trains should never be located in the same track section. Subsequently, any two routes cannot share any portion of a track circuit. The train must completely clear the route before another train may be allowed.

2.3 Reliability, availability and safety definition

The European Standard EN 50126 explains processes for the specification and demonstration of RAMS requirements [14]. Basic elements of the RAMS are described in the same standard as:

2.3.1 Reliability (R)

Reliability is a characteristic of an item, expressed by the probability that the item will perform its required function under given conditions for a stated time interval (t1, t2). It is generally designated by R. From a qualitative point of view, reliability can be defined as the ability of the item to remain functional. Quantitatively, reliability specifies the probability that no operational interruptions will occur during a stated time interval. This does not mean that redundant parts may not fail, such parts can fail and be repaired (without operational interruption at item (system) level). The concept of reliability thus applies to non-repairable as well as to repairable items [19].

This is the requirement of failure-free working of the component (here called ‘item’) during a specified time without entering maintenance. Therefore, besides reliability, the maintainability of the used components is an important factor for the availability of the system. Reliability, defined as a probability, is usually specified in a parameter called failure rate and the associated Mean Time Between Failures (MTBF) [20], [21].

2.3.2 Availability (A)

Availability is defined as the ability of a product to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval assuming that the required external recourses are provided. This means that the system (here called ‘product’) will fulfil the required tasks (here called ‘functions’) under the defined framework conditions. It is often designated by A [19].

An important function of the railway system is the safe transport of persons and goods. The precondition to fulfil these functions is the required external sources of help. In the case of the railway system, these are reliable functioning technical components (interlocking, signals …) and also the reliable performance of railway staff in undertaking their tasks. Therefore reliability is an important factor for availability [22].

2.3.3 Safety (S)

Safety is the ability of the item not to cause injury to persons, nor significant material damage or other unacceptable consequences during its use. Safety evaluation must consider the following two aspects: Safety when the item functions and is operated correctly and safety when the item or a part of it has failed. The first aspect deals with accident prevention, for which a large number of national and international regulations exist. The second aspect is that of technical safety [19]. However, a distinction between technical safety and reliability is necessary. Safety assurance examines measures that allow an item to be brought into a safe state in the case of failure (fail-safe behavior), reliability assurance deals more generally with measures for minimizing the total number of failures. Moreover, for technical safety, the effects of external influences like human errors, catastrophes, sabotage, etc. are of great importance and must be considered carefully. The safety level of an item influences the number of product liability claims. However, increasing safety can reduce reliability [19], [23]. Safety and reliability differ because reliability is the probability that a system will perform its functions correctly, while safety is the probability that a system will either perform its functions correctly or will discontinue the functions in a manner that causes no harm [20], [24].

2.4 Reliability, availability and safety in railway

Special norm items define relations between reliability, availability, maintainability and safety (RAMS) and railway service quality and also between RAMS characteristics, i.e. elements interrelation. Railway RAMS is realized through the application of established engineering concepts, methods and techniques in the system life cycle and it is an important parameter of railway quality of service.

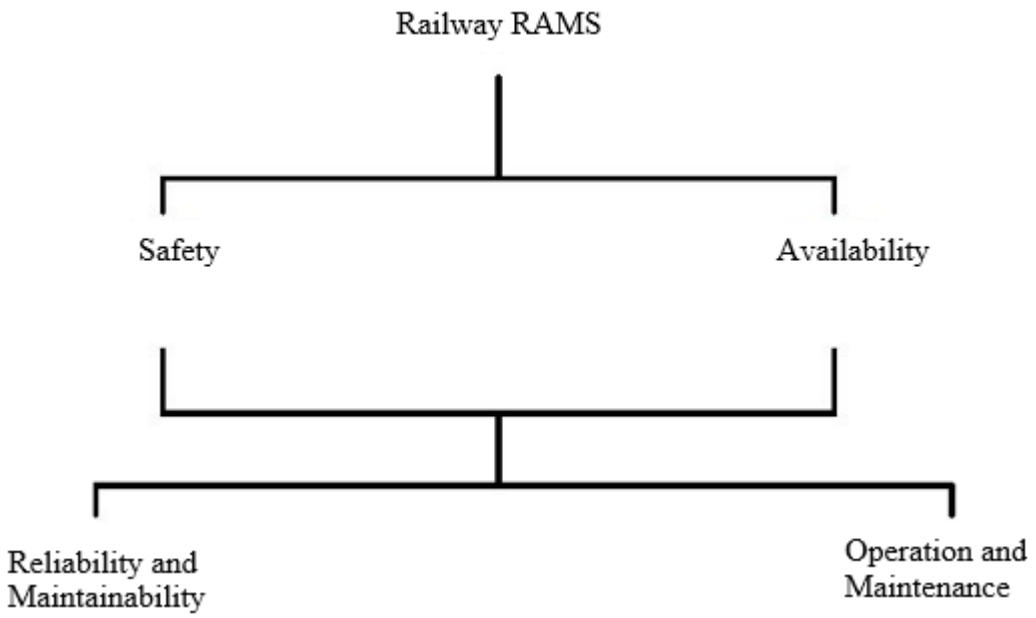

Figure 2-2: Inter-relations of railway RAMS elements [25]

Safety and availability are interlinked in the sense that weakness in either or mismanagement of conflicts between safety and availability requirements may prevent the achievement of a dependable system as shown in Figure 2-2. Attainment of in-service safety and availability targets can only be achieved by meeting all reliability and maintainability requirements and controlling the ongoing, long-term, maintenance and operational activities and the system environment [26].

The interrelation between RAMS elements of technical systems (Reliability, Availability, Maintainability and Safety) is shown in Figure 2-2. It can be seen from the same figure that safety and availability are output RAMS characteristics. Availability appears to be a more appropriate measure than reliability for measuring the effectiveness of maintained systems because it includes reliability as well as maintainability [27], [28].

2.5 Factors influencing railway RAMS

To achieve a dependable system, factors that could influence the RAMS of the system need to be identified, their effect needs to be assessed and the causes of these effects need to be managed throughout the lifecycle of the system [11].

The RAMS of a railway system is influenced in three ways: by sources of failure introduced internally within the system at any phase of the system lifecycle (system

conditions), by sources of failure imposed on the system during operation (operating conditions), and by sources of failure imposed on the system during maintenance activities (maintenance conditions) (EN 50126, 1999); Figure 2-3. These sources of failure can interact. Improving the factors influencing the RAMS will improve dependability [29].

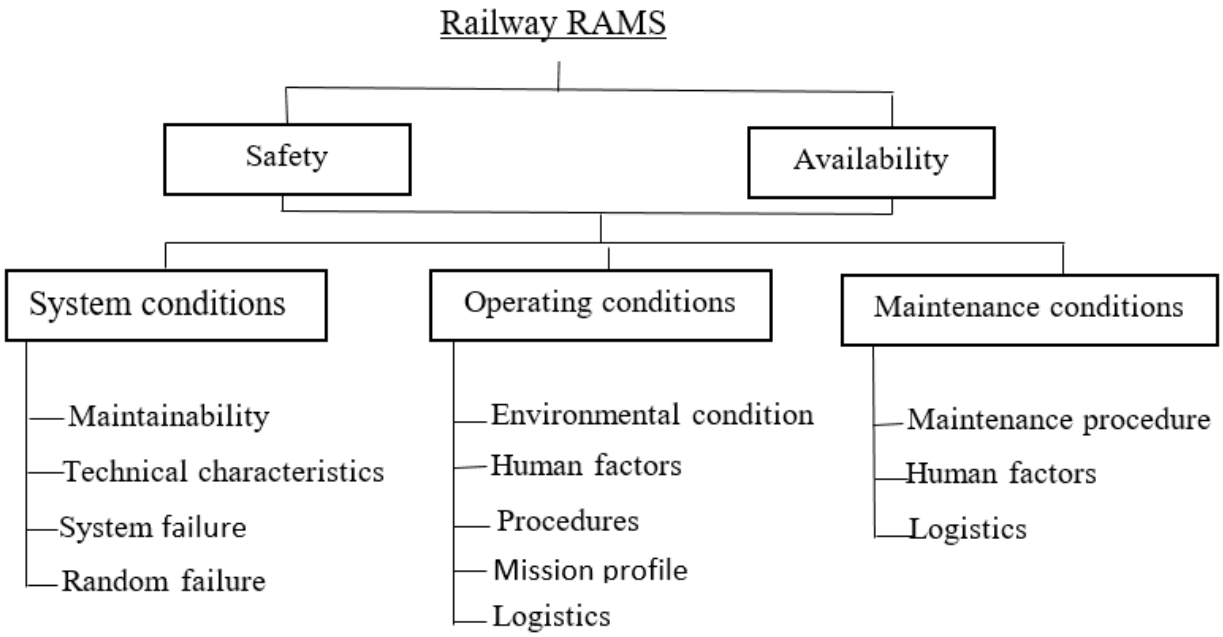

Figure 2-3: Factors influencing railway RAMS [16]

The factors mentioned above affect the characteristics of RAMS. Similarly, the quality of RAMS data affects the correctness of RAMS estimation. Many types of data are relevant to the estimation and prediction of reliability, availability and safety [11].

2.6 Reliability, availability and safety parameters

This section examines several basic definitions that are fundamental to quantitative evaluation techniques. Once the basic definitions are in place the various modeling approaches are considered in more detail.

Reliability, availability and safety of the system can be defined as qualitative and quantitative indexes related to the systems, subsystems and components relied on and available to functions as specified. These can be used as an available tool to understand how the whole system functions, to predict the imperfections and to show the influence on the quality and performance of the system.

2.6.1 Reliability parameters

Reliability is an error-free operation of the system in a stated time interval (t1, t2). Reliability can be specified as the mean number of failures in a given time which can be also described as failure rate or can be expressed as mean time between failures (MTBF) for replicable items, or as the mean time to failure (MTTF) for non-replicable items. Reparable items are repaired and return to use again after repair. The basic reliably parameters are failure rate ($\boldsymbol{\lambda}$), Mean Time Between Failures (MTBF) and Mean Time To Failure (MTTF) [22].

For complex systems, the reliability requirement is normally specified in terms of Failure Rate ($\boldsymbol{\lambda}$) or as Mean Time Between Failures (MTBF).

i. Failure rate ($\boldsymbol{\lambda}$)

Failure Rate ($\boldsymbol{\lambda}$) is the probability of occurrence of a failure at a specific component age, defined as terms of failure per time, load cycle, or cumulative load [24].

It is the probability of failure per unit time of items in operation; sometimes estimated as a ratio of the number of failures to the accumulated operating time for the item. The failure rate is usually time-dependent and thus the rate changes over time versus the expected life cycle of a system. In the special case when the likelihood of failure remains constant with time, the failure rate is simply the inverse of the Mean Time Between Failure (MTBF). It is computed as a simple ratio of the number of failures, f, during a specified time interval T.

$$\lambda(t) = \frac{\text{failures}}{\text{time unit}} = \frac{f}{T} = \frac{1}{MTBF} \tag{2.1}$$

The failure rate is the frequency with which an engineering system or component falls, expressed for example in failure per hour.

ii. Mean time to failure (MTTF)

The probable time to failure for a non-replicable system is described as Mean Time to Failure. MTTF is an estimate of the average, or mean time until components first failure or disruption in the operation of the product, process, procedure, or design occurs. MTTF assumes that the product cannot resume any of its normal operations as it cannot be repaired.

MTTF for all the products which is identical in their design and operate under identical conditions is assumed to be the same. If we have life tests data on the population of N items with failure time $t_1, t_2, t_3, \ldots t_n$ then the MTTF can be mathematically expressed as [24]:

$$\text{MTTF} = \frac{\text{Total time}}{\text{number of units under test}} = \frac{1}{N}\sum_{1}^{N} t_i. \quad (2.2)$$

iii. Mean time between failures (MTBF)

Mean time between failures is the expected or predicted average (arithmetic mean) time between failures of a specific system, assuming that the system goes through cyclic periods of failure and repair [24].

$$\text{MTBF} = \frac{\text{Total operating time}}{\text{number of failures}} = \frac{1}{\lambda} = \frac{T}{f}. \quad (2.3)$$

If we assume that all repairs to a system make the system perfect once again just as it was when it was new, the relationship between the MTTF and the MTBF can be determined easily. Once successfully placed into operation, a system will operate, on average, a time corresponding to the MTTF before encountering the first failure. The system will then require some time, MTTR, to repair the system and place it back into operation once again. The system will then be perfect once again and will operate for a time corresponding to the MTTF before encountering its next failure. The time between the two failures is the sum of the MTTF and the MTTR and is the MTBF. Thus, the difference between the MTTF and the MTBF is the MTTR. Specifically, the MTBF is given by:-

$$\text{MTBF} = \text{MTTF} + \text{MTTR}.$$

In most practical applications the MTTR is a small fraction of the MTTF, so the approximation that the MTBF and MTTF are equal is often quite good [24].

The reliability of a system is generally derived in terms of the reliabilities of the individual components of the system. In a series system, each element of the system is required to operate correctly for the system to operate correctly. In a parallel system, on the other hand, only one of several elements must be operational for the system to perform its functions correctly.

The series system is best thought of as a system that contains no redundancy; that is, each element of the system is needed to make the system function correctly. In general, a system may contain N elements, and in a series system, each of the N elements is required for the

system to function correctly. The reliability of the series system can be calculated as the probability that none of the elements will fail. Another way to look at this is that the reliability of the series system is the probability that all of the elements are working properly.

Reliability of a system composed of N components connected in a serial topology [22]:

$$R_{Series}(t) = R_1(t)R_2(t) \dots R_N(t) = \prod_{i=1}^{N} R_i(t). \quad (2.4)$$

An interesting relationship exists in a series system if each component satisfies the exponential failure law. Suppose that we have a series system made up of N components, and each component, i, has a constant failure rate of λ_i. Also, assume that each component satisfies the exponential failure law. The reliability of the series system is given by [24]:

$$R_{Series}(t) = e^{-\lambda_1(t)}e^{-\lambda_2(t)} \dots e^{-\lambda_N(t)} = e^{-\sum_{i=1}^{N}\lambda_i(t)} \quad (2.5)$$

The distinguishing feature of the basic parallel system is that only one of N identical elements is required for the system to function.

$$R_{Parallel}(t) = 1 - \prod_{i=1}^{N}(1 - R_i(t)). \quad (2.6)$$

It should be noted that the equations for the parallel system assume that the failures of the individual elements that make up the parallel system are independent. For random hardware failures, the independence of failures is a good assumption; however, for failures that are the result of items such as external disturbances, the independence assumption is not very good. Therefore, combinatorial modeling techniques are most often applied to the analysis of random failures in the hardware of a system.

M-out-of-N systems are a generalization of the ideal parallel system. In the ideal parallel system, only one of the N modules is required to work for the system to work. In the M-out-of-N system, however, M of the total of N identical modules are required to function for the system to function. A good example is the Triple Modular Redundancy (TMR) configuration where two of the three modules must work for the majority voting mechanism to function properly. Therefore, the TMR system is a 2-out-of-3 system.

In general, if there are N identical modules and M of those are required for the system to function properly, then the system can tolerate N minus M (N-M) module failures. The expression for the reliability of an M-out-of-N system can be written as [24],

$$R_{M-out-of-N}(t) = \sum_{i=0}^{N-M} \binom{N}{i} R^{N-i}(t)\left(1 - R(t)\right)^{i}, \quad (2.7)$$

where $\binom{N}{i} = \frac{N!}{(N-1)!i!}$

2.6.2 Availability parameters

Formulas for availability calculation of railway system are given in the norm EN 50126 as:

$$\text{Availability} = 1 - \frac{\text{Unavailability}}{\text{Availability max}}. \quad (2.8)$$

The intrinsic availability facilitates measurement of the availability of an element of a system which indicates the operation of the element depending on the design.

To calculate this parameter it will be necessary to have all the design information, the configuration of the subsystems and the methodology that it is going to be used. Notice that there are different ways to calculate this parameter.

For systems without redundancy (simplex), availability is measured as:

$$A = \frac{MTBF}{MTBF + MTTR}. \quad (2.9)$$

Here A is the fraction of the total time the system is available, MTBF is its mean time before failure and MTTR is the mean time to repair. For the series of subsystems, there is an equation that puts this into perspective. It says that the failure rate for the total system λ_T is the sum of the failure rates λ_i for all of the series subsystems.

$$\lambda_T = \lambda_1 + \lambda_2 + \lambda_3 + \cdots + \lambda_n. \quad (2.10)$$

Availability of a system composed of two components connected in a serial topology:

$$A = \prod_{i=1}^{N} A_i. \quad (2.11)$$

Parallel topology:

$$A = 1 - \prod_{i=1}^{N}(1 - A_i). \quad (2.12)$$

Formulas for the availability calculation of railway vehicles are given in the norm EN 50126. According to this norm, the following generally indicate the availability formula:

$$A = \frac{MTBF}{MTBF + MTTR}; \text{ with } 0 \leq A \leq 1, \quad (2.13)$$

where MTBF = Mean Time between Failures in hours, and MTTR = Mean Time to Restore in hours.

2.6.3 Safety parameters

Safety analysis deals with the category and severity levels of hazardous events that can occur to the track system. Hazard identification is the first step in the safety analysis. The hazardous events can be categorized as frequent, probable, occasional, remote, improbable and incredible. Similarly, the severity level can be divided into four categories i.e. catastrophic, critical, marginal and insignificant [27].

Typical reliability and safety parameters that have been used for railway interlocking scenario are [30]:

- P (t) – Failure-free probability
- Q (t) – Probability of failure
- λ (t) – Failure rate
- T – Mean operating time to failure
- $P_S(t)$ – Probability of safety
- $Q_D(t)$ – Probability of dangerous failure
- $\lambda_D(t)$ – Dangerous failure rate
- T_D – Mean Operating time to hazardous failure

Reliability, availability, safety and maintainability data of AA-LRT taken from the signaling system design are the following [10]:

1) Availability

- The availability degree of the computer system of individual subsystems shall be ≥ 99.998%;
- The availability degree of the whole signaling system shall be ≥ 99.99%.

2) Safety

- The safety integrity level (SIL) of safety-related equipment in the signaling system reaches level 4 (Table 2-1).

Table 2-1: Safety integrity level of interlocking subsystems

Subsystem	Safety integrity level
Intermittent Automatic Train Protocol (IATP)system	Level 4
CBI system of mainline and depot	Level 4
Train position detection equipment	Level 4

- The wrong side output probability of safety equipment in the whole signaling system is ≤ 10^{-9}/h.

3) Reliability

- Automatic Train Supervision (ATS) system: MTBF ≥ 2.0×10^5 h;

- IATP system: MTBF $\geq 2.0 \times 10^5$h;
- CBI system: MTBF $\geq 2.0 \times 10^5$h;
- Single outdoor balise beacon: MTBF $\geq 10^6$h;
- Onboard Driving Machine Interface (DMI): MTBF $\geq 2.0 \times 10^5$h;
- Mean correct counts of axle counter is $\geq 1 \times 10^9$ axles;
- Axle counter: MTBF $\geq 1.75 \times 10^5$h

4) Maintainability

- Onboard equipment: MTTR $\leq$ 30 minutes;
- Operation Control Center (OCC) equipment: MTTR $\leq$ 30 minutes;
- Station equipment: MTTR $\leq$ 30 minutes;
- Electronic and electrical equipment (except switch machine) of trackside equipment: MTTR $\leq$ 30 minutes;
- Level crossing signaling equipment: MTTR $\leq$ 30 minutes

2.7 Reliability, availability and safety analysis techniques

For as long as technology has allowed us to create complex systems, a challenge inherent to these systems is the problem of analyzing and predicting how reliable they are. With the advancement of technology and the modification and improvement of these complex systems, one goal has always been to make them safer and more reliable. First, understand these systems and find a way to determine which parts contribute the most to the risk involved with their use. For a long time, this was done merely by approximation and use of existing data. However, many techniques have been developed and refined to more accurately represent these complex systems. Both qualitative and quantitative methods have been developed to analyze complex systems, and there are constantly more being researched, especially in the academic community. Some are used more widely than others, while some are developed primarily for one specific application, but all techniques have their advantages and disadvantages [31].

2.7.1 Qualitative techniques

Qualitative reliability analysis methods have always been used to help identify all possible failures that could occur within a system and the general risks associated with each of those

failures. The most widely used qualitative method is failure modes and effects analysis (FMEA).

2.7.1.1 Failure modes and effects analysis (FMEA)

A failure modes and effects analysis (FMEA) is a frequently applied, systematic method for analyzing an item to identify its potential failure modes, their likelihood of occurrence, and their effects on the performance of the respective item and of the system that embeds it. This is done to document the current status of the item (e.g., for regulatory purposes), as well as derive measures that may lead to improved characteristics of the item such as higher reliability, reduced frequency and/or severity of hazardous events, or optimized maintenance strategies. Moreover, the results of an FMEA may serve as input for other analyses, such as fault tree analysis (FTA) [8].

Strengths and limitations: The strengths of the FMEA methodology are that (a) it is widely applicable to human operator, equipment, and system failure modes to hardware, software and processes (b) a systematic approach to identify component failure modes, their causes and their effects on the system and to present them in an easily readable format. For instance, it helps avoid the need for costly equipment modifications in service by identifying problems early in the design process. Among others, the limitations of the FMEA methodology are that (a) it can generally only be used to identify single failure modes, not combinations of failure modes (in which case other methods like FTA are more appropriate) and (b) analysis can be time-consuming and, therefore, costly, if it is not properly planned and focused. Even if this is the case, it can involve large efforts for complex systems [8].

2.7.2 Quantitative techniques

There are several methods of quantitative reliability analysis techniques, with various theories behind them. The three that are most widely used are fault tree analysis (FTA), reliability block diagrams (RBD) and Markov analysis (MA). All three of these methods are best for different situations, and all have their inherent pros and cons. The quantitative analysis aims to use knowledge of how a system works, often gained from previously completed qualitative assessments, and apply information about failure rates, probabilities, characteristics etc. The information concerning failure rates, distributions, or probabilities can be gained in a variety of ways, but the most accurate is always through test and flight data. However, when this data is not available, or sufficient data does not exist, a variety

of theories can be applied to hypothesize and predict the failure characteristics of a component or subsystem. Then, depending on which analysis method is used, the outcome is some form of failure data of the system and can be used to perform a range of tasks, the most obvious being to identify the largest risk contributors in a system to improve them and consequently reduce the risk the system undergoes [32].

2.7.2.1 Reliability block diagram (RBD)

A reliability block diagram (RBD) is an effective means to visually represent and quantitatively assess the behavior of a system concerning functioning or failure and, thus, may help decide upon possible improvement measures in the system logic configuration. An RBD shows the logical connection of (functioning) components needed for the successful operation of the system, which essentially makes it a graphical representation of Boolean expressions linking the success state (upstate) of a system (i.e., the overall RBD) to the success states (up states) of its components.

The RBD methodology is analogous to FTA in the sense that the underlying mathematical relations are the same; however, an RBD is focused on system success while the FTA is focused on system failure.

The basic assumptions of the RBD methodology are the following [8]:

- The system, as well as the individual blocks that it is made of, have only two states (success/upstate or failure/downstate).
- The RBD represents the success state of a system in terms of connections of the success states of its components (success paths).
- The individual components (blocks) are assumed as statistically independent.

Essentially, an RBD is constructed by drawing the various success paths between the input and output of the diagram that pass through the combinations of blocks that need to function for the system to function. The elementary structures that form an RBD are shown in Figure 2-4 and explained in the following. Hereby, the input and output of the diagram are represented by the ends of the connection, which are usually interchangeable.

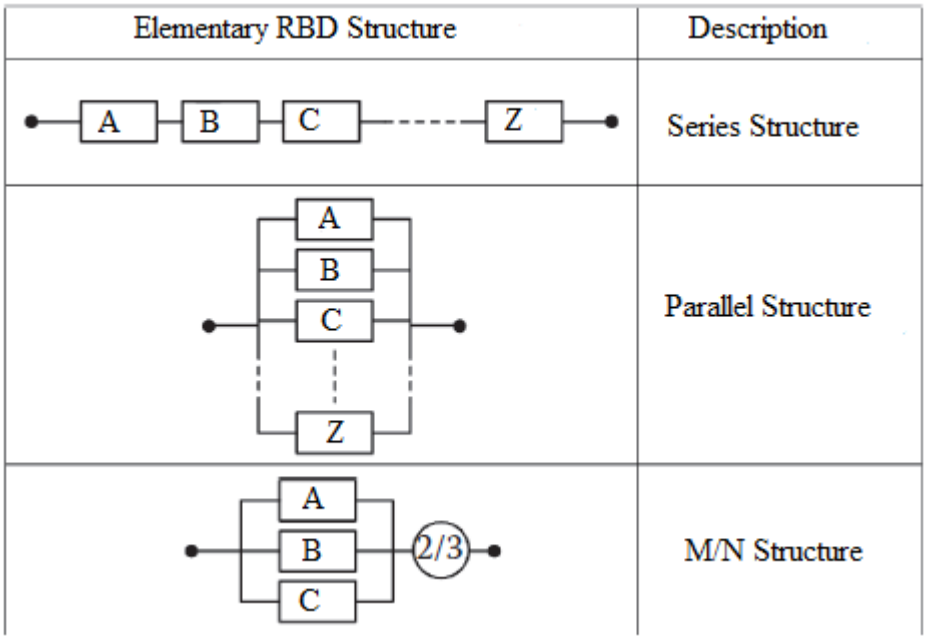

Figure 2-4: Elementary structures of RBDs [8]

Series structures imply that all the blocks need to function for the system to function. In terms of Boolean expressions, if *S* represents the event that the system is in an up state, then we have $S = A \cap B \cap C\ldots \cap Z$, where *A*, *B*, *C* … represent the events that the corresponding blocks are in an up state. For a parallel structure, only one out of a given number of blocks needs to function for the system to function. We then have the Boolean expression $S = A \cup B \cup C\ldots \cup Z$ (where the same symbols as before are used). For *M*/*N* structures, it is assumed that at least *M* out of *N* blocks need to function for the system to function, which is sometimes referred to as a "majority vote" structure. The Boolean expression is $S = (A \cap B) \cup (A \cap C) \cup (B \cap C)$ [8].

Strengths and limitations: The strengths of RBDs lie in the fact that most system configurations can be described in the form of a compact, easily understandable diagram, which can often be derived from functional diagrams of the system. Moreover, qualitative and quantitative assessments can be obtained from RBDs, as well as certain important measures. The limitations are that the application of RBDs cannot describe systems, where the order of failures is to be taken into account or complex repair strategies, are to be modeled (e.g., repaired blocks do not behave independently from each other) [8].

2.7.2.2 Fault tree analysis (FTA)

Fault tree analysis (FTA) is an established methodology for system reliability and availability analysis, as well as safety analysis. It was originally developed in 1962 at Bell Laboratories. Based on a logical representation of a technical system, it provides a rational framework for modeling the possible scenarios that contribute to a specified undesired event, referred to as the top event (TE) of the tree. These scenarios originate from so-called basic events (BE) at the bottom of the tree and are described by a series of logical operators and intermediate events leading to the TE. The system is analyzed in the context of its operational and safety requirements, in addition to its environment, to find all combinations of BEs that will lead to the occurrence of the TE. It is, hence, a deductive method that investigates a system by understanding in which ways a system can fail, rather than looking at a system in terms of how it can successfully operate. A graphical representation is called a fault tree (FT) and describes the relationship between TE, intermediate events and BEs using symbols for events, for gates that describe the relationship between events using Boolean logic, as well as transfer symbols [8].

The two gates that form the building blocks for the other (more complicated, less used) gates are the "OR" gate and the "AND" gate. The "OR" gate symbolizes that the output event will occur if any of the input events occur. The "AND" gate means that the output even will occur only if all of the input events occur. There are only two gates that were originally used when fault trees were developed, but since then many more types of gates have been created to fit specific needs (such as Inhibit gates, Priority AND gates, Exclusive OR gates and k-out of-n gates) [22].

Strengths and limitations: The strengths of FTA are that it is a systematic, deductive approach that can account for a variety of failure causes, including human interactions, and it is especially useful for analyzing systems with many interfaces and complex combinations that lead to system failure. Moreover, the graphical representation makes it easy to understand the system behavior and the factors included. Its limitations include that sequences of occurrence of events are not addressed, and the FTA deals only with binary states. Further, FTAs consider only one TE or failure mode at a time, respectively [8].

2.7.2.3 Markov models

When applied in the context of reliability and safety analyses, Markov models provide a quantitative technique to describe the time evolution of a system in terms of a set of discrete states and transitions between them, given that the current and future states of the system do not depend on its state at any time in the past but only on the present state. Markov models are particularly useful for analyzing systems with redundancy, as well as systems where the occurrence of system failure depends on the sequence of occurrence of individual component failures. They are also well suited for analyzing systems with complex operation and maintenance strategies such as cold standby components, prioritized repair actions, and limited resources for corrective maintenance activities [33].

Depending on the system and the type of analysis, various transient and stationary reliability and availability measures can be obtained by solving the corresponding model, such as instantaneous and steady-state availability, average availability, mean operation time to (first) failure and mean down time. In the context of functional safety, Markov models allow the computation of measures such as dangerous failure rate and the average probability of failure on demand [8].

Strengths and limitations: The strengths of Markov modeling include the capability of describing complex redundancies and dynamic multistate systems, providing various transient or stationary measures as results. The supporting state-transition diagrams provide a simple and intuitive means for visualizing and communicating the structure of the model. However, Markov modeling is complicated by the fact that the numerical evaluation requires more effort and is limited in that the number of states may explode for complex systems [8].

2.7.2.4 Petri nets

Petri nets (PNs) are a technique for describing the global behavior of a system by modeling local states, local events (transitions) and their relations to each other. Their graphical notation, in the form of a directed graph with tokens, allows intuitive and compact modeling of deterministic or stochastic systems for various applications, such as concurrent processes in logistics and transportation, as well as distributed and parallel communication systems as depicted in Figure 2-5.

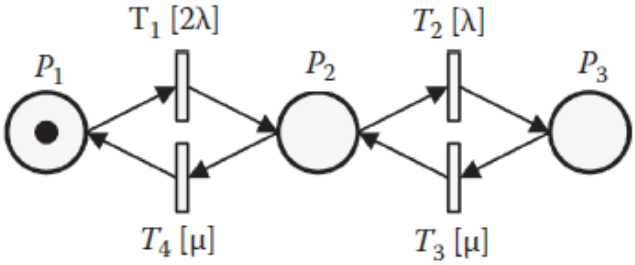

Figure 2-5: Example of a parallel system modeled with a stochastic PN [8]

Very relevant for RAM purposes are the so-called generalized stochastic PNs, where random variables are introduced to represent random times until certain events occur. Local events may represent failure or repair events, while local states may represent functioning states, failure states, or states with various degrees of degraded performance. In case the random transitions in the model are exponentially distributed and the deterministic transitions have no delays (immediate transitions), PNs can be represented as Markov models; however, the former usually have a much more compact representation [8].

Strength and limitations: Similarly to MA, the use of Petri Nets is advantageous because it represents the state of one or many components (or systems), and therefore is more representative of what it is modeling over time. Also, since this method is not limited to constant failure rates, it can sometimes more accurately denote the actions of a system than an MA. However, since it is a state-space analysis, it tends to get incredibly large and hard to work with, as the model it represents gets more complex and complicated. Between this and the fact that it is not very well known, to begin with, it is rarely used as a reliability analysis method except for its application to simple models.

2.7.3 Simulation methods

It is hard (or sometimes impossible) to obtain reliability and availability measures analytically, for modern large and complex systems with equipment that follows different failure and repair distributions. Simulation is used in these cases as an approximation to remedy the limitations of analytical methods. The first step in the simulation method is to construct a system model (FTA, RBD, Markov state-space diagram, etc.) describing the interrelations between underlying components. A computer program generates random draws from these distributions to simulate when the system is up and down, stores tables of failure, failure effects, etc. in a log and tracks system or function capability over the

considered time horizon. A variety of relevant parameters can then be derived from the log. The number of simulation runs required for accurate availability measure results will depend on the variation in the output measure at each run.

Simulation methods are very flexible and can provide accurate predictions for systems that perform measures. In particular, they overcome the limitations of the analytical methods and provide time-dependent availability, number of failures and other time-dependent measures (cost, throughput, etc.) even in cases where non-exponential distributions are used to describe equipment failure and maintenance actions. Therefore, they are well suited for commercially available software used for RAM studies. The advantage of this approach is that the occurrence of rare events can be easily taken into account and a large number of cycles is necessary to have significant statistics for comparison [34].

Table 2-2 shows a comparison of the different approaches to reliability analysis and a summary of some of the important characteristics of the methods discussed.

Table 2-2: Comparison of reliability analysis method characteristics [32]

Characteristic	FTA	RBD	MA	Petri Nets
Static	X	X		
Dynamic			X	x
Logic-based	X	X		
State-space			x	x
Top-down	x	x		
Variable distributions	x	x		x
Can be used for dependent event			X	x

In this study, RBD and Markov analysis methods are used to obtain reliability, availability and safety parameters of interlocking systems, because they can be implemented easily to the railway systems.

2.8 Literature review

Many research works have been done to improve the working of the interlocking system to make it more reliable, available and safe to decrease operational cost and make it work efficiently. Therefore, this thesis has discussed some of the researches based on the relevance of this work.

Tao and Jianxin [13] discussed the reliability methods adopted to analyze the RAM indexes of the All-electronic Computer Interlocking System when its execution layer is equipped with a single configuration or the dual-redundant configuration. So, the track line which has lower efficiency and is not very busy but sensitive to the local economy can be equipped with the single configuration of the All-electronic Interlocking System, but for the busy track line, the redundant All-electronic Interlocking System is the best choice. Of course, the redundant configuration can be both adopted in the station bottleneck and the main track line to improve the system's availability and the local economy. Finally, the paper briefly includes suggestions on how the All-electronic Computer Interlocking System's RAM indexes may be increased and, how the system may be used practically. But in this research, models for interlocking architecture were not suggested to improve the reliability, availability and safety of interlocking components.

Bellek [35] aimed to design and implement an example railway interlocking mechanism with formal methods. The main objective of the thesis was to make a RAMS analysis for the designed model stations using two widely used formal methods, "Petri Nets" and "Finite State Machines" which indicated in the same standard were examined with detailed examples. Using one of these models, some RAMS parameters were obtained as a final step. Then, these parameters were implemented to equipment with artificial data as an example analysis. A graph was discussed to understand the interaction between data and RAMS parameters. In modern railway signaling systems, the interlocking unit is designed about hardware and software redundancy. Hardware redundancy is considered to prevent the dangerous consequences of any failure in the hardware of the interlocking unit. On the other hand, software redundancy is used to protect the system against software failures that may occur in the interlocking program. Therefore, the diversity of interlocking software is recommended to a high safety level. In the design of interlock loops for the signal exchange in machine protection systems, the choice of the hardware architecture impacts machine safety and availability. But the resulting outcome of this thesis report is not comparable to a real interlocking system.

Wagner and Apollonio [4] presents the results and illustrates the potential of the analysis method for supporting the choice of interlock system architectures. To compare various interlock loop architectures in terms of safety and availability, the occurrence frequencies of related scenarios have been calculated in reliability analysis, using a generic analytical

model. This paper presents the method and results of a reliability analysis addressing the properties of various interlock loop architectures about machine safety and availability. It shows the advantages of a 2oo3 architecture for systems with high requirements in both safety and availability. In this study, only M-out-of-N architectures are analyzed. Complex interlocking control architectures such as double 2oo2 are not included.

This thesis addresses the objectives; analyze redundancy architectures that enhance reliability, availability and safety for the interlocking control system, and interlocking components of AA-LRT using RBD and Markov process model. Reliability block diagram (RBD) system configurations can be described in the form of a compact, easily understandable diagram, which can often be derived from functional diagrams of the system. Moreover, qualitative and quantitative assessments can be obtained from RBDs, as well as certain important measures. Also, Markov analysis is the best method to analyze repairable systems with constant failure and repair rates.

CHAPTER 3 RAILWAY INTERLOCKING SYSTEMS

3.1 Introduction

Interlock is the relationship that can function or be established only when the signal, switch and route are under certain procedures and meet certain conditions. In other words, to ensure the safety of the transportation in a station, a series of interlocking rules must be formulated to constrain the opening and closing of the signal as well as the turning of switch and establishment of the route. To implement these interlocking rules, a technical mean must be used [36]. Railway interlocking is a functional arrangement of apparatus that controls signaling system components to achieve safe, expected outcomes of controlling train movement [37]. Railway signaling systems are very critical systems. Any dangerous situation which may occur in the system can cause very dangerous accidents. Therefore, interlocking systems are used to prevent any hazardous cases in the signaling systems. The interlocking mechanism implemented in the signaling equipment is called the railway interlocking system. Interlocking is the core system in railway signaling. It ensures that all signaling equipment is in proper status for the train movement. It obtains information about train occupancy and locks the movable wayside elements in the correct position for a certain route. Then, it permits movements via signals [35], [38].

An interlocking system has three main functions which can be split into three levels [39]:

- **Operational level**: it includes the interface between the human signaler performing the request and the machine.
- **Interlocking level**: it includes the functions required to decide if the request performed by the signaler can be accepted or not, and to do the proper actions consequently.
- **Element control level**: it mainly includes the functions required to transmit information between the components.

Depending on the technological developments, different kinds of interlocking systems are developed until today, namely the mechanical interlocking system, the electro-mechanic interlocking systems, the relay interlocking system and the electronic interlocking system.

Mechanical interlocking systems: Towards the end of the 19th century mechanical interlocking systems were used. The system created inter-dependency between signals and

points using wire pulls. At a given time the operations that would lead to a collision were mechanically blocked [35], [5], [40].

Electro mechanic interlocking systems: From around 1915 until 1950. The interlocking system is a mix of the mechanical interlocking system and the relay interlocking system. External components such as points and signals were now controlled by relays instead of wire pulls. The part of the interlocking system that prevented trains from colliding, were still mechanically controlled. The control was now made by a mechanical registry consisting of steel beams with holes in [35], [40].

Relay interlocking systems: Relay-based interlocking system was introduced after the mechanical interlocking system. A signal relay is specially designed for safety-related operation. The interlocking consists of complex circuitry implemented by relays and the field elements are operated and controlled purely electrically [35], [37], [41].

Electronic interlocking systems: Electronic interlocking systems became prevailing after the 1980s. The systems have a high degree of complexity and are easily affected by external influences. The interlocking functions are programed by software and the hardware's are made by electronic components which are not robust as mechanical components. This cause that the inherent fail-safe design is hardly applied to electronic interlocking systems as before. To increase reliability, hardware dependency is widely used in electronic interlocking systems [5], [35], [37], [41].

3.2 The structure of interlocking system

According to the functional division and the location of the equipment in the system, the interlocking system can be decomposed into the interlocking mechanism (interlocking layer), the man-machine layer and the controlled device layer as shown in Figure 3-1. The interlocking agency must meet the fail-safe principle and their equipment should be located in the machinery room of the signal building of the station; the man-machine interface layer is located in the duty room of the station [36].

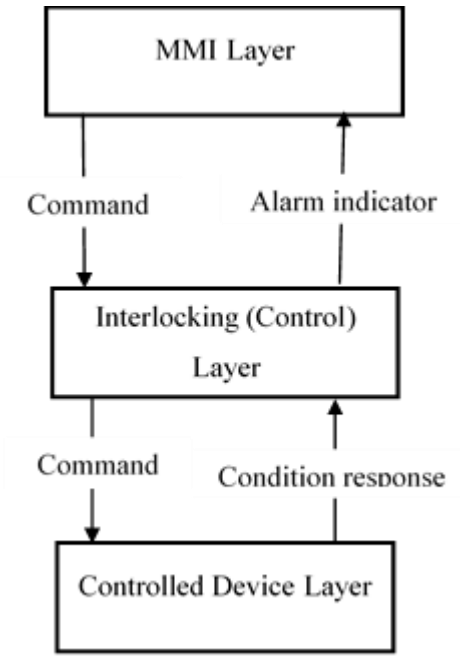

Figure 3-1: The structure of interlocking system [36]

Controlled devices: tracks, switches and signals.

The interlocking mechanism is the core of the interlocking system. It receives not only the manipulation information from the man-machine layer but also the information from the outdoor signal, switch machine and the track circuit of the controlled device layer. Also, according to the interlocking condition, it processes the control information and status information and produces the corresponding signal control commands and switch control commands.

The main function of the man-machine interface layer is that the operator inputs the operation information into the interlocking mechanism at the layer and accepts the equipment status information and the traffic situation information fed back by the interlocking mechanism.

The automatic train supervision (ATS) human machine interface is the interface to be used by the central dispatcher and local operator. Through the human machine interface, the operator obtains the line operation information, and inputs control command to ensure the necessary control of running. All human machine interfaces in ATS support bilingualism showing and provide necessary aiding information, which is convenient for users to interact with the system. The mouse is mainly used to operate and the keyboard is the second.

The central workstation has the same human machine interface as the local station workstation for the convenience of operators. The interface is composed of a title bar, menu bar, equipment status display column, time display, track layout, train running information and operation area. The status of the command operation can be seen from the interface. The non-operation command cannot be selected. The two monitors are independent. They can display different information and one does not affect the other one. This function is used to supervise signal equipment present state and train state of the whole line. The displaying information is included as follows [10]:

- Track layout
- Station control/central control state
- Equipment working state
- Signal, switch and track state
- Automatic fleet route state
- Automatic turn back route state
- System control mode and state
- Automatic route state according to train schedule or destination
- Train location, train number and train state
- The destination of out depot train
- Departure information of station and depot
- Operation result
- Switch split alarm
- Platform information
- Power supply state
- Track number, signal number and switch number(can be displayed when needed)
- Other fault alarms

3.3 Elements of interlocking system

3.3.1 Ilock 2*2oo2 CBI system

The basic interlocking equipment function is to ensure safe train operation and to realize correct interlocking relations and route control between track sections, point machines and signals on the train route via safety relay interface. The interlocking equipment is also responsible for the interface with line encoder unit (LEU) so that the train can obtain information regarding trackside signal and point machine through an active beacon corresponding to the signal under ATP operation mode.

3.3.2 Signal

As shown in Figure 3-2, signals are physical characteristics and symbols specified in running and shunting operations to indicate the operating conditions to the staff concerned [42]. Signals are the basic equipment that provides an interface between technical devices and people. In railway signaling systems signals are used for conveying information from the system to the train driver or workers on the track. Most generally conveyed information can be listed as follows:

- Movement authority
- Permitted speed
- Information about the direction of the route
- Position of points
- Commands for the brake test

Figure 3-2: Light-Emitting Diodes (LED) signal [9]

The signal indicates the sign for the train with lights as followed.

Green light: Indicates clear route in the front; all the switch directions are straight in the route, and the train must run within the predefined speed according to the line [42].

Yellow light: Indicates a clear route in the front; at least one of the switch direction is lateral. The driver shall reduce the running speed of the train and allow the train to run at a lateral speed of passing the switch [42].

Red + yellow light: calling-on signal; trains are allowed to pass the route at no-higher-than-specified speed (e.g.10Km/h) and shall be ready to stop at any time. Calling-On is only used in failure conditions and approach axle counter section occupied [42].

White light: Permitted signal, the train shall run at less than 10km/h speed. This light is only used in the depot [42].

Restrictive signal (red light or dark): Indicates no passing; when seeing the red lamp, the driver must ensure that the train stops in front of the signal [42].

The signal systems have different types of aspects. That is two aspects, three aspects and four aspects. All have their advantages and disadvantages. The interpretation for three aspect signal indication is explained. A red aspect indicates that the following track section is occupied. A yellow aspect states that the following track is clear but the next track section is occupied and a green aspect indicates that the following two-track sections are clear. The interlocking monitors and controls the signal aspects to ensure adequate warnings are provided for train drivers to stop at a danger signal or to reduce speed in time. Signal aspects are always set to red in emergencies. Where signals are visible beyond the current approaching signal, more restrictive aspects must be applied to limit the risk of incorrect interpretation of the signal aspect. A signal shall only clear from its most restrictive aspect (red) when the appropriate conditions are fulfilled. These conditions shall continue to be confirmed until the trail has entered the route to which the signal applies. If the conditions are not proved, the signal reverts to a danger indication and displays a red aspect.

A start signal can only display precedes aspect provide the route between the start and destination signals is clear. The defined overlap must be unoccupied and all points in the

route must be set in the required position and locked. The start signal of any directly opposing route must be proven to be displaying a red aspect before the start signal can display a proceed aspect. Also, for a signal to obtain a proceed aspect, the next signal in the same direction of movement must continuously display a proceed aspect. If no aspect is displayed on a signal (e.g. due to a lamp failure), the preceding signal must show a red/stop aspect. In the event of a failure of a signal aspect which could lead the driver to interpret the signal as less restrictive, the aspects shall be tested. If the test indicates that the aspect is non-functional the signal aspect must be reduced to the most restrictive aspect, i.e. a red aspect and the proceeding signal aspect must be restricted to ensure the signal is not passed at danger. In exceptional circumstances it is permissible for a signal aspect to be extinguished in the event no route has been set up to the signal, no train is approaching within viewing distance of the signal aspects or no confusion will be caused by not showing any aspect indications. If a signal needs to be replacing, it must first be set to display a red danger aspect and the associated route must be canceled [35].

3.3.3 Switch

A switch is a point on the railway network which diverge one rail track into two or converges two deferent tracks into a single track as depicted in Figure 3-3. The single track is called a stem and the two deferent tracks are classified as left and right branches. In the definition, the left and right branches are identified from the stem of the switch. The train can move from any branch to the station and from the station to any branch while a train can't move from one branch to another. Switch operation is controlled by a switch rod controller. The point machine is the equipment to move the switch.

Figure 3-3: Switch and Point machine [42]

The switch individually operated or locked shall be operated on human machine interface (HMI). The functions include route lock, section lock and manual lock. The control and indication circuit of the switch machine shall satisfy the requirements. The switch shall be controlled both by single switch calling and route independently, and man's control is before the route. The interlocking switch is controlled by route lock, section lock and individually manual lock or other ways. If the switch is locked, it cannot be activated. When the switch starts up, it shall be switched to the correct position. If the switch cannot convert to the required position within the required time because of failure, the alarms will be shown, and the switch shall be operated to its original position. The circuit shall be cut off automatically when the switch completes its switch over. The action current shall be cut off automatically if the circuits of the switch machines are fault [43]. The switch has its position display and ensures: the correct display of a switch position must satisfy, the actual position of the switch is in accordance with the operation requirements, and two contacts of the switch machine are in the right position. When switch starting, position indication must be shut off in advance. When there is a switch split, it shall be displayed. The individually locking of the switch cannot influence the position indication.

3.3.4 Train detection

There are different types of train detection systems. Axel counter is one of them. The system checks whether the zone is free by setting the corresponding axle counter in the section being examined to count the number of axles entering and leaving the zone and also controls the corresponding track relay, to automatically check the section of the idle condition and occupation [42]. The axle counter is divided into indoor and outdoor equipment, a wheel sensor is arranged respectively at the starting point and ending point of the track section, and used together with the evaluation board for detecting the information of the wheelset of the train. Each wheel sensor includes two groups of systems, which are used for distinguishing the driving direction of the train. Each wheel sensor is connected with the evaluation board by four core signal cable, which supplies the power for the wheel sensor and transfers the data of the axle to the evaluation board.

The axle counting board (ACB) of the axle counting system process the data of axle of all connected counting probes, and outputs the results of vacancy and occupation of the detected section into the relevant system (e.g. interlocking system) in the manner of

interface conditions of a relay (output of the vacant section is direct current (DC) >=21.6V; the output of the occupied section is DC<=2Volt); Figure 3-4.

The block diagram of the system components is shown as follows:

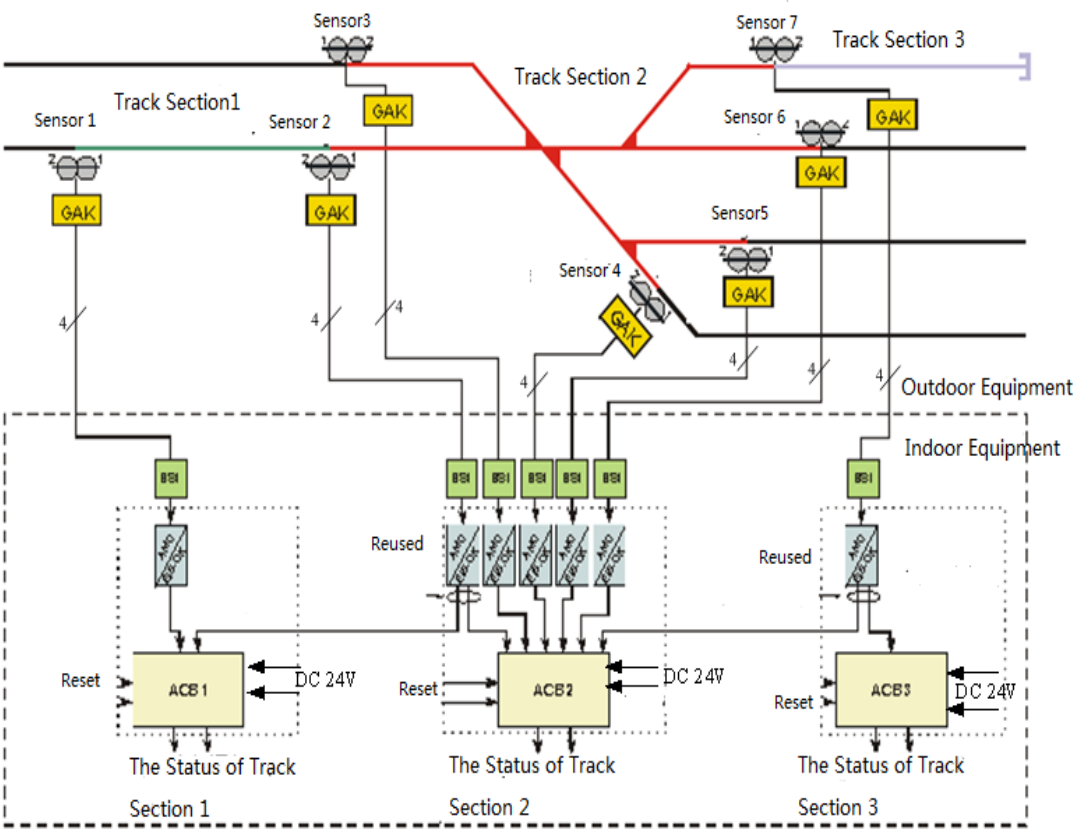

Figure 3-4: Block diagram of axle counting system [10]

The function of the axle counting system is to check and distinguish the state of vacancy and occupation by train on the track section under monitoring. Meanwhile, the distinguishing results are outputted in the form of relay conditions. When the train enters the track section under monitoring, the condition of loss of excitation representing the occupation of the track section is outputted. In case of equipment failure, the condition of loss of excitation for the occupation of the track section is outputted until the equipment is repaired.

Figure 3-5: Axle counter [42]

If A Axle= B Axle, then the section is clear; If A Axle≠ B Axle, then the section is occupied; Figure 3-5.

The interfaces of the axle counting system are divided into internal interface and external interface, in which, the external interface includes the interface for axle counting and interlocking system, as well as the interface for axle counting and maintenance support system (MSS) system.

The external interface is between the system and interlocking. The interface between the host axle counting device and the interlocking device is of safety relay interface, including track relay and zero-reset relay. In case of initial use of the equipment or fault repairing, it is needed that the person on duty of the station carries out the zero-reset of the section while confirming the state of vacancy of section manually. The host axle counting device gathers the closed contact of the zero-reset relay for the realization of zero resets of the section.

ACS2000 computer axle counting subsystem (Figure 3-6) adopts the two-channel programmable microprocessor system, the 2-in-2 safety-type arithmetic unit checks and processes all safety information.

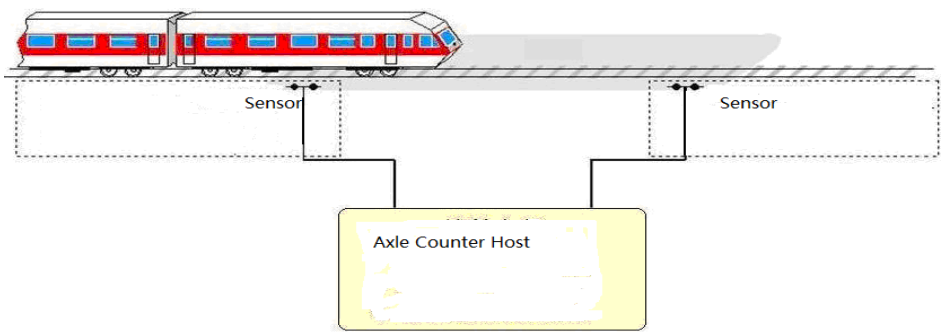

Figure 3-6: Function diagram of ACS2000 axle counting system [10]

The function of the ACS2000 axle counting system is to check and distinguish the state of vacancy and occupation by train on the track section under monitoring. Meanwhile, the distinguishing results are outputted in the form of relay conditions.

3.3.5 Cable cabinet

Connect the cables between the equipment of indoor and outdoor with lighting protection function by using a lighting protection device.

3.3.6 Relay cabinet

Contain the safety relays that are related to the interlocking relationship.

3.3.7 Interface cabinet

Connected with Relay cabinet and Ilock cabinet to collect the status of relay for Ilock process system.

3.3.8 Ilock cabinet

It is the brain of Ilock system by using **"**2*2oo2**"** structure. "2*2oo2" means, there are two IPSs (Interlocking Process System) with the redundant structure of hardware in each IPS [44].

3.3.9 SDM (Signal Diagnosis Maintenance)

The main function of Signal Diagnosis Maintenance (SDM) of ilock is system diagnosis and maintenance of the Computer Interlocking system as well as monitoring of interface equipment on-line. As a subsystem of ilock, it realizes the function of monitoring and recording the system and interface equipment of ilock on-line. SDM is responsible for CBI diagnostic and failure recording, then sending the corresponding information to SDM through the network; the equipment shall be set in the signaling equipment room.

3.3.10 Redundant network subsystem (RNET)

Ilock system adopts an Ethernet redundancy network structure based on a high-speed switch, enhancing the reliability of the network system. Dual Ethernet interface cards are installed in each subsystem using a network to communicate with other subsystems. One network is the fault, the subsystem can use another network, at the same time, the fault diagnosis shall be given in the SDM subsystem and the faults hall be maintained in time.

3.4 Principles for safe train movement

A few of the requirements defined for the safe movement of trains on a railway are summarized. Principles for the safe movement of trains refer to the prevention of safety-critical events and safely ensuring the interlocking response. Safety-critical events include collisions between trains traveling on the same track or in the same direction. In the event a safety-critical event cannot be prevented, the interlocking must then act to minimize the loss of human life and infrastructure damage by safely controlling the operation of the signaling elements. The signaling element functions are controlled by preventing the setting of routes with the affected elements [45].

The POSMOR (Principles of Safe Movement on Rails) states that railway infrastructure must be functional and in good condition such that railway vehicles can safely travel upon the tracks. Railway vehicles must conform to applicable loading specifications. Defined sections in a station must be clear, i.e. sections must be free of all obstructions, required points must be set in the correct position and the complete train must pass/leave a section. Departure and destination points in signal plans and design layouts must be clearly defined. Train drivers and control operators must be aware of the limit of authority given to a train to travel across a designated section. A movement authority shall not allow conflicting train movements along a route. Whilst moving, train drivers must adhere to speed instructions and trackside indications. A train driver must always halt train movement when and where scheduled to do so [38].

3.5 Fail-safe system

Safety-critical systems include some equipment which are very important for the system safety and it is required that this equipment should be always failure-free. Whereas, any device or equipment cannot be fully reliable in the real world. A fail-safe system is defined as a control system that either responds safely by forcing a system into a predefined safe state or continues to function safely after a failure. A safe state refers to the system executing an appropriate response in the event of a critical situation [38]. The fail-safe logic of the interlocking is built into the system. This logic is extracted from the control table conditions which only allows the interlocking to set a route provided all safety requirements are met first. A signaling element that fails should fail silently and should

not affect the operation of other elements. In the event of an element failure, a route that requires this element should not be allowed to be set. For an element to fail safely, it must either perform a right or a wrong side failure. An example of a right-side failure is when a signal aspect indicates red when it should be showing green. This is incorrect but not a hazardous situation. An example of a wrong side failure is when a signal aspect is displaying green instead of a red indication. This could result in a critical accident.

Every equipment and device has a fail-safe procedure in the railway interlocking system [35]. System engineers are also considered the fail-safe procedure of all components used in the signaling system when they are designing an interlocking system.

3.6 Fail-safe interlocking

The interlocking system must satisfy safety requirements for both software and hardware. The software must be developed according to defined standards and under key fail-safe railway interlocking principles. Safety certified components can be used to satisfy the hardware requirements for the interlocking. The hardware (i.e. signaling field equipment) is also instructed to operate in a defined manner in the event of failure [35].

These requirements state that route requests received by the interlocking must first proceed through a series of checks which are used to verify the behavior of the interlocking system. These checks ensure that no train can be directed into a route already occupied by another train [38]. To avoid a collision, two trains should never be located in the same track section. Subsequently, any two routes cannot share any portion of a track circuit. Additional requirements state that a safe separation between trains must be ensured by providing an overlap beyond the end of a route and the destination signal. A train should sequentially occupy all track sections and overlaps of its required route until it reaches the last track section, i.e. the train must completely clear the route before another train may be allowed [41].

The basic contents of interlocking are [36]:

1. To prevent the establishment of a route that will lead to a conflict between vehicles, and guarantee that all the switches that the train or shunting car went through are locked at the position in accordance with the direction of the opening route; the signal indication must conform to the established route.

2. Open the signal only when the route is free.
3. The switch position is required to be checked correctly; the switches should be locked after the signal is opened.
4. If a hostile signal is not closed, the relevant signal cannot be opened.

When route request comes from train control center (TCC), firstly tracks that are included in the requested route are checked and if there is an occupation, the route request is rejected by the interlocking system. If there is no occupation, these tracks are locked electronically. Then if there is a switch on the route, the switch position is changed to the appropriate position (switch has two positions named normal or reverse) and feedback (position indication information) has waited for confirmation. If any problem occurs, route request is rejected and necessary notifications are sent to TCC. After that signal lights are set up properly and again feedback (signal light indication information) is waited for confirmation. If there is no problem, the route request is accepted [38].

While the train is moving on a reserved route for itself, track circuits are checked by an interlocking system if the train is entering to tracks respectively. If there is a switch, its position is always checked until the route is released to ensure safety, and also signal lights are checked to be sure if it shows the right notification or not. Finally, when the train reaches to end of the route, all track circuit occupations are cleared and the route is released for the next request by the interlocking system [46].

3.7 Computer-based interlocking system

Computer hardware (microprocessor, memory, hard drive, etc. and input and output cards) and computer software (firmware, operational system and control program) create CBI interlocking [47]. Computer-based interlocking uses the computer to realize the interlocking relationship in the station and uses the relay circuit as interface equipment between a computer host and outdoor signal, switch machine and track circuit [36]. Interlocking functions are defined in a control program, also interlocking inputs and outputs and their association with the hardware are declared in the control program. The control program in the case of CBI is called interlocking logic. In the instance of the point's machine, the computer interlocking is not capable to provide power to directly control the point's machine. Relays are still used to perform this functionality [48].

Computer hardware of CBI interlocking is different from a normal personal computer (PC) because the hardware must be specialized for safety-related applications. Therefore, its construction is specific as well as the operating system and firmware that is again different from a PC. However, CBI computers like PCs process information sequentially reading and executing instructions step by step in a clock cycle. Interlocking logic is kept in a central processing unit module. This is a list of instruction predesigned specifically for a signaling layout and rules of operation (defined in control tables), checked, tested and compiled that can be performed by this interlocking hardware (computer) preventing trains from colliding.

To ensure the high degree of reliability of computer interlocking, the host computer and the interlocking machine of the computer interlocking system generally adopts a redundant structure. There are three major forms of system redundancy, depended on special national requirements, in various electronic interlocking systems. They are a 2oo2 system, 2oo3 system and 2*2oo2 system.

For the 2oo2 system, the same inputs are processed by two independent channels. The outputs of two independent channels are compared using a safety comparison circuit. The interlocking functions are carried out only if both results are equal, otherwise, the system will enter into a safe state. Consider the 2oo3 system, the system can operate as long as two channels are functioning. The 3-vote-2 system structure is a reliable multicomputer interlock system composed of fault handling shielding technology. The system has three hosts: host A, host B and host C. Each host is a separate module, and each host running the same software, the implementation of the same operation, and the results of the implementation of the vote into the voting machine. So it can lead to results of the vote as a result of the system output to the control output layer [36].

Double 2oo2: There are two IPSs (Interlocking Process System) with a redundant structure of hardware in each IPS. Includes Series I & Series II (Figure 3-7); a work, the other is hot standby. For series I/II; includes 2 CPU modules, each CPU module executes an interlocking control program, the result of execution was compared. If the result is the same, then output the result, else the other Series (hot standby) works [5].

3.7.1 AA-LRT CBI subsystem

AA-LRT CBI subsystem is mainly composed of "2*2oo2" interlocking computer, hot-redundant network, HMI, SDM, etc. as depicted in Figure 3-7. CBI must ensure the safety train-running, and control the routes, signals and switches under the stipulated interlocking conditions and time sequences to make sure that the interlocking among the signal elements in the route such as track sections, switches and signals are safe. For the safety operation, CBI must adopt the security guarantees measure.

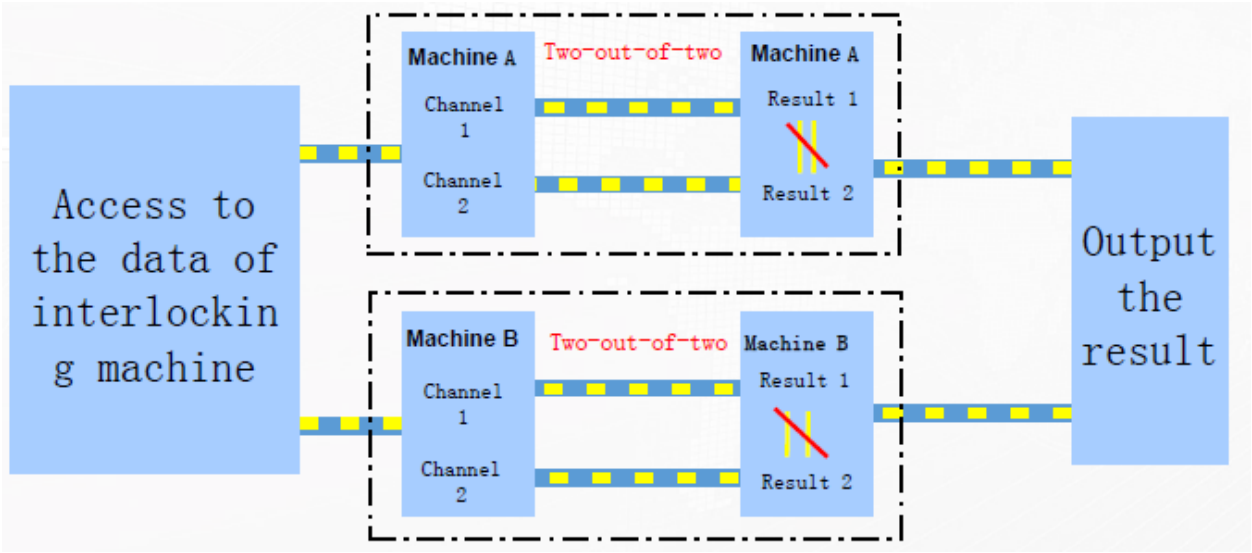

Figure 3-7: Double two-out-of-two redundancy [44]

3.7.2 AA-LRT CBI subsystem structure

There are 8 main stations on the East-West line and the North-South line, controlling the signals, switches and routes on the mainline through the CBI subsystem installed in 8 stations. Mainline CBI subsystem structure is shown in Figure 3-8.

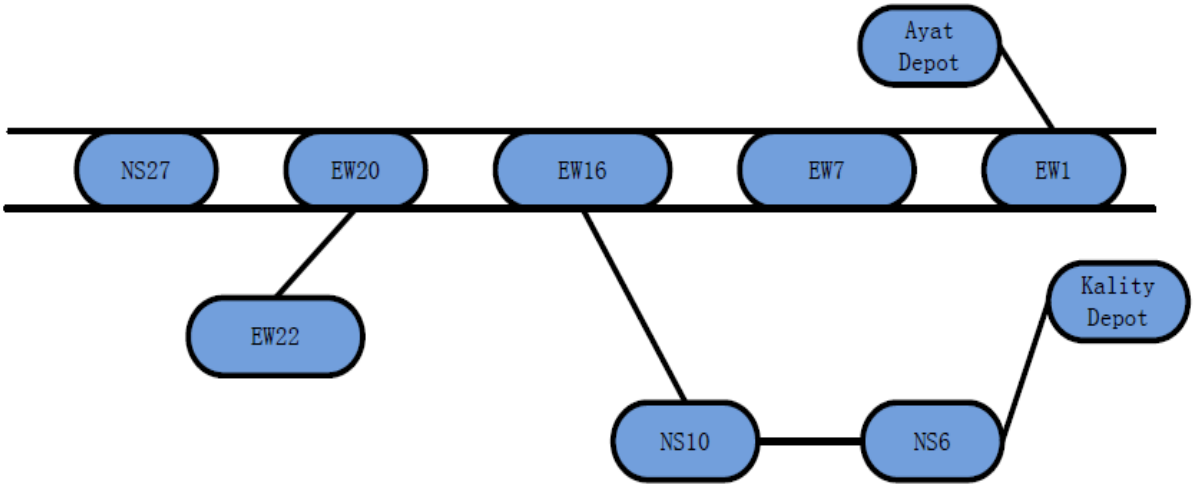

Figure 3-8: Structure figure of CBI subsystem stations [10]

The equipment of the CBI subsystem mainly distributed in main stations, the structure is as the following:

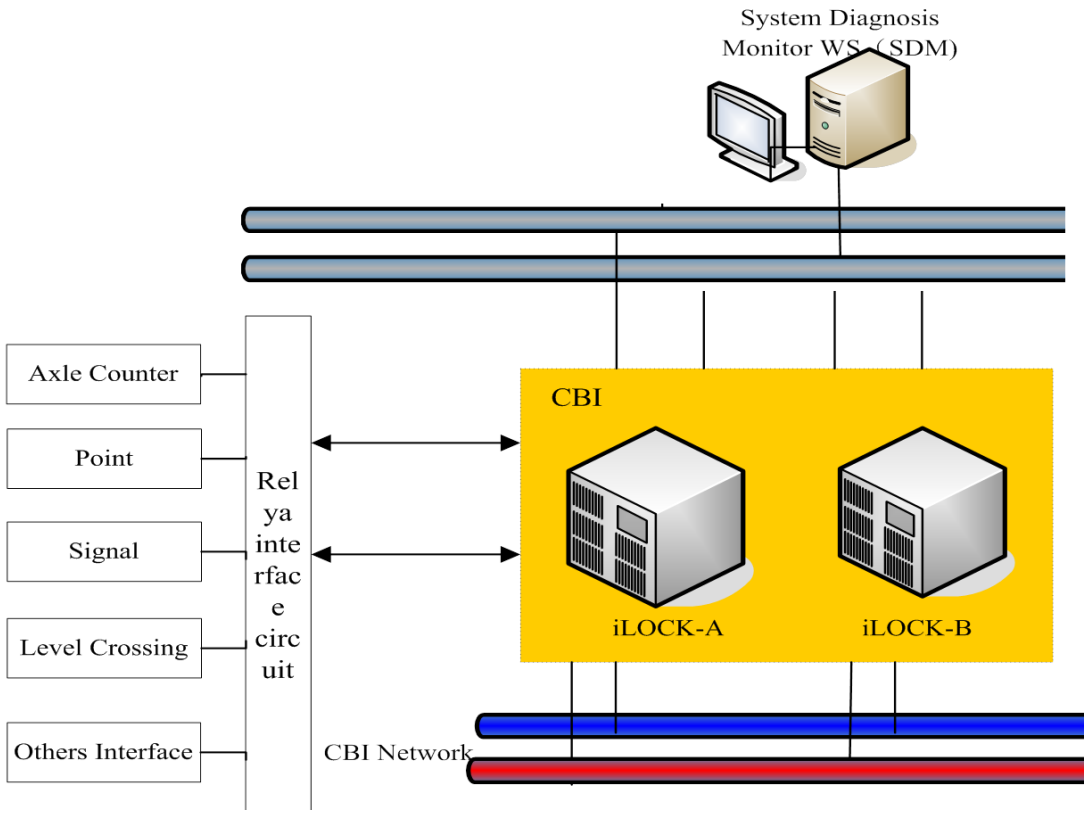

Figure 3-9: Centralized station CBI subsystem structure [10]

There are eight main stations on the East-West Line and the North-South line: EW1, EW7, EW16, EW20、EW22, NS27, NS10 and NS6.

The interlocking system in Ayat depot and Kality depot are the same as the iLOCK system in the mainline. There is a test line in Kality depot supporting the test operation function. Test line and Kality depot share a set of interlocking equipment, a test terminal used to train operation shall be set in the test line control room.

CHAPTER 4 MODEL DEVELOPMENT

4.1 Introduction

It is desirable to obtain a numeric indicator of interlocking system performance effectiveness by considering important factors such as reliability, availability and safety.

Reliability, availability and safety analysis of interlocking system controller and components of AA-LRT is used to decide system changes that increase system efficiency and profits to a company. Reliability, availability and safety modeling simulates the configuration, redundancy architecture, operation, failure and repair of interlocking equipment. The inputs to this modeling include the physical components structure, failure and repair data in a system. The outputs can determine how effective the system can be over the railway transportation system.

This chapter goes through the quantitative calculation of reliability, availability and safety of interlocking control architecture/the CBI controller and interlocking system components of AA-LRT.

The key benefits of reliability, availability and safety modeling of the interlocking system include:

- Identifying appropriate interlocking control architectures in the early design
- Identifying the interlocking system equipment's failure priorities
- Optimizing investment cost of production
- Increasing the effectiveness of the interlocking system

4.2 Markov analysis model

Modeling using Markov analysis is widely used in safety and reliability engineering. The reliability behavior of a system is modeled by Markov chains as a state transition net of sequence which consists of a set of descript states that the system can be in, and defines the speed at which transitions between those states takes place. As such, Markov models consist of representations of possible chains of events that are the transition, within

systems, which in the case of reliability and availability analysis corresponds to sequences of failures and repair [8].

Markov analysis is a technique used to obtain numerical measures related to the probability of a given state concerning the availability and reliability of a system or part of a system. The common Markov model is analyzed to determine such measures as the probability of certain states at a time, the amount of time a system is expected to spend in a given state, for example representing the rate of failures and repairs. Based on the approximation of the temporality of all stochastic events by the exponential distribution the Markov analysis is well-suited to handle rare events, unlike simulation-based analysis, and therefore allows such events to be analyzed within a reasonable amount of time. A Markov model (chain) describes a stochastic process within some states in which the probability of occurrence of future states is conditional only upon the current state; past states are inconsequential (the memory-less property).

A Markov model divides the system configuration into several states. Each of these states is connected to all other states by transition rates. It then utilizes transition matrixes and state transition diagrams to represent the various system states and the possible transitions between these states. These state diagrams are more visual than mathematical representations thus they are much easier to interpret. Therefore, Markov analysis can be a powerful RAMS analysis tool. It allows the analyst to model complex, dynamic, highly distributed, fault-tolerant systems that would otherwise be very difficult or impossible to model with classical techniques. Markov techniques decrease the analyst‘s task by reducing the problem from one of mathematical computation to that of state modeling. Model reduction techniques also exist which can yield relatively simple models with an insignificant impact on model accuracy. In many situations, it is also possible to use a combination of Markov analysis and more conventional approaches, e.g., reliability block diagrams, fault trees, etc. in such a way that the resulting individual dynamic portions are relatively small and easy to control.

Markov modeling offers many advantages over other RAMS modeling techniques, some of which are [33]:

- Simplistic modeling approach: The models are simple to generate although they require a more complicated mathematical approach. This is not a problem, however, because mathematics is well suited for the digital computer.

- Redundancy management techniques: system reconfiguration required by failures easily incorporated in the model.

- Coverage: Covered and uncovered failures of components are mutually exclusive events. These are not easily modeled using classical techniques but are readily handled by Markov mathematics.

- Complex systems: many simplifying techniques exist which allow the modeling of complex systems.

- Sequenced events: Often the analyst is interested in computing the probability of an event resulting from a sequence of sub-events. While these types of problems do not lend themselves well to classical techniques, they are easily handled using Markov modeling.

The advantage of the Markov process is that it neatly describes both the failure of an item and its subsequent repair as depicted in Figure 4-1. It develops the probability of an item being in a given state, as a function of the sequence through which the item has traveled.

In this study the interlocking subsystem is treated as a discrete state continuous-time system with two possible outcomes, namely, S1: Good condition and S2 System completely fails. Partial degradation failures and partially working were not considered. The calculation of the reliability and availability of the interlocking subsystem is complicated since the system has elements or subsystems exhibiting dependent failures and involving repair and standby operations.

In this thesis, the state transition model is constructed using two assumptions for Markov modeling.

1. Only one failure will occur at a time.
2. The system starts in the perfect operation when all of the system's modules are operating correctly.

The methodology of the Markov process of reliability modeling of the AA-LRT interlocking system (IS) is shown as follows.

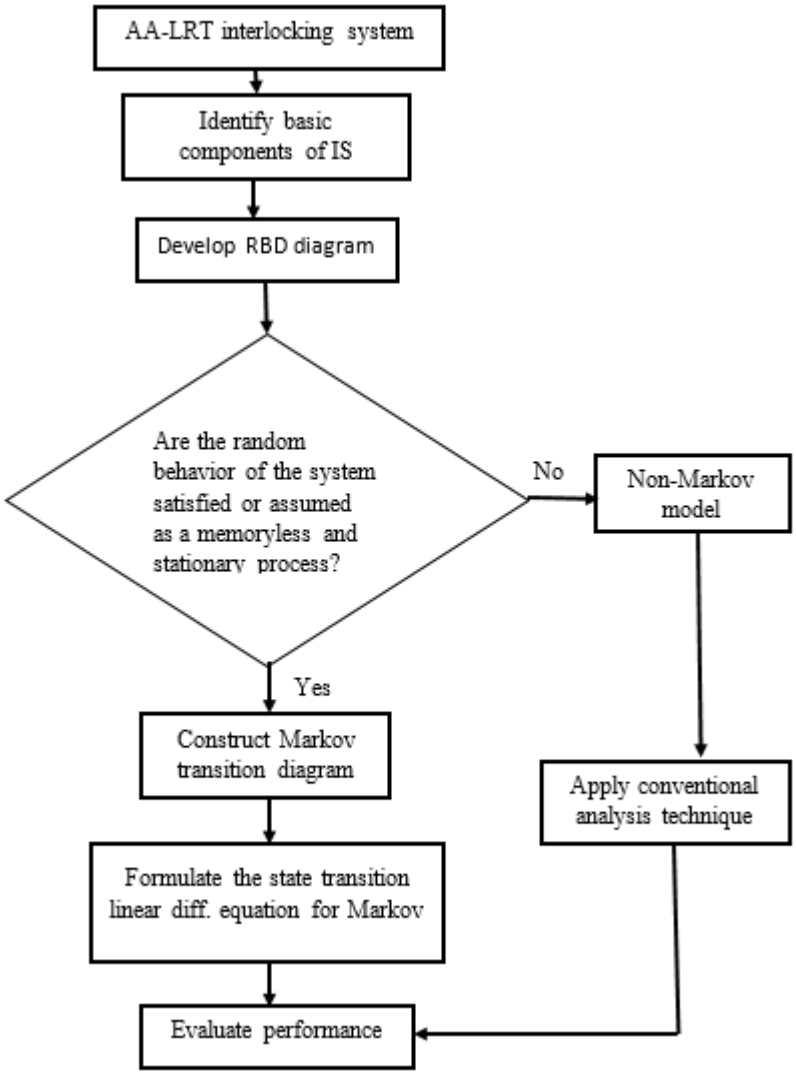

Figure 4-1: Reliability modeling by Markov process [49]

4.3 Modeling of interlocking system controller architectures

4.3.1 Model description

The architecture of an interlocking control system includes the arrangement of all of the individual system components (control processors). It considers the parallel arrangement of system components with a safety comparator circuit, voter circuits, or a combination of the two. When subsystems are arranged in parallel structure with a safety comparator circuit (SCC), the system will not work if one element failed. The safety comparison circuit compares output signals of the processors and forms a control signal only when all the outputs signals coincide otherwise the system will enter into a safe state. When subsystems are arranged in parallel with the voter circuit the system to work only if one element can

operate independently of others. The voter circuit forms a control signal when one of the output signals works.

The M-out-of-N Safety Computing System consists of some computational nodes and logic comparator/voter. Its overall structure is as shown in Figure 4-2.

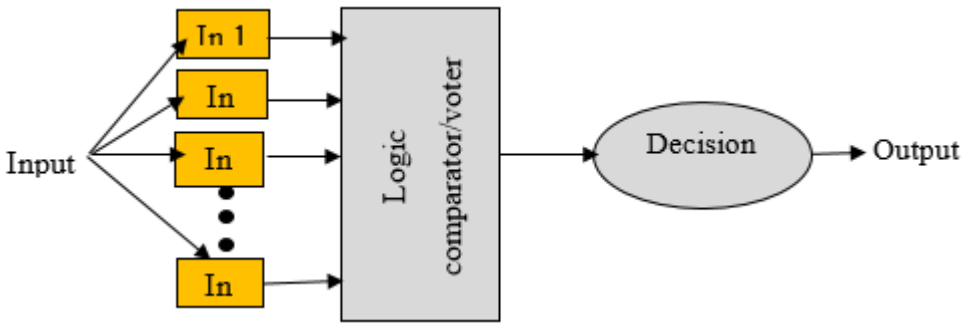

Figure 4-2: Basic model of M-out-of-N interlocking system controller

The simplest case of components in the M-out-of-N configuration is when the components are independent and identical. In other words, all the components have the same failure distribution and whenever a failure occurs, the remaining components are not affected.

The Comparator/voter: output the calculation results decision, so its failure will seriously affect the safety and reliability of the M out of N Safety Computing System.

The Calculation Results Decision Function: The M out of N Safety Computing System makes a decision based on the results that come back from the computational nodes. If the number of the same results is equal to or bigger than M, then output the result as depicted in Figure 4-3. Otherwise, output the fault signal.

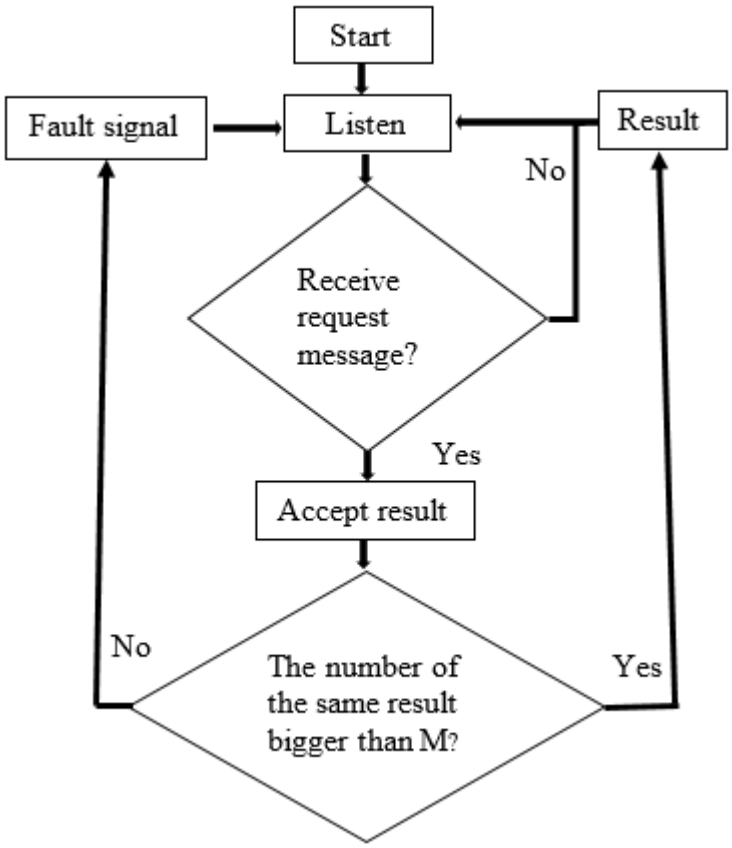

Figure 4-3. The detail process of decision [50]

The comparator and voter circuits are mainly responsible for data distribution, computational nodes scheduling and output decision.

4.3.2 Concept of reliability, availability and safety of railway interlocking equipment

Quality of railway transportation is determined especially by speed and safety of conveyance of passengers and goods to the destination. Both of these parameters depend critically on the reliability of signaling and interlocking systems. Failure of these systems can lead to trains being delayed and, in the worst cases, to derailments and collisions. The reliability of signaling and interlocking equipment is the capability to provide uninterrupted and safe control of train movement in all specified modes and conditions of operations, maintenance and repair.

The set of states in the signaling and interlocking equipment is divided into the following subsets.

- Up States (S_U)
- Operable States (S_O)
- Disabled Protected States (S_P)
- Disabled Hazardous States (S_H)

The up State is a state in which the system is completely suited to all functional and technical requirements on the application and environment conditions. A system in this state is also operable.

The operable state is a state in which all parameters of the system are suitable for all technical requirements related to its possibility to fulfill all intended functions. The disabled state is a state in which even one parameter of the system mismatches its requirements. The disabled protected state is a state in which values of all parameters of the systems determining its possibility to fulfill intended safety functions, are suitable to all given requirements. The disabled hazardous state is a state in which even one parameter of the system determining its possibility to fulfill intended safety functions, is no suited to its requirements. Scenario 4 (worst case scenario) includes the potential of severe damage to the system, hence interfering with railway safety.

Failure-free operation of interlocking equipment is a property of the system to provide continuously its up or operable state during a determined time span or operating time. Safety of interlocking equipment is a property of the system to provide continuously it's up, operable or protected state during a determined time span or operating time. Protected failure does affect the failure-free operation of signaling equipment, but does not affect its safety. Failure-free operation is characterized by up and operable states:

$$\text{Failure} - \text{free operation} = S_U \cup S_O$$

And Safety is characterized by up, operable and protected states.

$$\text{Safety} = S_U \cup S_O \cup S_P$$

Comparison of the two sets shows that failure-free operation is always lesser or equal to Safety: Safety ≥ Failure-free operation

In a specific case, when any failure in the system is a dangerous failure (no protected or degraded operation), safety is equal to failure-free operation.

4.3.3 Model assumptions

The present model includes a series of assumptions and simplifications:

- Independent failures of components
- Exponentially distributed failures, the constant failure rate
- Identical components (with regard to failure rate)
- All components in the initial state at t = 0, the system as good-as-new
- The probability of the same error occurring simultaneously in two different processor modules is very small.
- The safety comparator circuit (SCC) and the voter circuit (V) is considered as absolutely reliable, the component failure rate is zero.
- Repair always restores the system to a fully functional state.

4.3.4 Architectures for interlocking system controller

The interlocking functions programed by software and hardware are made by electronic components which are not robust as mechanical components. This cause that the inherent fail-safe design is hardly applied to electronic interlocking systems. To increase reliability and safety, hardware redundancy is widely used in electronic interlocking systems. There are three major forms of system redundancy, depended on special national requirements, in various electronic interlocking systems. They are the 2oo2 system, 2oo3 system and 2*2oo2 system, where a 1oo1 system is used as a baseline.

4.3.4.1 1oo1 (One-out-of-one architecture)

This is the simplest and minimal system configuration as shown in Figure 4-4. Failure of the one processor (processor A) will cause the whole system to fail (enter into a hazardous state) and the system is operational only if the control system (processor) is available.

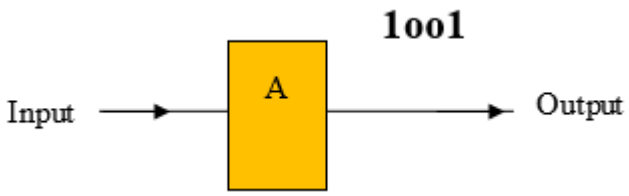

Figure 4-4: 1oo1 architecture [2]

Table 4-1: The states of 1oo1 system depending on the channel state [2]

N.o	State	State of 1oo1 system
	A	
1	Operable	Operable
2	Disabled	Hazardous

If the failure rate ($\boldsymbol{\lambda}$) of the processor is known, parameters of reliability and safety are calculated at a given time according to Table 4-1 as follows [30]:

Failure-free probability $P_{1oo1}(t)$ is given by

$$P_{1oo1}(t) = e^{-\lambda t}. \tag{4.1}$$

Probability of safety $P_{S1oo1}(t)$ is given by

$$P_{S1oo1}(t) = e^{-\lambda t} = P_{1oo1}(t). \tag{4.2}$$

Probability of failure $Q_{1oo1}(t)$ is given by

$$Q_{1oo1}(t) = 1 - e^{-\lambda t}. \tag{4.3}$$

Dangerous failure $Q_{D1oo1}(t)$ is given by

$$Q_{D1oo1}(t) = 1 - e^{-\lambda t} = Q_{1oo1}(t). \tag{4.4}$$

Failure rate $\lambda_{1oo1}(t)$ is given by

$$\lambda_{1oo1}(t) = -\frac{P'_{1oo1}(t)}{P_{1oo1}(t)} = -\frac{\lambda e^{-\lambda t}}{e^{-\lambda t}} = \lambda \tag{4.5}$$

Mean operating time to failure $T_{1oo1}(t)$ is given by

$$T_{1oo1}(t) = \frac{1}{\lambda}. \tag{4.6}$$

Dangerous failure rate $T_{D1oo1}(t)$ is given by

$$T_{D1oo1}(t) = \int_0^\infty P_{S1oo1(t)dt} = \int_0^\infty e^{-\lambda t} dt = \frac{1}{\lambda}. \tag{4.7}$$

To calculate the availability of the control system, the Markov process model is developed with a given failure rate ($\boldsymbol{\lambda}$) and repair rate (μ) of the control system.

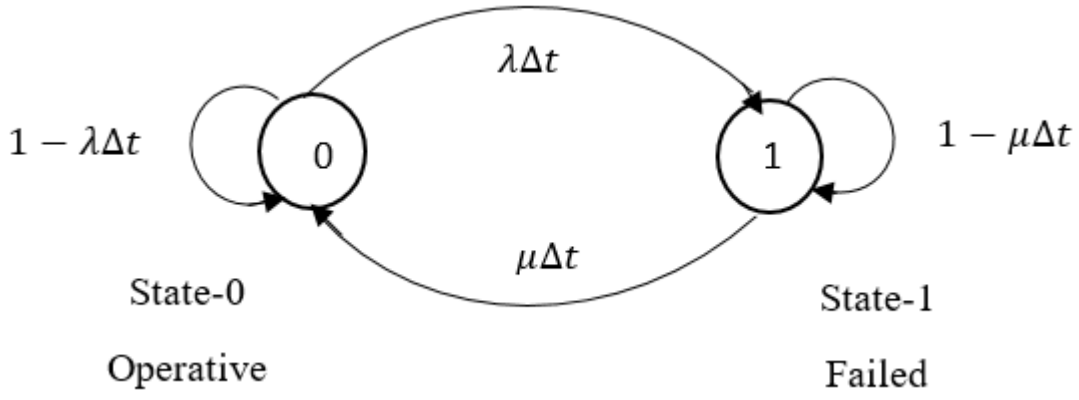

Figure 4-5: Markov model of 1oo1 system [51], [52]

Where $\boldsymbol{\lambda}$ and μ are the failure rate and repair rate of each processor respectively.

It is assumed that repair always restores the system to a fully functional state for all architectures.

The probability that the system is in the operating state after time interval Δt i.e. at time (t + Δt) is given by:
p(t + dt) = [(Probability of being in operating state at time t) and (Probability of not failing between t and t + dt)] + [(Probability of being failed states at time t) and (Probability of being repaired between t and t + dt)].
Probabilities of failure between t and dt are $\lambda_i$dt.
Probabilities of not failing between t and dt are $(1-\lambda_i dt)$.
Probabilities of repair between t and dt are $\mu_i$dt.

The Markov equations for this system are:

$$\begin{bmatrix} p_0(t+\Delta t) \\ p_1(t+\Delta t) \end{bmatrix} = \begin{bmatrix} 1-\lambda\Delta t & \mu\Delta t \\ \lambda\Delta t & 1-\mu\Delta t \end{bmatrix} \begin{bmatrix} p_0(t) \\ p_1(t) \end{bmatrix}. \quad (4.8)$$

Availability permits the model to have a cyclic Markov chain, thus allowing one to examine the effect of repair on system performance. For this simple example, the availability $A(t) = p_0(t)$.

The differential equations describing the model of Figure 4-5 are:

$$\frac{dp_0(t)}{dt} = -\lambda p_0(t) + \mu p_1(t). \quad (4.9)$$

$$\frac{dp_1(t)}{dt} = \lambda p_0(t) - \mu p_1(t). \quad (4.10)$$

The operational state of this subsystem is state 0.

As the time approaches infinity, the probability of being in the operational state approaches a steady-state value is given by

$$p_0(\infty) = \frac{\mu}{\lambda + \mu}. \quad (4.11)$$

Subsequently, we will see that this constant is known as steady-state availability. The steady-state availability is given by

$$A_{1oo1} = p_0(\infty) = \frac{\mu}{\lambda + \mu}. \quad (4.12)$$

4.3.4.2 2oo2 (Two-out-of-two architecture)

In this system, the same inputs are processed by two independent control processors A and B, connected in parallel, and are working simultaneously; Figure 4-6. Safety comparison circuit (SCC) compares output signals of the processors and forms a control signal only when both the outputs signals coincide otherwise the system will enter into a safe (protected) state. When both the processors are disabled, the system will enter into hazardous state as depicted in Table 4-2.

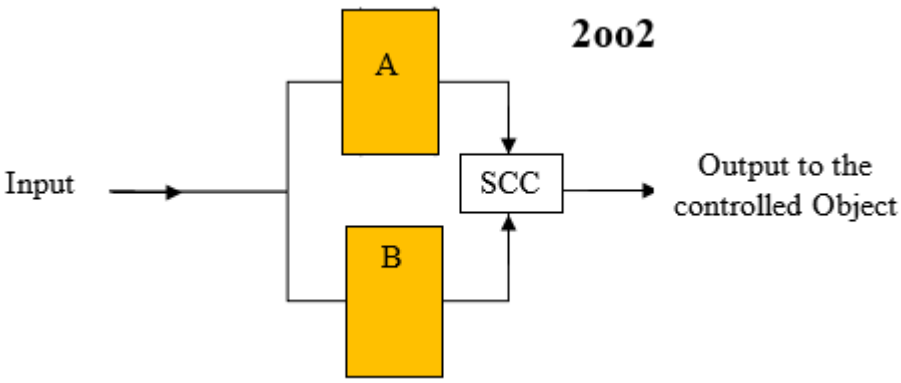

Figure 4-6: 2oo2 architecture [5]

Table 4-2: The states of the 2oo2 system depending on the channel states [2], [30]

No	State		State of 2oo2 system
	A	B	
1	Operable	Operable	Operable
2	Operable	Disabled	Protected
3	Disabled	Operable	Protected
4	Disabled	Disabled	Hazardous

Reliability and safety parameters of 2oo2 can be calculated according to Table 4-2 with the following formula [30]:

Failure-free probability $P_{2oo2}(t)$ is given by

$$P_{2oo2}(t) = P^2{}_{1oo1}(t) = e^{-2\lambda t}. \tag{4.13}$$

Probability of failure $Q_{2oo2}(t)$ is given by

$$Q_{2oo2}(t) = 1 - e^{-2\lambda t}. \tag{4.14}$$

Failure rate $\lambda_{2oo2}(t)$ is given by

$$\lambda_{2oo2}(t) = -\frac{P'_{2oo2}(t)}{P_{2oo2}(t)} = -\frac{(e^{-2\lambda t})'}{e^{-2\lambda t}} = -\frac{(-2\lambda)e^{-2\lambda t}}{e^{-2\lambda t}} = 2\lambda. \tag{4.15}$$

Probability of safety $P_{S2oo2}(t)$ is given by

$$\begin{aligned} P_{S2oo2}(t) &= (e^{-\lambda t})^2 + 2e^{-\lambda t}\left(1 - e^{-\lambda t}\right) = e^{-2\lambda t} + 2e^{-\lambda t} - 2e^{-2\lambda t} \\ &= 2e^{-\lambda t} - e^{-2\lambda t}. \end{aligned} \tag{4.16}$$

Mean operating time to failure T_{2oo2} is given by

$$T_{2oo2} = \int_0^\infty P_{2oo2}(t)dt = \int_0^\infty (e^{-2\lambda t})dt = \frac{1}{2\lambda}. \tag{4.17}$$

Probability of dangerous failure $Q_{D2oo2}(t)$ is given by

$$Q_{D2oo2}(t) = Q^2{}_{1oo1}(t) = (1 - e^{-\lambda t})^2 = 1 - 2e^{-\lambda t} + e^{-2\lambda t}. \tag{4.18}$$

Dangerous failure rate $\lambda_{D2oo2}(t)$ is given by

$$\lambda_{D2oo2}(t) = -\frac{P'_{S2oo2}(t)}{P_{S2oo2}(t)} = \frac{2\lambda\left(1 - e^{-\lambda t}\right)}{2 - e^{-\lambda t}}. \tag{4.19}$$

Mean Operating time to hazardous failure T_{D2oo2} is given by

$$T_{D2oo2} = \int_0^\infty P_{S2oo2}(t)dt = \int_0^\infty (2e^{-\lambda t} - e^{-2\lambda t})dt = \frac{3}{2\lambda}. \tag{4.20}$$

To calculate the availability of the control system, the Markov process model is developed with a given failure rate ($\boldsymbol{\lambda}$) and repair rate (μ) of the control system.

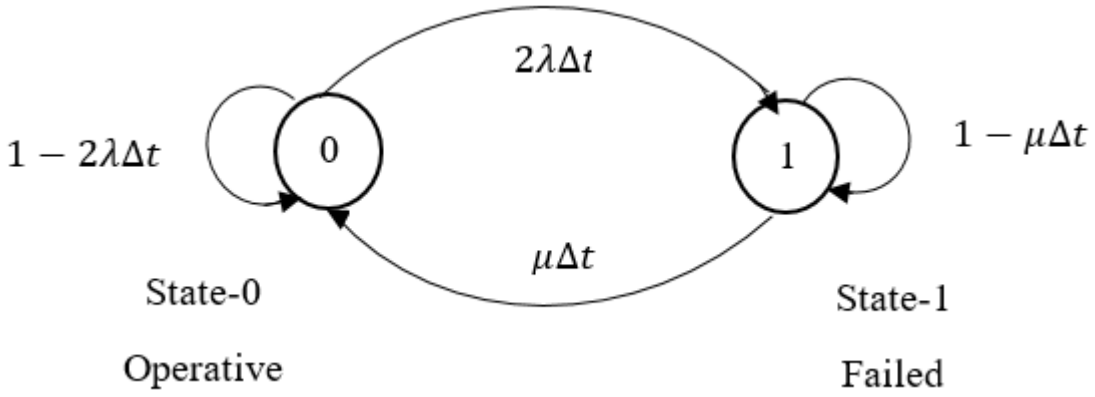

Figure 4-7: Markov model of 2oo2 system

The Markov equations for this system are:

$$\begin{bmatrix} p_0(t+\Delta t) \\ p_1(t+\Delta t) \end{bmatrix} = \begin{bmatrix} 1-2\lambda\Delta t & \mu\Delta t \\ 2\lambda\Delta t & 1-\mu\Delta t \end{bmatrix} \begin{bmatrix} p_0(t) \\ p_1(t) \end{bmatrix}. \quad (4.21)$$

For this system, the availability $A(t) = p_0(t)$.

The differential equations describing the model of Figure 4-7 are:

$$\frac{dp_0(t)}{dt} = -2\lambda p_0(t) + \mu p_1(t). \quad (4.22)$$

$$\frac{dp_1(t)}{dt} = 2\lambda p_0(t) - \mu p_1(t). \quad (4.23)$$

The operational state of this subsystem is state 0.

As the time approaches infinity, the probability of being in the operational state approaches a steady-state value is given by

$$p_0(\infty) = \frac{\mu}{2\lambda+\mu}. \quad (4.24)$$

Subsequently, we will see that this constant is known as steady-state availability. The steady-state availability is given by

$$A_{2oo2} = p_0(\infty) = \frac{\mu}{2\lambda+\mu}. \quad (4.25)$$

4.3.4.3 2oo3 (Two-out-of-three architecture)

Two-out-of-three architecture functions are processed in three independent control processors A, B and C as depicted in Figure 4-8. If a failure occurs in one of the processors, then that processor is isolated. The interlocking continues as a 2oo2 until the failure is repaired.

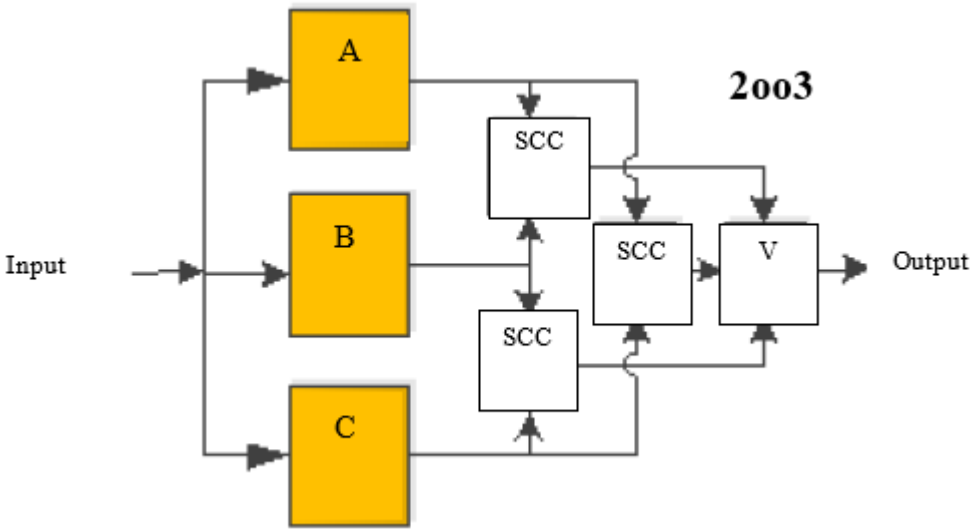

Figure 4-8: 2oo3 architecture [5]

The CPU of the 2oo3 system consists of three identical processor modules which operate as a triple-redundant fault-tolerant system with redundancy management. In the majority voting system, the processor modules operate in parallel, all receiving the same inputs and performing the same tasks. Their outputs are compared by using a safety comparison circuit (SCC) and the system output is derived in accordance with the majority vote. The comparison and voting are achieved by redundancy management hardware which can isolate any module which is in disagreement with the other two. The system will continue to work as a fail-safe system in two-out-of-two configuration until the failed module is repaired or replaced when the system reverts to the triple system. When all or two of the processors are operable, the 2oo3 system is also operable. When two of the processors are disabled at the same time, the system will enter into a safe (protected) state and when all of the processors are disabled simultaneously, the system will enter into a hazardous state as depicted in Table 4-3.

Table 4-3: The states of 2oo3 system depending on the channel state

N.o	State						State of 2oo3 system
	A	B	C	**A ∩ B**	**B ∩ C**	**A ∩ C**	
1	Operable	Operable	Operable	Operable	Operable	Operable	Operable
2	Operable	Operable	Disabled	Operable	Protected	Protected	Operable
3	Operable	Disabled	Operable	Protected	Protected	Operable	Operable
4	Operable	Disabled	Disabled	Protected	Hazardous	Protected	Protected
5	Disabled	Operable	Operable	Protected	Operable	Protected	Operable
6	Disabled	Operable	Disabled	Protected	Protected	Dangerous	Protected
7	Disabled	Disabled	Operable	Hazardous	Protected	Protected	Protected
8	Disabled	Disabled	Disabled	Hazardous	Hazardous	Hazardous	Hazardous

Reliability and safety parameters of 2oo3 architecture can be calculated according to Table 4-3 with the following formula:

Failure-free probability $P_{2oo3}(t)$ is given by

$$P_{2oo3}(t) = (e^{-\lambda t})^3 + 3\left(e^{-\lambda t}\right)^2\left(1 - e^{-\lambda t}\right). \tag{4.26}$$

Let $p = e^{-\lambda t}$,

$$\begin{aligned} P_{2oo3}(t) &= p^3 + 3p^2(1-p) = 3p^2 - 2p^3 \\ &= 3e^{-2\lambda t} - 2e^{-3\lambda t}. \end{aligned} \tag{4.27}$$

Probability of safety $P_{S2oo3}(t)$ is given by

$$P_{S2oo3}(t) = 3p - 3p^2 + p^3 = 3e^{-\lambda t} - 3e^{-2\lambda t} + e^{-3\lambda t}. \tag{4.28}$$

Probability of failure $Q_{2oo3}(t)$ is given by

$$Q_{2oo3}(t) = 1 - P_{2oo3}(t) = 1 - 3e^{-2\lambda t} + 2e^{-3\lambda t}. \tag{4.29}$$

Failure rate $\lambda_{2oo3}(t)$ is given by

$$\begin{aligned} \lambda_{2oo3}(t) &= -\frac{P'_{2oo3}(t)}{P_{2oo3}(t)} = -\frac{\left(3e^{-2\lambda t} - 2e^{-3\lambda t}\ \right)'}{3e^{-2\lambda t} - 2e^{-3\lambda t}} \\ &= -\frac{-6\lambda e^{-2\lambda t} + 6\lambda e^{-3\lambda t}}{3e^{-2\lambda t} - 2e^{-3\lambda t}} = 6\lambda\,\frac{e^{-\lambda t} - e^{-2\lambda t}}{3e^{-\lambda t} - 2e^{-2\lambda t}}. \end{aligned} \tag{4.30}$$

Mean operating time to failure T_{2oo3} is given by

$$T_{2oo3} = \int_0^\infty P_{2oo3}(t)dt = \int_0^\infty (3e^{-2\lambda t} - 2e^{-3\lambda t})dt = \frac{5}{6\lambda}. \tag{4.31}$$

Probability of dangerous failure $Q_{D2oo3}(t)$ is given by

$$\begin{aligned} Q_{D2oo3}(t) &= {Q^3}_{1oo1}(t) = \left(1 - e^{-\lambda t}\right)^3 = 1 - 3p + 3p^2 - p^3 \\ Q_{D2oo3}(t) &= 1 - 3e^{-\lambda t} + 3e^{-2\lambda t} - e^{-3\lambda t}. \end{aligned} \tag{4.32}$$

Dangerous failure rate $\lambda_{D2oo3}(t)$ is given by

$$\lambda_{D2oo3}(t) = -\frac{P'_{S2oo3}(t)}{P_{S2oo3}(t)} = -\frac{\left(3e^{-\lambda t} - 3e^{-2\lambda t} + e^{-3\lambda t}\ \right)'}{3e^{-\lambda t} - 3e^{-2\lambda t} + e^{-3\lambda t}}$$

$$\lambda_{D2oo3}(t) = 3\lambda \frac{1 - 2e^{-\lambda t} + e^{-2\lambda t}}{3 - 3e^{-\lambda t} + 2e^{-2\lambda t}}. \quad (4.33)$$

Mean Operating time to hazardous failure T_{D2oo3} is given by

$$T_{D2oo3} = \int_0^\infty P_{S2oo3}(t)dt = \int_0^\infty \left(3e^{-\lambda t} - 3e^{-2\lambda t} + e^{-3\lambda t}\right)dt = \frac{11}{6\lambda}. \quad (4.34)$$

To calculate the availability of the control system, the Markov process model is developed with a given failure rate ($\boldsymbol{\lambda}$) and repair rate (μ) of the control system.

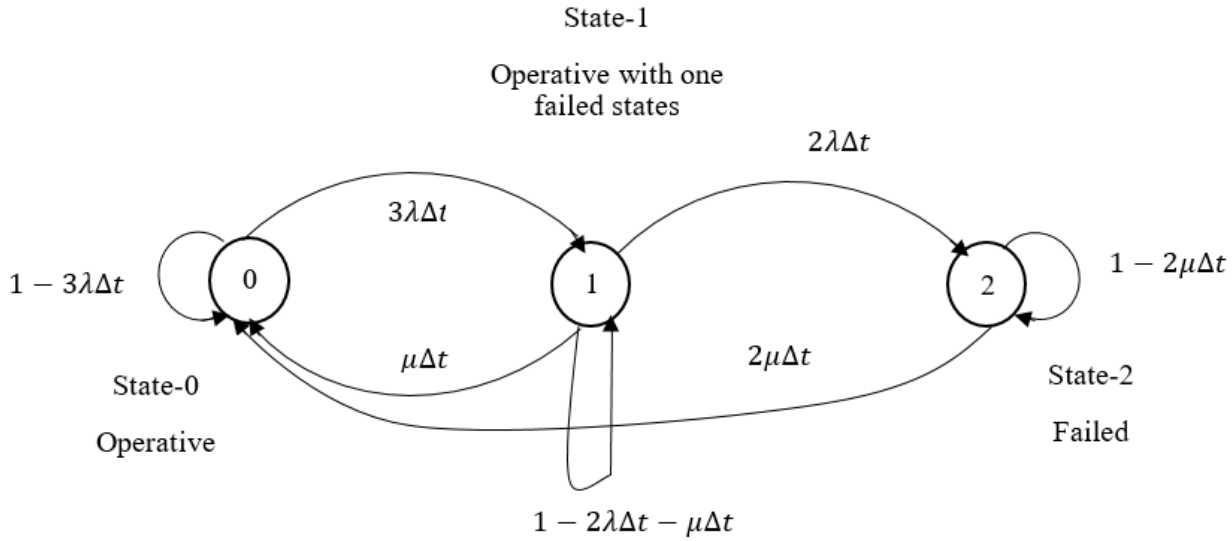

Figure 4-9: Markov model of 2oo3 system [53]

The Markov equations for this system are:

$$\begin{bmatrix} p_0(t+\Delta t) \\ p_1(t+\Delta t) \\ p_2(t+\Delta t) \end{bmatrix} = \begin{bmatrix} 1 - 3\lambda\Delta t & \mu\Delta t & 2\mu\Delta t \\ 3\lambda\Delta t & 1 - 2\lambda\Delta t - \mu\Delta t & 0 \\ 0 & 2\lambda\Delta t & 1 - 2\mu\Delta t \end{bmatrix} \begin{bmatrix} p_0(t) \\ p_1(t) \\ p_2(t) \end{bmatrix}. \quad (4.35)$$

For this 2oo3 system, the availability $A(t) = p_0(t) + p_1(t)$.

The differential equations describing the model of Figure 4-9 are:

$$\frac{dp_0(t)}{dt} = -3\lambda p_0(t) + \mu p_1(t) + 2\mu p_2(t). \quad (4.36)$$

$$\frac{dp_1(t)}{dt} = 3\lambda p_0(t) - (2\lambda + \mu)p_1(t). \quad (4.37)$$

$$\frac{dp_2(t)}{dt} = 2\lambda p_1(t) - 2\mu p_2(t). \quad (4.38)$$

The operational states of this subsystem are state 0 and state 1.

As the time approaches infinity, the probability of being in the operational state approaches a steady-state value is given by:

$$p_0(\infty) + p_1(\infty) = \frac{2\lambda\mu + \mu^2}{3\lambda^2 + 5\lambda\mu + \mu^2} + \frac{3\lambda\mu}{3\lambda^2 + 5\lambda\mu + \mu^2} = \frac{5\lambda\mu + \mu^2}{3\lambda^2 + 5\lambda\mu + \mu^2}. \quad (4.39)$$

The steady-state availability of the 2oo3 system is given by:

$$A_{2oo3} = p_0(\infty) + p_1(\infty) = \frac{\mu(5\lambda + \mu)}{3\lambda^2 + 5\lambda\mu + \mu^2}. \quad (4.40)$$

*4.3.4.4 2*2oo2 (Double two-out-of-two architecture)*

The current double 2-out-of-2 system has an active hardware redundancy [54]. The active hardware redundancy system can be classified into a cold standby system, hot standby system, and warm standby system according to the status of system operation. Among these systems, the hot standby system has the shortest reconfiguration time. The standby system with a comparator is widely used in high reliability, availability and safety systems. The current double 2-out-of-2 system in this paper is a hot standby system, which has fault-detection, fault-location, and fault-recovery functions, as shown in

Figure 4-10. It is comprised of two 2-out-of- 2 sub-systems; one is the operation sub-system and the other is the hot standby sub-system.

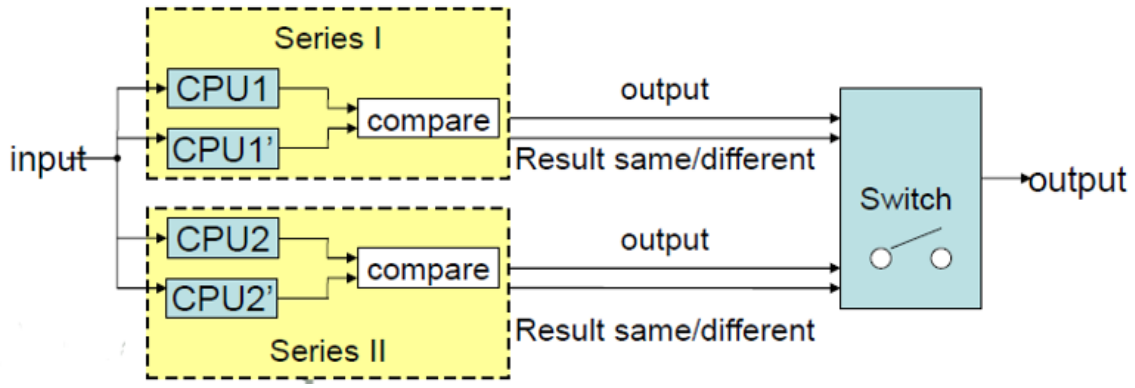

Figure 4-10: Double 2-out-of-2 system [44]

The double 2-out-of-2 system has 4 CPU modules, each CPU module executes the interlocking control program, and the result of execution was compared. If the result is the same, then output the result, else the other Series (hot standby) works. The double 2-out-of-2 system is a fault-tolerant control system that detects a fault using a hardware comparator that switches to a hot standby redundancy. If some certain module of the main sub-system detects faults, the corresponding module of the standby subsystem continues the same operation by speedy reconfiguration. The double 2-out-of-2 system always

supervises each sub-system by detection logic. If any module of the two sub-systems detects a fault, the faulty module is repaired without system power down.

Table 4-4: The states of each 2-out-of-2 system depending on the channel states

No	A		State of 2oo2 system
	A1	A2	
1	Operable	Operable	Operable
2	Operable	Disabled	Protected
3	Disabled	Operable	Protected
4	Disabled	Disabled	Hazardous

No	B		State of 2oo2 system
	B1	B2	
1	Operable	Operable	Operable
2	Operable	Disabled	protected
3	Disabled	Operable	protected
4	Disabled	Disabled	Hazardous

The state of a system represents all that must be known to describe the system at any instant. For reliability models, each state represents a distinct combination of working and failed modules. If each module is in one of two conditions—working or failed—then the complete model for a system of n modules has 2^n states. $2^4 = 16$ states.

When two of the processors from the same series (series I or series II) are operable at the same time, the double 2oo2 system is operable. When two of the processors from different series are disabled at the same time, the system will enter into a safe (protected) state and when all of the processors are disabled simultaneously, the system will enter into a hazardous state as depicted in Table 4-5

Table 4-5: The states of the double 2-out-of-2 system depending on the channel states

No	A1	A2	A	B1	B2	B	2*2oo2 system
1	Operable	Operable	Operable	Operable	Operable	Operable	Operable
2	Operable	Operable	Operable	Operable	Disabled	protected	Operable
3	Operable	Operable	Operable	Disabled	Operable	protected	Operable
4	Operable	Operable	Operable	Disabled	Disabled	Hazards	Operable
5	Operable	Disabled	Protected	Operable	Operable	Operable	Operable
6	Operable	Disabled	Protected	Operable	Disabled	protected	Protected
7	Operable	Disabled	Protected	Disabled	Operable	protected	Protected
8	Operable	Disabled	Protected	Disabled	Disabled	Hazards	Protected
9	Disabled	Operable	Protected	Operable	Operable	Operable	Operable
10	Disabled	Operable	Protected	Operable	Disabled	protected	Protected
11	Disabled	Operable	Protected	Disabled	Operable	protected	Protected
12	Disabled	Operable	Protected	Disabled	Disabled	Hazards	Protected
13	Disabled	Disabled	Hazards	Operable	Operable	Operable	Operable
14	Disabled	Disabled	Hazards	Operable	Disabled	protected	Protected
15	Disabled	Disabled	Hazards	Disabled	Operable	protected	Protected
16	Disabled	Disabled	Hazards	Disabled	Disabled	Hazards	Hazardous

Double 2-out-of-2 reliability and safety parameters can be calculated according to Table 4-5, with the following formula [2]:

Failure-free probability $P_{2*2oo2}(t)$ is given by

$$P_{2*2oo2}(t) = 2e^{-2\lambda t} - e^{-4\lambda t}. \tag{4.41}$$

Probability of safety $P_{S2*2oo2}(t)$ is given by

$$P_{S2*2oo2}(t) = 4e^{-\lambda t} - 6e^{-2\lambda t} + 4e^{-3\lambda t} - e^{-4\lambda t}. \tag{4.42}$$

Probability of failure $Q_{2*2OO2}(t)$ is given by

$$Q_{2*2OO2}(t) = 1 - P_{2*2OO2}(t) = 1 - 2e^{-2\lambda t} + e^{-4\lambda t}. \tag{4.43}$$

Probability of dangerous failure $Q_{D2*2oo2}(t)$ is given by

$$\begin{aligned} Q_{D2*2oo2}(t) = Q^4{}_{1oo1}(t) &= \left(1 - e^{-\lambda t}\right)^4 \\ &= 1 - 4p + 6p^2 - 4p^3 + p^4 \\ &= 1 - 4e^{-\lambda t} + 6e^{-2\lambda t} - 4e^{-3\lambda t} + e^{-4\lambda t}. \end{aligned} \tag{4.44}$$

Failure rate $\lambda_{2*2oo2}(t)$ is given by

$$\lambda_{2*2oo2}(t) = -\frac{P'_{2*2oo2}(t)}{P_{2*2oo2}(t)} = -\frac{\left(2e^{-2\lambda t} - e^{-4\lambda t}\right)'}{2e^{-2\lambda t} - e^{-4\lambda t}} = 4\lambda\frac{1 - e^{-2\lambda t}}{2 - e^{-2\lambda t}}. \tag{4.45}$$

Mean operating time to failure T_{2*2oo2}

$$T_{2*2oo2} = \int_0^\infty P_{2*2oo2}(t)dt = \int_0^\infty (2e^{-2\lambda t} - e^{-4\lambda t})dt = \frac{5}{4\lambda}. \tag{4.46}$$

Dangerous failure rate $\lambda_{D3oo3}(t)$ is given by

$$\lambda_{D2*2oo2}(t) = -\frac{P'_{S2*2oo2}(t)}{P_{S2*2oo2}(t)} = -\frac{\left(4e^{-\lambda t} - 6e^{-2\lambda t} + 4e^{-3\lambda t} - e^{-4\lambda t}\right)'}{4e^{-\lambda t} - 6e^{-2\lambda t} + 4e^{-3\lambda t} - e^{-4\lambda t}}$$

$$\lambda_{D2*2oo2}(t) = 4\lambda\,\frac{1 - 3e^{-\lambda t} + 3e^{-2\lambda t} - e^{-3\lambda t}}{4 - 6e^{-\lambda t} + 4e^{-2\lambda t} - 4e^{-3\lambda t}}. \tag{4.47}$$

Mean Operating time to hazardous failure T_{D3oo3} is given by

$$T_{D2*2oo2} = \int_0^\infty P_{S2*2oo2}(t)dt = \int_0^\infty \left(4e^{-\lambda t} - 6e^{-2\lambda t} + 4e^{-3\lambda t} - e^{-4\lambda t}\right)dt$$

$$T_{D2*2oo2} = \frac{25}{12\lambda}. \quad (4.48)$$

To calculate the availability of the control system, the Markov process model is developed with a given failure rate ($\boldsymbol{\lambda}$) and repair rate (μ) of the control system.

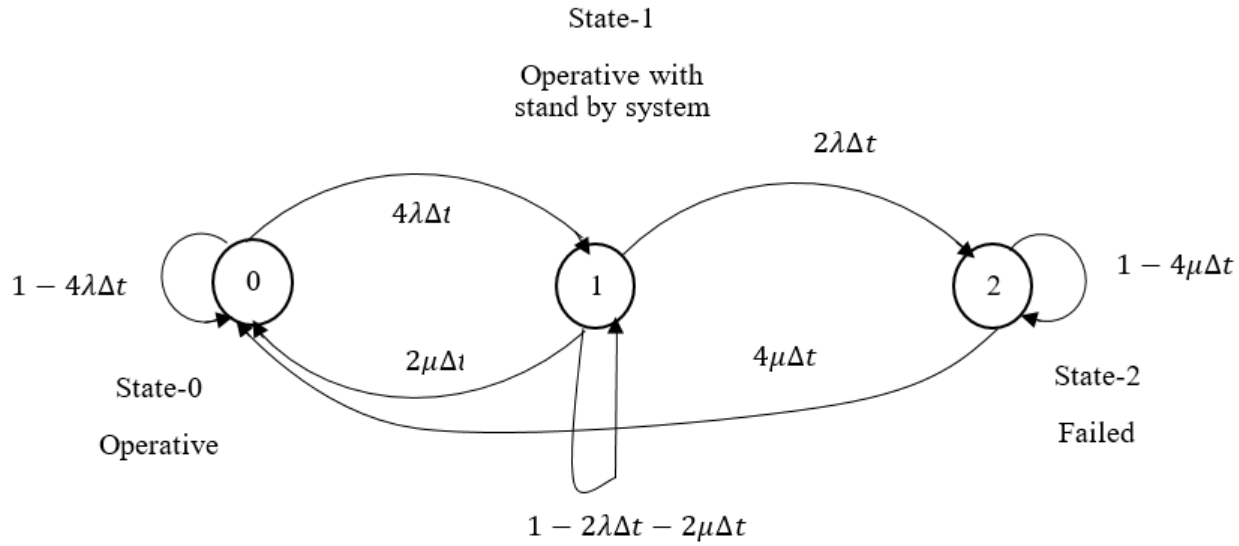

Figure 4-11: Markov model of double 2oo2 system

The Markov equations for this system are:

$$\begin{bmatrix} p_0(t+\Delta t) \\ p_1(t+\Delta t) \\ p_2(t+\Delta t) \end{bmatrix} = \begin{bmatrix} 1-4\lambda\Delta t & 2\mu\Delta t & 4\mu\Delta t \\ 4\lambda\Delta t & 1-2\lambda\Delta t-2\mu\Delta t & 0 \\ 0 & 2\lambda\Delta t & 1-4\mu\Delta t \end{bmatrix} \begin{bmatrix} p_0(t) \\ p_1(t) \\ p_2(t) \end{bmatrix}. \quad (4.49)$$

For this 2*2oo2 system, the availability $A(t) = p_0(t) + p_1(t)$.

The differential equations describing the model of Figure 4-11 are:

$$\frac{dp_0(t)}{dt} = -4\lambda p_0(t) + 2\mu p_1(t) + 4\mu p_2(t). \quad (4.50)$$

$$\frac{dp_1(t)}{dt} = 4\lambda p_0(t) - (2\lambda + 2\mu)p_1(t). \quad (4.51)$$

$$\frac{dp_2(t)}{dt} = 2\lambda p_1(t) - 4\mu p_2(t). \quad (4.52)$$

The operational states of this subsystem are state 0 and state 1.

As the time approaches infinity, the probability of being in the operational state approaches a steady-state value is given by:

$$p_0(\infty) + p_1(\infty) = \frac{\lambda\mu + \mu^2}{\lambda^2 + 3\lambda\mu + \mu^2} + \frac{2\lambda\mu}{3\lambda^2 + 5\lambda\mu + \mu^2} = \frac{3\lambda\mu + \mu^2}{\lambda^2 + 3\lambda\mu + \mu^2}. \quad (4.53)$$

The steady-state availability of the 2oo3 system is given by:

$$A_{2*2OO2} = p_0(\infty) + p_1(\infty) = \frac{\mu(3\lambda + \mu)}{\lambda^2 + 3\lambda\mu + \mu^2}. \quad (4.54)$$

4.4 Reliability and availability modeling of interlocking subsystems

From the structure of the interlocking subsystem (Figure 3-9), it is clear that CBI, Axle counter, rail signal and switch are the measure part of the interlocking system of AA-LRT. Hence this study considered these four subsystems of the interlocking system to analyze their reliability and availability parameters.

4.4.1 Data collection

This thesis deals with the reliability and availability analysis of AA-LRT interlocking subsystems using a reliability block diagram (RBD) and the Markov model. The failure data of one year of signaling and interlocking system of AA-LRT is collected for this study.

To understand the following calculations, we take some kinds of a timeline. This timeline has two possible states i.e. the time between failure (TBF) and time to repair (TTR) and from these two states, we have got MTBF, failure and repair rate.

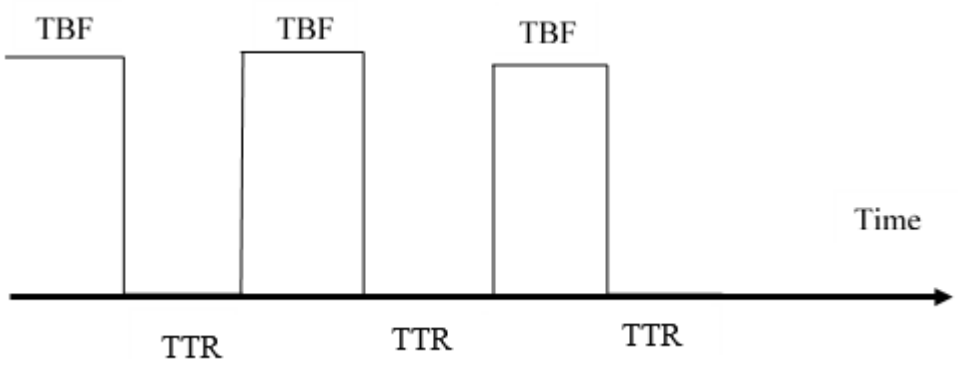

Figure 4-12: Time between failure and time to repair

Therefore MTBF is the average of the individual TBF and MTTR is also the average of the individual TTR.

Axle counter

Total TTR = 11.167h, number of failures that affects the system = 37.

The total timeline is one year

Total time = (1 * 365) days = 365 days = (365 * 24) h = 8760h.

Total uptime is equal to the total time the machine should be operational minus the amount of time taken up by time to repair.

$$\text{Total up time} = \text{Total TBF} = 8760\text{h} - 11.167\text{h} = 8748.833\text{h}.$$

$$\text{MTBF} = \frac{\text{total TBF}}{(\text{number of failures} + 1)} = \frac{8748.833}{38} = 230.232\text{h}.$$

$$\lambda = \frac{1}{\text{MTBF}} = \frac{1}{230.232} = 4.343 \text{ x } 10^{-3}\text{h}^{-1}.$$

$$\text{MTTR} = \frac{\text{total TTR}}{\text{number of failures}} = \frac{11.167}{37} = 0.302\text{h}.$$

$$\mu = \frac{1}{\text{MTTR}} = \frac{1}{0.302} = 3.311\text{h}^{-1}.$$

CBI

Total TTR = 0.354h, number of failures that affects the system = 1.

Total up time = Total TBF = Total time - Total TTR = 8760 – 0.354 = 8759.646h.

$$\text{MTBF} = \frac{\text{total TBF}}{(\text{number of failures} + 1)} = \frac{8759.646}{2} = 4379.823\text{h}.$$

$$\lambda = \frac{1}{\text{MTBF}} = \frac{1}{4379.823} = 2.283 \text{ x } 10^{-4}\text{h}^{-1}.$$

$$\text{MTTR} = \frac{\text{total TTR}}{\text{number of failures}} = \frac{0.354}{1} = 0.354\text{h}.$$

$$\mu = \frac{1}{\text{MTTR}} = \frac{1}{0.354} = 2.825\text{h}^{-1}.$$

Switch machine

Total TTR = 2.667h, number of failures that affects the system = 2.

Total up time = Total TBF = Total time - Total TTR = 8760 – 2.667 = 8757.333h.

$$\text{MTBF} = \frac{\text{total TBF}}{(\text{number of failures} + 1)} = \frac{8757.433}{3} = 2919.111\text{h}.$$

$$\lambda = \frac{1}{\text{MTBF}} = \frac{1}{2919.111} = 3.42 \text{ x } 10^{-4}\text{h}^{-1}.$$

$$\text{MTTR} = \frac{\text{total TTR}}{\text{number of failures}} = \frac{2.667}{2} = 1.3335\text{h}.$$

$$\mu = \frac{1}{\text{MTTR}} = \frac{1}{1.3335} = 0.750\text{h}^{-1}.$$

Rail signal

Total TTR = 0.8667h, number of failures that affects the system = 12.

Total up time = Total TBF = Total time - Total TTR = 8760 – 0.8667 = 8759.133h.

$$\text{MTBF} = \frac{\text{total TBF}}{(\text{number of failures} + 1)} = \frac{8759.133}{13} = 673.779\text{h}.$$

$$\lambda = \frac{1}{\text{MTBF}} = \frac{1}{673.799} = 1.484 \text{ x } 10^{-3}\text{h}^{-1}.$$

$$\text{MTTR} = \frac{\text{total TTR}}{\text{number of failures}} = \frac{0.8667}{12} = 0.072\text{h}.$$

$$\mu = \frac{1}{\text{MTTR}} = \frac{1}{0.072} = 13.89\text{h}^{-1}.$$

4.4.2 Interlocking subsystem reliability block diagram

Figure 4-13 shows the Reliability Block Diagram (RBD) for the minimum operative section for the interlocking system in a railway network. Therefore, the simplified reliability block diagram of AA-LRT interlocking subsystems using only four main subsystems are selected for this thesis.

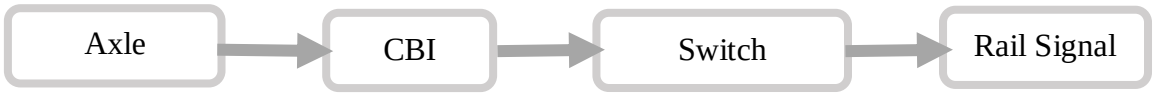

Figure 4-13: RBD of an interlocking subsystem

Track circuits (axle counters) provide input to interlocking systems. Interlocking systems receive information, process it, and make new restrictions on system components. The operation procedure conforms to the operation specification, the selected route is in the free-state, the filament of the signal at the beginning of the route is intact, all the track sections with lateral protection requirements for the route are in free-state, and there is no track segment occupied in the route. If the route check conditions are satisfied, the interlocking device begins to switch the switch, lock the switch, and then open the signal. If the route check conditions are not true, or if the switch position is not detected at the specified point, an invalid command is sent back to the control center to stop the establishment of the route.

4.4.3 Markov model architecture, state transition and mathematical analysis of Markov model

Markov model is a widely used method to perform reliability analysis of several engineering systems including railways. Generally, it is used to model repairable systems with constant failure and repair rates. Markov models can be defined as continuous and discrete-time. For a given system, a Markov model consists of a set of all possible states, transitions between those states, and the conditions described for the transitions. Conditions of the transitions are generally consisting of failures and repairs in reliability analysis. The state-space diagram for the Markov process visualized in Figure 4-14 shows the different states of the system and the possible transitions between them.

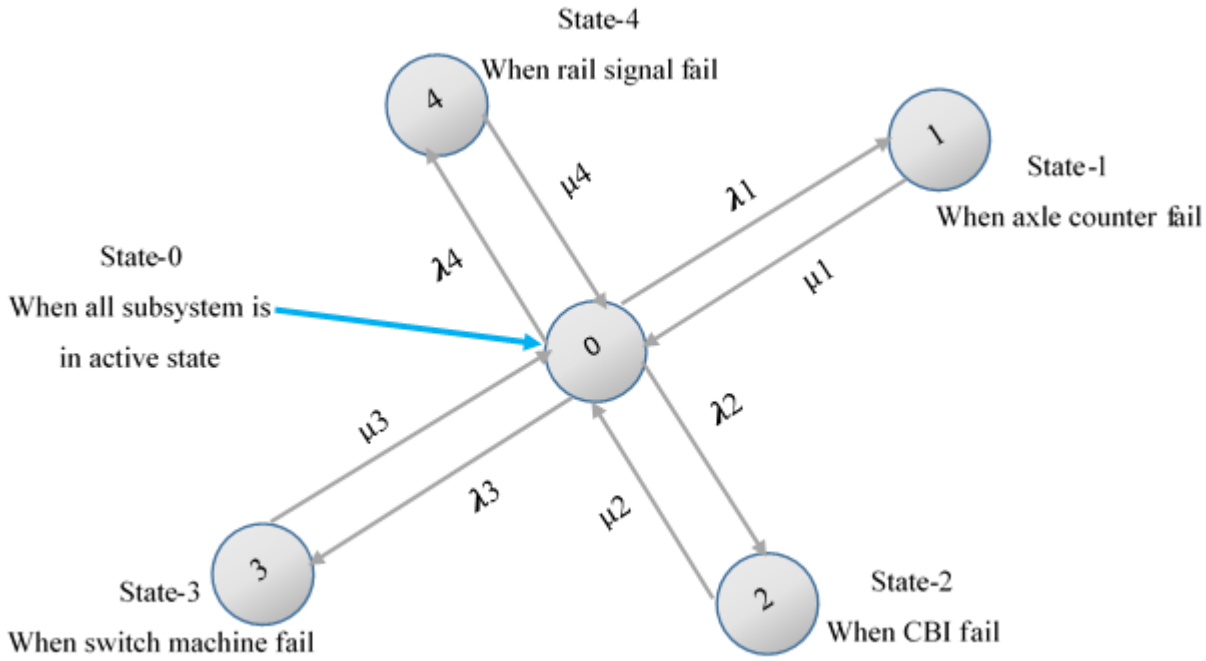

Figure 4-14: Markov diagram for interlocking subsystems

4.4.4 Model description

Many mathematical models can be used to perform reliability-related analysis in various railways signaling system. The transition diagram describes the signaling system model for analyzing the reliability of the railway signaling system. The model assumes that it represents the process of interlocking subsystem function and the alternation between the following five states:

0 – System is active (operating) state at the moment of time t

1 – Axle counter fail — λ_1 – The failure rate of axle counter

2 – CBI fail — λ_2 – The failure rate of CBI

3 – Switch machine fail — λ_3 – The failure rate of switch machine

4 – Rail signal fail — λ_4 – The failure rate of rail signal

The stochastic transitional probability matrix (P) shows the probability of going from one state to another (the probability of going from state i to state j is equal to $p_{i,j}$). The transition probabilities p_{ij} of a homogeneous Markov process form an n x n matrix called a transition matrix which is:

$$[p_{ij}] = \begin{bmatrix} p_{11} & p_{12} & \dots & p_{1j} & \cdots & p_{1n} \\ p_{21} & p_{22} & \dots & p_{2j} & \cdots & p_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ p_{i1} & p_{i2} & \dots & p_{ij} & \cdots & p_{in} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ p_{n1} & p_{n2} & \cdots & p_{nj} & \cdots & p_{nn} \end{bmatrix}. \quad (4.55)$$

The probability that the system is in the operating state after time interval Δt i.e. at time (t + Δt) is given by:

$p_0(t + dt)$ = [(Probability of being in operating state at time t) and (Probability of not failing between t and t + dt)] + [(Probability of being failed states at time t) and (Probability of being repaired between t and t + dt)].

Probabilities of failure between t and dt are $\lambda_i dt$.

Probabilities of not failing between t and dt are $(1 - \lambda_i dt)$.

Probabilities of repair between t and dt are $\mu_i dt$.

Transitions from state j to the same state j within time interval dt can be

$$p(s_j \to s_k) = p_{jj} = 1 - \sum_{k=0}^{n} p_{jk}\, dt = 1 - \lambda_{jj} dt, \quad (4.56)$$

where j = 0, 1, 2 … n; k = 0, 1, 2 …n; $j \neq k$

Using the addition and multiplication rule for probabilities gives:

$$p_0(t + dt) = p_0(t)[1 - (\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4)dt] + p_1(t)\mu_1 dt + p_2(t)\mu_2 dt + p_3(t)\mu_3 dt + p_4(t)\mu_4 dt$$

$$p_0(t + dt) = p_0(t) - p_0(t)(\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4)dt + p_1(t)\mu_1 dt + p_2(t)\mu_2 dt + p_3(t)\mu_3 dt + p_4(t)\mu_4 dt$$

And this is equal to

$$p_0(t + dt) - p_0(t) = -(\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4)dtp_0(t) + \mu_1 dtp_1(t) + \mu_2 dtp_2(t) + \mu_3 dtp_3(t) + \mu_4 dtp_4(t)$$

Rearranging (divide by dt on both sides)

$$\frac{p_0(t+dt)-p_0(t)}{dt} = -(\lambda_1+\lambda_2+\lambda_3+\lambda_4)p_0(t)+\mu_1 p_1(t)+\mu_2 p_2(t)+\mu_3 p_3(t)+\mu_4 p_4(t)$$

Taking the limit as dt approached zero ($dt \to 0$), we obtain the following differential equations.

$$\frac{dp_0(t)}{dt} = -(\lambda_1+\lambda_2+\lambda_3+\lambda_4)p_0(t)+\mu_1 p_1(t)+\mu_2 p_2(t)+\mu_3 p_3(t)+\mu_4 p_4(t)$$

$$\frac{dp_0(t)}{dt} = \sum \mu_i p_i(t) - p_0(t)\sum \lambda_i. \quad (4.57)$$

Similarly for other states will be

$$\frac{dp_1(t)}{dt} = \lambda_1 p_0(t) - \mu_1 p_1(t). \quad (4.58)$$

$$\frac{dp_2(t)}{dt} = \lambda_2 p_0(t) - \mu_2 p_2(t). \quad (4.59)$$

$$\frac{dp_3(t)}{dt} = \lambda_3 p_0(t) - \mu_3 p_3(t). \quad (4.60)$$

$$\frac{dp_4(t)}{dt} = \lambda_4 p_0(t) - \mu_4 p_4(t). \quad (4.61)$$

The transition rates can be expressed in form of a transition matrix as follows:

$$\begin{bmatrix} \frac{dp_0(t)}{dt} \\ \frac{dp_1(t)}{dt} \\ \frac{dp_2(t)}{dt} \\ \frac{dp_3(t)}{dt} \\ \frac{dp_4(t)}{dt} \end{bmatrix} = \begin{bmatrix} -(\lambda_1+\lambda_2+\lambda_3+\lambda_4) & \mu_1 & \mu_2 & \mu_3 & \mu_4 \\ \lambda_1 & -\mu_1 & 0 & 0 & 0 \\ \lambda_2 & 0 & -\mu_2 & 0 & 0 \\ \lambda_3 & 0 & 0 & -\mu_3 & 0 \\ \lambda_4 & 0 & 0 & 0 & -\mu_4 \end{bmatrix} \begin{bmatrix} p_0(t) \\ p_1(t) \\ p_2(t) \\ p_3(t) \\ p_4(t) \end{bmatrix}$$

Equating first order derivative to zero for a steady state ($t \to \infty$)

$$-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)p_0+\mu_1 p_1+\mu_2 p_2+\mu_3 p_3+\mu_4 p_4 = 0$$
$$\lambda_1 p_0 - \mu_1 p_1 = 0$$
$$\lambda_2 p_0 - \mu_2 p_2 = 0$$
$$\lambda_3 p_0 - \mu_3 p_3 = 0$$
$$\lambda_4 p_0 - \mu_4 p_4 = 0$$

Solving for p_0, p_1, p_2, p_3, p_4, the steady-state probabilities are the following:

$$p_0 = \frac{\mu_1 p_1+\mu_2 p_2+\mu_3 p_3+\mu_4 p_4}{\lambda_1+\lambda_2+\lambda_3+\lambda_4}. \quad (4.62)$$

$$p_1 = \frac{\lambda_1}{\mu_1} p_0. \tag{4.63}$$

$$p_2 = \frac{\lambda_2}{\mu_2} p_{0.} \tag{4.64}$$

$$p_3 = \frac{\lambda_3}{\mu_3} p_0. \tag{4.65}$$

$$p_4 = \frac{\lambda_4}{\mu_4} p_0. \tag{4.66}$$

The sum of all probabilities is equal to one.

$$p_0 + p_1 + p_2 + p_3 + p_4 = 1. \tag{4.67}$$

Substituting the value of p_1, p_2, p_3 and p_4 in equation (4.67)

$$p_0 + \frac{\lambda_1}{\mu_1} p_0 + \frac{\lambda_2}{\mu_2} p_0 + \frac{\lambda_3}{\mu_3} p_0 + \frac{\lambda_4}{\mu_4} p_0 = 1$$

Taking p_0 as common

$$p_0 \left[1 + \frac{\lambda_1}{\mu_1} + \frac{\lambda_2}{\mu_2} + \frac{\lambda_3}{\mu_3} + \frac{\lambda_4}{\mu_4}\right] = 1 = p_0 \left[1 + \sum \frac{\lambda_i}{\mu_i}\right]$$

Solving for p_0:

$$p_0 = \frac{1}{1+\sum \frac{\lambda_i}{\mu_i}}. \tag{4.68}$$

Substituting equation (4.68) into equation (4.63) to (4.66) and solving for p_1, p_2, p_3 and p_4:

$$p_1 = \frac{\lambda_1}{\mu_1 (1 + \sum \frac{\lambda_i}{\mu_i})}, \tag{4.69}$$

$$p_2 = \frac{\lambda_2}{\mu_2 \left(1 + \sum \frac{\lambda_i}{\mu_i}\right)}, \tag{4.70}$$

$$p_3 = \frac{\lambda_3}{\mu_3 \left(1 + \sum \frac{\lambda_i}{\mu_i}\right)}, \tag{4.71}$$

$$p_4 = \frac{\lambda_4}{\mu_4 (1 + \sum \frac{\lambda_i}{\mu_i})}, \tag{4.72}$$

where (i = 1, 2, 3, 4)

Hence, the steady-state availability of the interlocking system at $t \to \infty$ is:

$$A = p_0(\infty) = \frac{1}{1+\sum \frac{\lambda_i}{\mu_i}}. \tag{4.73}$$

At time t = 0,

$$p_0(0) = 1, p_1(0) = 0, p_2(0) = 0, p_3(0) = 0, p_4(0) = 0$$

Unavailability of the interlocking system is found as:

$$UA = p_1 + p_2 + p_3 + p_4 \tag{4.74}$$

Substituting the values of p_1, p_2, p_3 and p_4 in to the equation (4.74), we get:

$$UA = \frac{\lambda_1}{\mu_1(1 + \sum \frac{\lambda_i}{\mu_i})} + \frac{\lambda_2}{\mu_2(1 + \sum \frac{\lambda_i}{\mu_i})} + \frac{\lambda_3}{\mu_3(1 + \sum \frac{\lambda_i}{\mu_i})} + \frac{\lambda_4}{\mu_4(1 + \sum \frac{\lambda_i}{\mu_i})}$$

$$UA = \frac{1}{\left(1 + \sum \frac{\lambda_i}{\mu_i}\right)}\left[\frac{\lambda_1}{\mu_1} + \frac{\lambda_2}{\mu_2} + \frac{\lambda_3}{\mu_3} + \frac{\lambda_4}{\mu_4}\right]. \tag{4.75}$$

The reliability of the different components are:

$$R_1(t) = e^{-\lambda_1 t}, R_2(t) = e^{-\lambda_2 t}, R_3(t) = e^{-\lambda_3 t} \text{ and } R_4(t) = e^{-\lambda_4 t},$$

where R1, R2, R3 and R4 are the reliability of Axle counter, CBI, switch machine and rail signal respectively.

As these subsystems are connected in series, so the reliability of the interlocking system will be the product of the individual subsystem reliabilities.

$$R(t) = \prod R_i = R_1 R_2 R_3 R_4 = e^{-\lambda_1 t} e^{-\lambda_2 t} e^{-\lambda_3 t} e^{-\lambda_4 t} = e^{-\sum \lambda_i t}. \tag{4.76}$$

CHAPTER 5 RESULTS AND DISCUSSIONS

5.1 Interlocking system controller architectures results and discussions

This thesis presents the quantification of reliability, availability and safety parameters of railway interlocking control architectures using reliability block diagram (RBD) and Markov analysis method. Reliability, availability and safety parameters versus time curves of 1-out-of-1 system, 2-out-of-2 system, 2-out-of-3 system and double 2-out-of-2 system are drawn in the same figure as a contrast.

Table 5-1 presents the results for the study based on the input parameters. The designed values of AA-LRT signaling system failure and repair rate ($10^{-6}h^{-1}$and $2h^{-1}$respectively) are taken to calculate the reliability, availability and safety of interlocking control architectures.

$$\lambda = 10^{-6}h^{-1}$$
$$\mu = 2h^{-1}$$
$$t = 1\ year = 8760h$$

Table 5-1: Reliability, availability, safety, MTTF and Q_D values for different interlocking control architectures with input λ, μ and t

Parameters	Interlocking control architectures			
	1oo1	**2oo2**	**2oo3**	**2*2oo2**
R	0.9912	0.9824	0.9997	0.9996
$A_{(\infty)}$	0.9999995	0.9999990	0.9999999999992	0.9999999999997
S	0.9912	0.9999	0.9999993	0.999999993
MTTF(10^5h)	10.000	5.000	8.333	12.500
Q_D	0.0088	0.0001	0.000000681	0.000000006

5.1.1 Reliability

As shown in Figure 5-1, 2oo3 control architecture has the highest reliability and double 2-out-of-2 has the next highest reliability. Two-out-of-three redundancy control architecture enables a system to continue operating in the event of one processor failure from the three processors. In 2oo3 architecture, all three processors are interconnected and the system can operate if any of two processors from three are in an operable state. Whereas in double 2oo2 architecture, from the total of four control processors, two are connected in series I (Figure 4-10) and the other two are in series II, the system can be operable if and only if

two processors within the same series are in an operable state. This shows that 2oo3 architecture has the probability to be more reliable than double 2oo2 architecture.

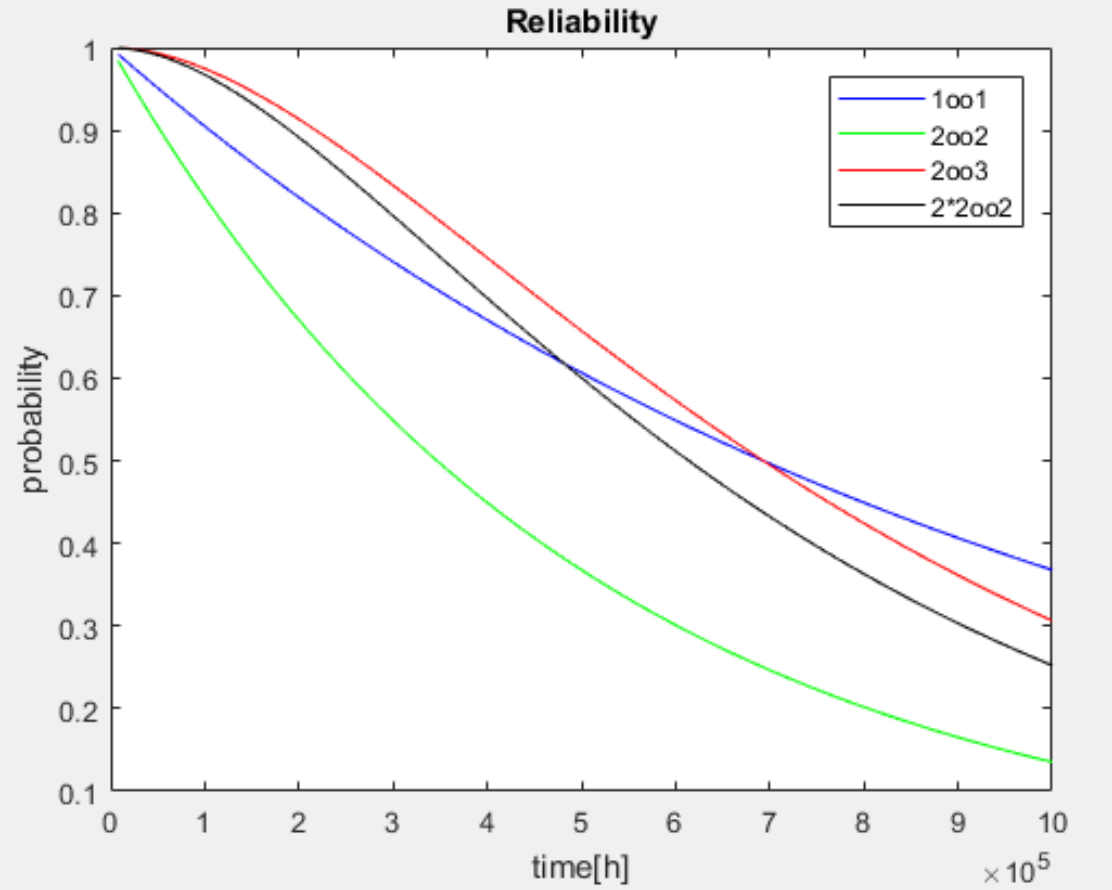

Figure 5-1: Reliability of each system architecture against time

As shown in Figure 5-1, the reliability performances of the 2*2oo2 and 2oo3 are lower than the 1oo1 architecture when time increases. As of a certain time t ($t = 6.93 \times 10^5$h for 2oo3 and $t = 4.81 \times 10^5$h for $2 * 2oo2$), the voting is no longer able to compensate the (for example three times greater for 2oo3) higher amount of processors. In other words, the reliability of the system initially increases at an increasing rate with an increase in the number of processors, but the rate of increase in reliability with each additional component decreases as the number of components increases.

The reliability of the 2oo2 system architecture is lower than the 1oo1 architecture because the 2oo2 control architecture can be operable only when both the outputs of control processors have coincided. When one of the two processors does not operate, the system will enter into a safe state. This architecture gives priority to safety.

When two processors are connected in parallel with the safety comparator circuit, the total reliability of the system is the product of the individual processor reliabilities (equation (4.13)). The reliability of the individual processor is between zero and one, the product is less than the reliabilities of individual processors. This is the reason why 1oo1 architecture is better reliability than 2oo2 architecture.

5.1.2 Availability

The availability of each interlocking architecture can be calculated based on the designed failure and repair data of the system (Table 5-2).

Table 5-2: Availability of each interlocking architecture

Redundancy architectures	Failure rate/hour (λ)	Repair rate/hour(μ)	Availability (A)
1oo1(Simple system)	10^{-6}	2	0.99999950000024
2oo2 (2-out-of-2)	10^{-6}	2	0.99999900000099
2oo3 (2-out-of-3)	10^{-6}	2	0.99999999999925
2*2oo2 (Double 2-out-of-2)	10^{-6}	2	0.99999999999975

The availability of a double 2oo2 control system is the highest among four redundancy architectures (Figure 5-2). This is because one part of the redundant 2oo2 system is in active mode and the other works in hot standby mode. The standby service is already running. It notices immediately when the active service fails and takes over. The active and the standby service are in constant communication; the standby receives updates from the active every time a significant event occurs. In hot standby mode, the standby is available almost immediately to take over – the ultimate reduction in mean time to repair (hot standby system has fast reconfiguration time) and this increases the availability of the system.

As shown in Figure 5-2, the availability of 1oo1 architecture is better than 2oo2 architecture. This is because, as the number of control processors connected with the safety comparator circuit increase, the probability of failures also increases and this drops the availability of the system. It can be observed that the reliability and availability of a safety comparator circuit-connected network of processors are lower than the specifications of individual processors.

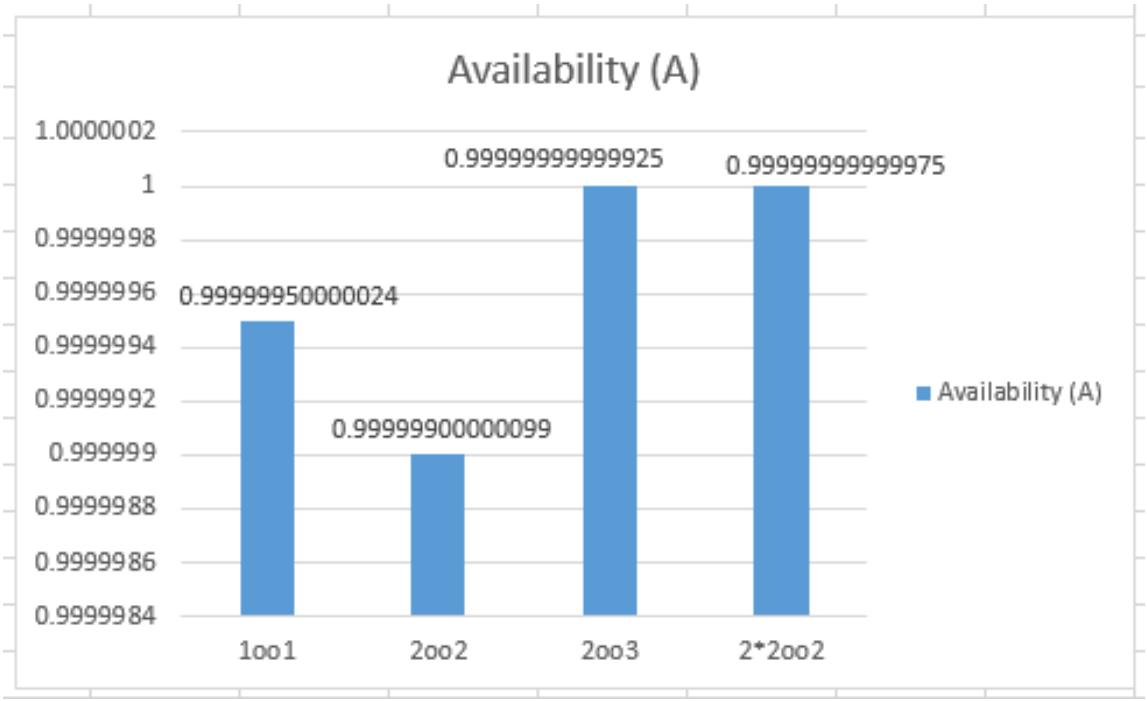

Figure 5-2: Availability pattern of each architecture

5.1.3 Safety

Safety is the probability of a system's state where there is no dangerous failure. The double 2-out-of-2 system has the highest safety in Figure 5-3, and the 1-out-of-1 system has the lowest. The double 2-out-of-2 system always supervises each sub-system by detection logic. If any module of the two sub-systems detects a fault, the faulty module is repaired without system power down. A single-structure control system costs the least but any errors cause the system to shut down. Systems with redundant structures that are more complex than single structures have proved to be very safe.

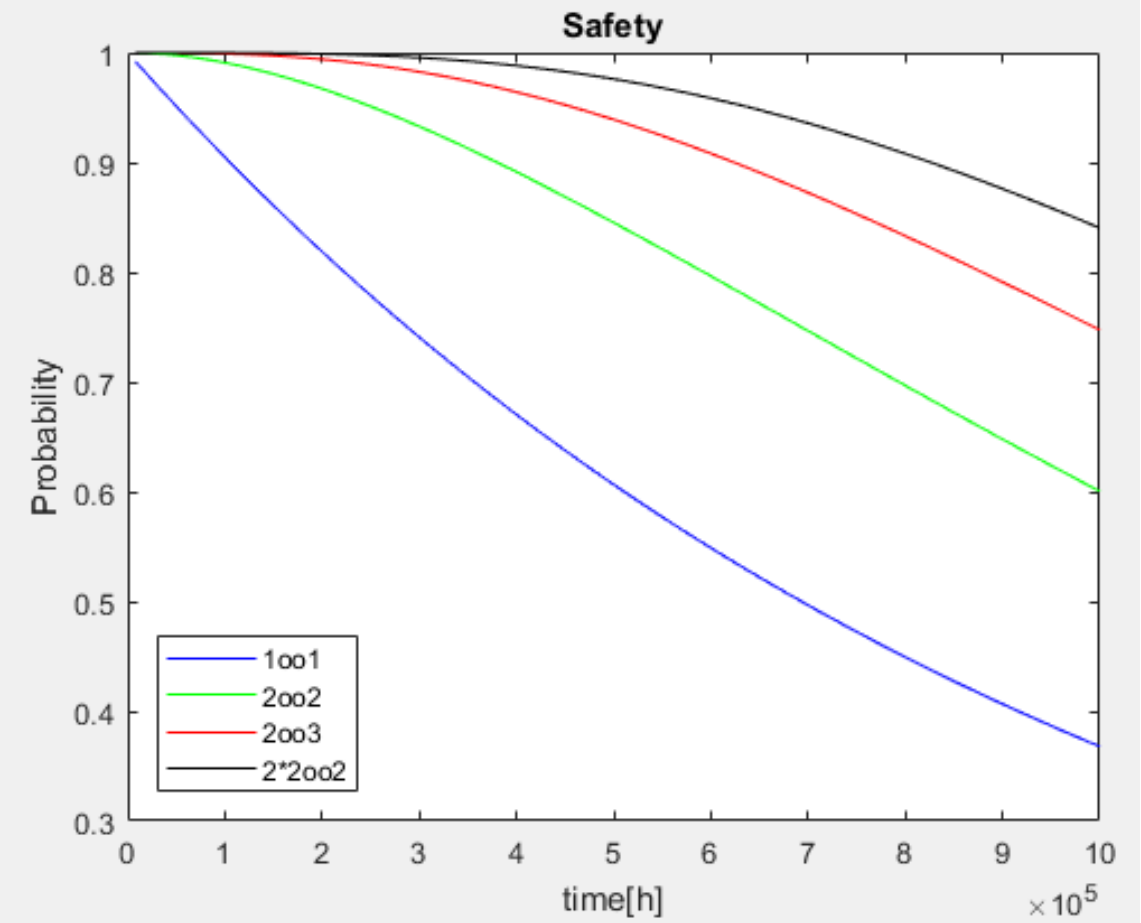

Figure 5-3: Safety of each system architecture against time

With regard to the combined aspects, the double 2-out-of-2 architecture (current architecture of AA-LRT control system) is the best redundancy architecture. The good quality for the system is easily achieved by hot standby redundancy even when faults occur. The active and standby control subsystems are powered on. Both the subsystems take input, process it, communicate with each other and finally give one output. If any one of the two subsystems fails/disabled, there is no interruption in the output. The process is continued by the standby subsystem without any time delay.

5.2 Interlocking subsystems results and discussions

Failure and repair data of the subsystems of the interlocking system for this study are obtained from the Signaling System Detailed Design of AA-LRT Part I Technical Specification, interview and site assessment. The failure data of one year of the interlocking equipment of one interlocking area (EW 16) is taken for this study. With the help of these data, the reliability and availability of four main subsystems (axle counter,

CBI, switch machine and rail signal) and the entire interlocking system are calculated using the reliability block diagram (RBD) and Markov process. The graphs for reliability and availability versus time are also plotted.

5.2.1 Reliability

As shown in Figure 5-4, the reliability of the axle counter, CBI, switch machine and rail signal are 0.1059, 0.8922, 0.8428 and 0.4771 respectively after 500 hours of operation. CBI has the highest reliability and the axle counter has the lowest. Reliability is failure-free working probability and directly proportional to the number of failure per given time. Frequent failure of axle counters (37 times per year as the data taken from AA-LRT) which affects the normal operation of trains makes it the lowest reliability.

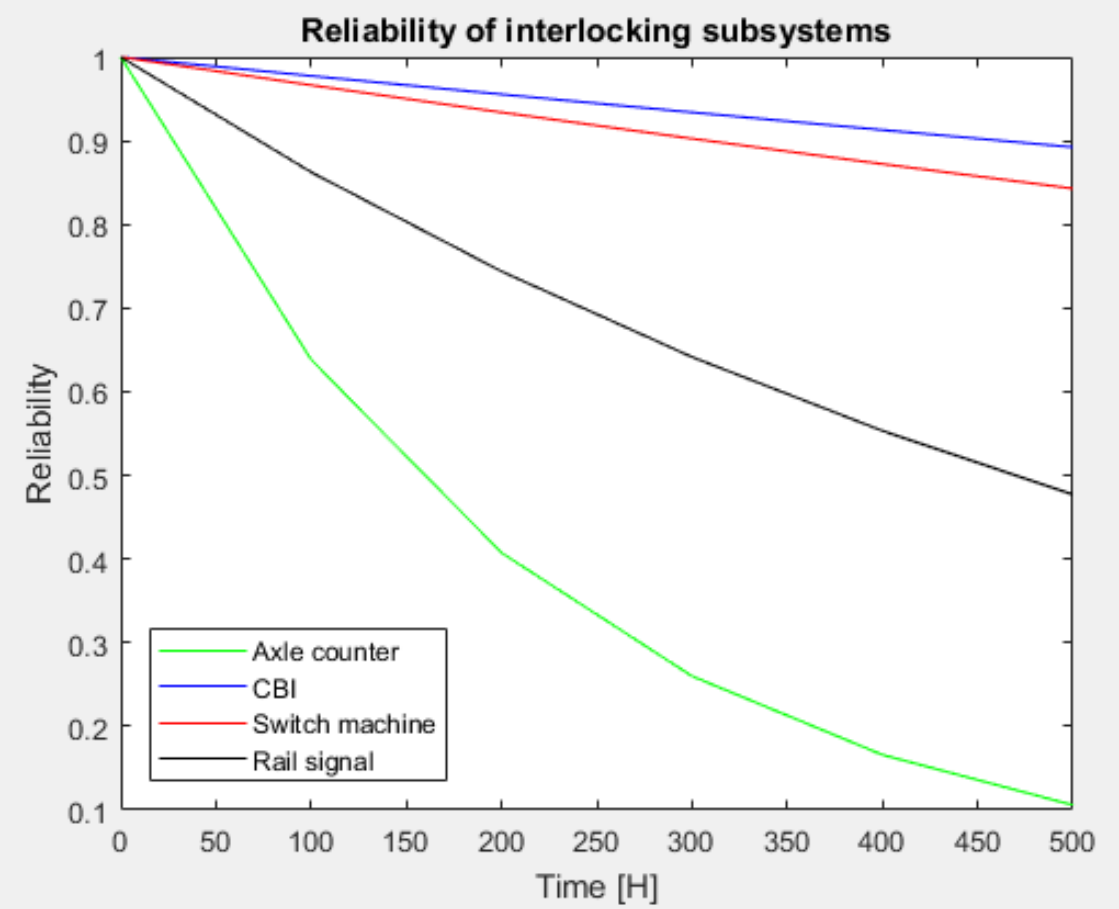

Figure 5-4: Reliability versus time pattern of AA-LRT interlocking subsystems

The reliability of the total interlocking system based on equation (4.73) is calculated as:

$$R_{(t)} = e^{-\Sigma\lambda_i t} = e^{-0.006391t}$$

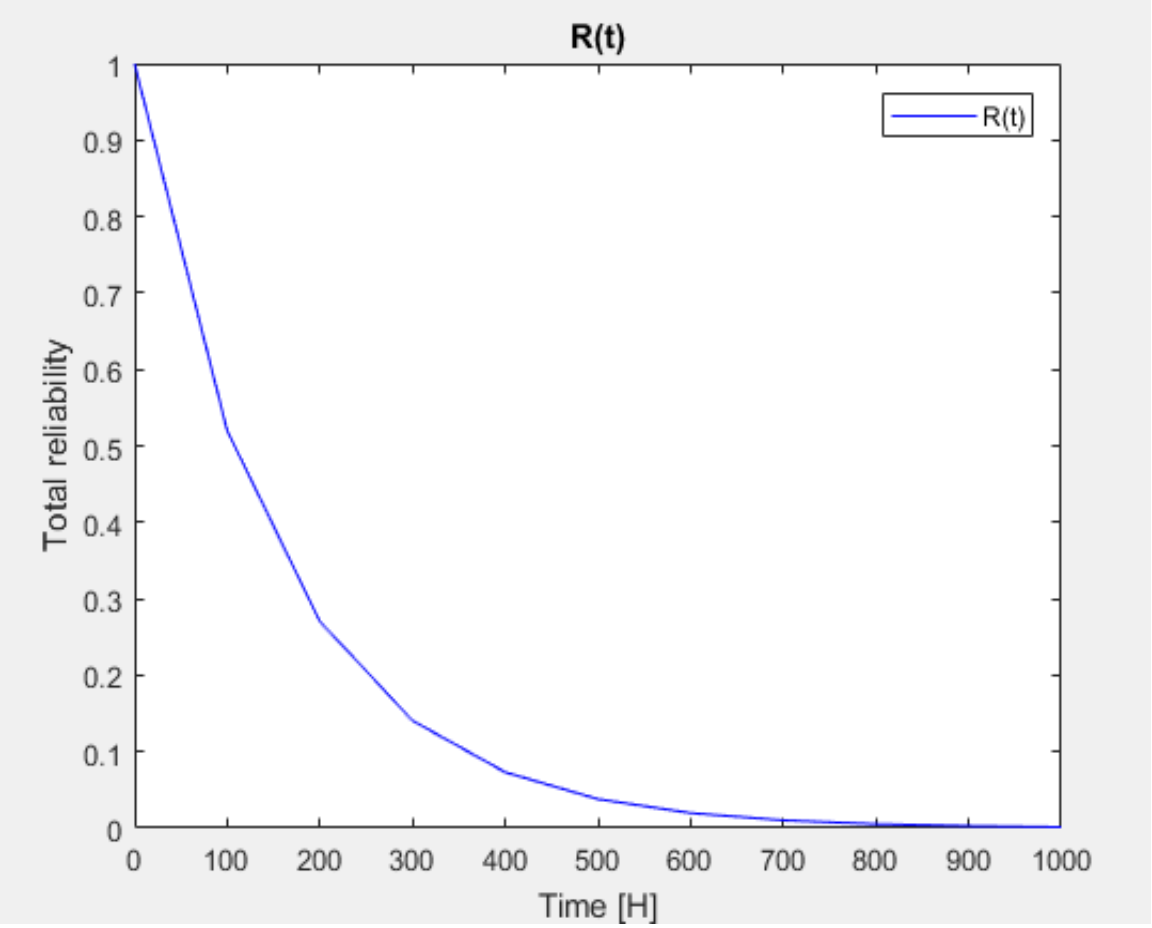

Figure 5-5: Reliability pattern of the total interlocking system

It is found that the reliability of the total interlocking system after 100 hours of operation is 52.00 %; in 400 hours of operation is 7.31 % and in 1000 hours of operation drops down to 0.14%. Then compare the result obtained from the analysis with the quantitative data taken from the signaling system design.

Table 5-3: Reliability values gained from signaling system design and the analysis

RAMS parameter	Quantitative data taken from the signaling system design	The result gained from the analysis
Reliability	MTBF≥2.0×10^5h	MTBF=156.470h

The reliability result gained from the analysis has a large variation from the quantitative data taken from the signaling system design because of the following reasons:

- This study considers only one sample interlocking area (EW16) for calculation but the design value of reliability is for all eight interlocking areas of AA-LRT.
- Only one-year failure data is taken for this study.

- Human factors (the time spent to repair failed subsystems and put the components back into operation), software and the environment that influence the total reliability of the system are not considered in this study.
- Interlocking area EW16 is common for both EW and NS line, many failures occur in this area and the result may affect the calculated value of total reliability.

It is proved that the reliability of one single subsystem can affect the total interlocking system as well as the whole railway system. This means that the failure of a single subsystem can stop the whole railway system. To improve the overall system of operation, the reliability of those subsystems require strengthening preventive and scheduled maintenance, which can result in decreasing their failure rate or increasing their time to failure (TTF).

The reliability of the interlocking system can be improved in the following ways:

- Select reliable equipment with low failure rates.
- Design with appropriate redundancy.
- Improve maintenance techniques (for example, by using better test equipment and/ or early replacement of limited-life components).

5.2.2 Availability

The availability of each subsystem can be calculated based on the given failure and repair rate of the subsystem (Table 5-4).

$$A = \frac{\mu}{\lambda + \mu}$$

Table 5-4: Availability of different interlocking subsystems

Components	Failure rate/hour (λ)	Repair rate/hour(μ)	Availability (A)
Axel counter	0.00434	3.311	0.9986
CBI	0.000228	2.825	0.9999
Switch machine	0.000342	0.750	0.9995
Rail signal	0.00148	13.89	0.9998

The CBI subsystem has the highest availability among the four subsystems (Figure 5-6). Availability of axle counter and switch machine are the lowest. If a failure occurred on a switch machine, it takes time to repair (average TTR = 1.33h per failure) and makes it lower availability next to the axle counter.

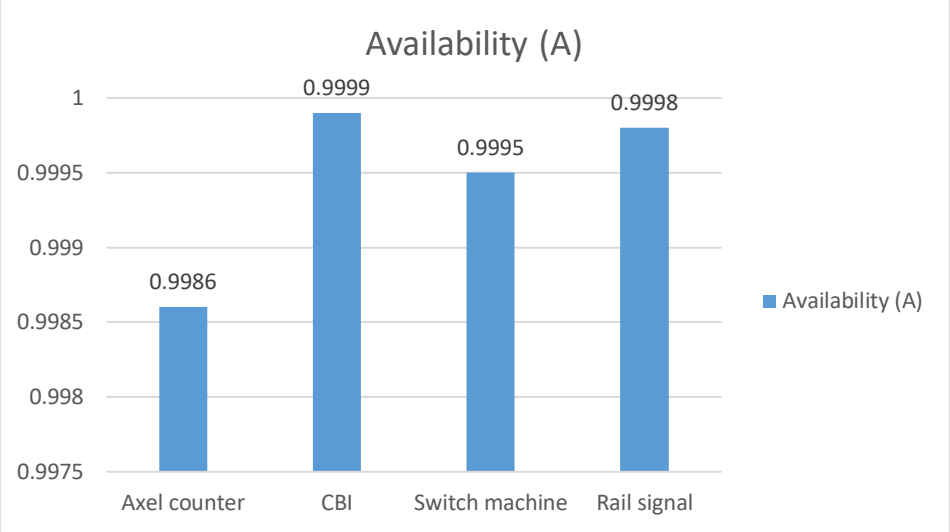

Figure 5-6: Availability pattern of each subsystem

The availability of the total interlocking system is calculated based on the formulas gained from Markov analysis (equation (4.73)).

$$A = p_0(\infty) = \frac{1}{(1 + \sum \frac{\lambda_i}{\mu_i})},$$

$$A = 0.99805 = 99.805\%.$$

Table 5-5: Availability values gained from signaling system design and the analysis

RAMS parameter	Quantitative data taken from the signaling system design	The result gained from the analysis
Availability	≥ 99.99%.	99.805%

Table 5-5 shows the results that has gained from the analysis and the quantitative data taken from the signaling system design. The results are almost similar. Availability is the ability of a product to be in a state to perform a required function under given conditions at a given instant of time. If failures occur on interlocking equipment repeatedly but repairs within a short period of time, the availability of the total interlocking system may not be affected that much. For example, axle counters fail repeatedly but usually repairs within less than 20 seconds.

The results show the reliability and availability of axle counter are the lowest, and 92.15% of failures are axle counters failure and this affects the normal operation of both EW and NS railway lines.

The reasons for axle counter failures are:

- Power failure: Axle counters forget how many axles are in a section. Therefore, a manual override is necessary to reset the system. This hand-operated override introduces the human element which may be unreliable.

- The number of trains that pass over the axle counter: Currently 39 trains are working in AA-LRT. If the number of trains moves on the axle counter increases, the probability of axle counter failure increases. This is observed on the axle counter which is installed on the common track of AA-LRT. For example EW16 interlocking area.

- Failure frequency on the interlocking device: frequent maintenance degrades device performance.

- Turnouts: Where there are interlocked turnouts, an axle counter unit needs to be provided for each leg of that turnout. On lines with non-interlocked/hand-operated switches, detection of the switch points would have to be monitored separately. This case is expected in the EW16 interlocking area.

- Installation: One method of mounting an axle counter sensor is to drill through the rail and this has the disadvantage of weakening the structure of the rail.

- Siding and shunting movements: axle counters have problems maintaining correct counts when train wheels stop directly on the counter mechanism. This occurs at stations or other areas where cars are shunted, joined and divided. This also happens when a wheel has entered a track section but rolled back. Where main lines have switches to siding, extra counters will need to be deployed to detect trains entering or exiting the line.

Another frequently failed component that is occurred in AA-LRT is LED failure. According to the data analysis, 12 LED failures occur in EW 16 interlocking area. The common reasons are a power cut and blown fuse in the circuit. Replacing ageing cables in areas that don't have Uninterruptible Power Supply (UPS), and continuously monitor the health of interlocking equipment reduces LED signal failures.

Another failed system that occurred in AA-LRT is switch machine failure which takes time to repair. The causes of failure are switch mechanical failure (stuck at a position or slowness of shifting) or switch motor problems, clogged with debris, or they might expand too much in hot weather.

CHAPTER 6 CONCLUSIONS AND RECOMMENDATIONS

6.1 Conclusion

Most failures in railway interlocking system can cause loss of human life, huge environmental damages, or economic penalties. From operation index and failure statistical data of AA-LRT, 47.5% of failures are interlocking system failure. Therefore, the key feature of an interlocking system should assure the reliability, availability and safety of railway transportation. In modern railway systems, the interlocking control systems are designed with specific development methods and concerning hardware redundancy. Hardware redundancy prevents the dangerous consequences of failure in the hardware of the interlocking control unit.

This thesis identified that the current interlocking control architecture of AA-LRT has the best characteristics in reliability, availability and safety compared to the 2-out-of-2 and 2-out-of-3 systems where a 1oo1 system is used as a baseline. This is because one part of the redundant 2oo2 system is in active mode another works in standby mode. If a failure occurs in the active one, the process is continued by the standby subsystem. The reliability, availability and safety of double 2-out-of-2 architecture is 99.96%, 99.99999999997% and 99.9999993% respectively. The analysis is based on component hardware redundancy technique and calculated both with RBD and Markov process approach. The study makes to assure the current interlocking control system of AA-LRT is designed with the best hardware redundancy technique.

This study also analyzes the reliability and availability of four components of the interlocking system of AA-LRT based on the failure data by using Markov analysis model. These are Axle counter, CBI, switch machine and rail signal. The analysis shows that 92.15% of AA-LRT interlocking system failure is axle counter failure. Stable power supply and swift wheel sensor maintenance can improve axle counter failures.

6.2 Recommendation

Recommendations of this work are described as follows:

- This thesis analyzes the reliability, availability and safety of the hardware redundancy of interlocking control system. Further analysis should be done by considering software, time and information redundancy of the control system.

- The models developed for calculating the failure and repair rate is taken by considering the data of EW 16 interlocking area. Modeling should be done by considering failure and repair data of the total (eight) interlocking areas to get accurate results for AA-LRT interlocking system.

- By considering human factors (the time spent to repair failed subsystems and put the components back into operation), the results can be more accurate in the analysis.

- This study considers one year failure and repair data of AA-LRT. Thus, by using more data, the result may be improved in this thesis.

- Markov process may also apply to other interlocking subsystems (level crossings and other interfaces) and other sections of AA-LRT.

REFERENCES

[1] E. E. King, *Railway Signaling*, 1st ed. New York, NY, USA: McGraw-Hill, 1921.

[2] Y. Negash, "Interlocking Principles and Systems [PowerPoint slides]," lecture notes for REGM-6214 Railway Signaling and Interlocking, Department of Railway Engineering, Railway Signaling and interlocking, Addis Ababa Institute of Technology, 2017.

[3] W. H. Elliott, "Block Signaling: What They Are For; What They Do; How They Do It," in *Block and Interlocking Signals*, New York, NY, USA: Kessinger, 2010, pp. 1–16.

[4] S. Wagner, A. Apollonio, R. Schmidt, M. Zerlauth, and A.Vergara-Fernandez, "Architecture for interlock systems: reliability analysis with regard to safety and availability," in *Proc. 13th Int. Conf. Accelerator and Large Experimental Physics Control Systems (ICALEPCS2011)*, 2011, pp. 1058–1061.

[5] L. Tang, "Reliability assessments of railway signaling systems: A comparison and evaluation of approaches," M. S. thesis, Norwegian Univ., 2015.

[6] M. Mulazzani, "Reliability and Safety in Electronic Interlocking," in *IFAC Control in Transportation Systems*, vol. 13, pp. 321–329, 1986.

[7] B. Pei and Y. Ming, "An Embedded Fail-Safe Interlocking System," *Tandem Nonstop Himalaya K200*, pp. 22–27, 1997.

[8] M. Qamar and E. Zio, Eds, *Handbook of RAMS in Railway Systems*. New York, NY, USA: CRC Press, 2018.

[9] China Railways Group Limited, "Addis Ababa LRT Project East-West and North-South Line Project Study Report," 2009.

[10] Ethiopian Railway Corporation, "Addis Ababa E-W & N-S (Phase 1) LRT Project, Signaling System Detailed Design," Version: ET/AA/LRT/CREC/EPC/DD/XH-01/A, Jun. 2013.

[11] A. P. Patra, "RAMS and LCC in rail track maintenance," Licentiate thesis, Lulea University of Technology, 2007.

[12] Ethiopian Railways Corporation, "Failure data of AA-LRT," Addis Ababa, 2018.

[13] H. Tao and R. Jianxin, "Research of Reliability, Availability and Maintainability on the All-electronic Computer Interlocking System," *J. Electr. Eng.*, vol. 12, no. 8, pp. 5877–5885, Aug. 2014, doi: 10.11591/telkomnika.v12i8.6044.

[14] S. Wollny, "Reliability, Availability, Maintainability, Safety (RAMS) and Life Cycle Costs (LCC)," *Eur. Assoc. Bus. Commer.*, Jul. 2017.

[15] Innovative Track Systems, Guideline for LCC and RAMS analysis, Thematic Priority 6: Sustainable Development, Global Change and Ecosystems, Project No. TIP5-CT-2006-031415, 2006.

[16] *Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process*. I. Standard EN 50126-1, European Committee for Electrotechnical Standardization (CENELEC), 2017.

[17] *Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems, European Committee for Electrotechnical Standardization (CENELEC)*. I. Standard EN 50128, European Committee for Electrotechnical Standardization (CENELEC), 2001.

[18] *Railway Applications - Communication, Signaling and Processing Systems - Safety Related Electronic Systems for Signaling*. I. Standard EN 50129, European Committee for Electrotechnical Standardization (CENELEC), 2018.

[19] A. Birolini, *Reliability Engineering, Theory and Practice*, 5th ed. Verlag Berlin Heidelberg: Springer, 2007.

[20] V. Andras and M. Istvan, "Safety-Critical Systems: Requirements & Architecture," Dept. Meas. and Inf. Syst., Budapest University of Technology and Economics, 2012.

[21] D. P. Siewiorek and R. S. Swarz, *Reliable Computer Systems: Design and evaluation*, 3rd ed. Natick, Massachusetts: A K Peters, 1998.

[22] E. Zio, *An Introduction to the Basics of Reliability and Risk Analysis*, 13th ed. Singapore: World Scientific, 2007.

[23] Exida, "A Summary of the IEC 61508 Standard for Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems," USA, Rep. PA-18960, Jan. 2006.

[24] B. W. Johnson, "An introduction to the design and analysis of fault-tolerant systems," Dept Elect. Eng., Virginia Univ., 2014.

[25] G. Ardavanis, "RAMS Systems Assurance for Railways," pp. 1–13, 2014.

[26] A. K. Pandey, "RAMS management for a complex railway system: a case study," in *2014 Int. Applied Reliability Symp. (ARS)*, Apr. 2014.

[27] J. H. Mize and W. J. Fabrycky, *Systems Engineering and Analysis*, 4th ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 1998.

[28] Z. N. Tatenda, "Application of reliability analysis for performance assessments in railway infrastructure asset management," M. S. thesis, Stellenbosch Univ., 2017.

[29] A. Morant, "Dependability and maintenance analysis of railway signalling systems," Licentiate thesis, Lulea Univ., 2014.

[30] A. Pfeiffer, "Safety and Reliability in Signaling Systems," 1st ed., Leipzig, Germany: Eurail Press, 2009.

[31] W. R. Blischke and D. N. Murthy, *Reliability: Modeling, Prediction and*

Optimization, 1st ed. Hoboken, NJ, USA: Wiley, 2000.

[32] B. A. Keisner, "Reliability Analysis Technique Comparison, as Applied to the Space Shuttle," 2003.

[33] N. B. Fuqua, "The Applicability of Markov Analysis Methods to Reliability, Maintainability, and Safety," vol. 10, no. 2, 2003.

[34] A. Garro and A. Tundis, "Modeling and Simulation for System Reliability Analysis : The RAMSAS Method," 2015.

[35] M. Bellek, "Design and RAMS analysis of railway interlocking systems using formal methods," M. S. thesis, Dept. Elect. Eng., Istanbul Technical Univ., 2013.

[36] J. Wang, "Existing technology of train safety control," in *Safety Theory and Control Technology of High-Speed Train Operation*, New York, NY, USA: Elsevier, 2018, pp. 33–77.

[37] J. Mocki, "Railway interlocking process: a formal method for documenting and evaluating railway junction signalling and interlocking," PhD dissertation, Griffith Univ., Queensland, Australia, 2015.

[38] K. Nathoo, "Establish a generic railway electronic interlocking solution using software engineering methods," M.S. thesis, Dept. Elect. & Inf. Eng., Witwatersrand Univ., Johannesburg, 2014.

[39] M. L. Bliguet and A. A. Kjaer, "Modelling interlocking systems for railway stations," M. S. thesis, Technical University of Denmark, 2008.

[40] L. E. Eriksen and B. Pedersen, "Simulation of relay interlocking systems," Technical University of Denmark, 2007.

[41] Q. Cappart, "Verification of railway interlocking systems," M. S. thesis, Louvain Univ., Belgium, 2014.

[42] Ethiopian Railways Corporation, "Introduction to AA-LRT signaling system," Pre-service training document, 2009.

[43] Ethiopian Railways Corporation, "AA-LRT point machine components and maintenance," Pre-service training document.

[44] Ethiopian Railways Corporation, "AALRT constitution and basic principle of light rail line interlocking system," pre-service training document.

[45] P. Woolford, "Interlocking principles," *Rail Saf. Stand. Board*, vol. 1, no. 4, Jan. 2003.

[46] E. Dincel and S. Kurtulan, "Interlocking and Automatic Operating System Design with Automaton Method," in *13th IFAC Symposium on Control in Transportation Systems*, 2012, vol. 45, no. 24, pp. 191–196, Sep. 12-14, doi: 10.3182/20120912-3-BG-2031.00039.

[47] J. Mocki and L. Vlacic, “Railway interlocking process - building a base for formal methods,” vol. 232, pp. 1407–1424, 2018.

[48] G. Hockings, “Computer-based interlocking requirements,” RailCorp Eng. Specification, Australia, Tech. Note. TN-014-3, Aug. 23, 2017.

[49] W. Mesafint, “Case study of Addis Ababa LRT IATP signaling subsystem RAM analysis,” M. S. thesis, Addis Ababa Univ., 2017.

[50] X. Dai, X. Sun, W. Dong, X. Yan and Y. Ji, “M out of N safety computing system based on general-purpose computers,” in *Int. Conf. Computer and Information Technology Application (ICCITA 2016)*, 2016, pp. 90–95.

[51] H. Kim, J. Lee, K. Lee, and H. Lee, “Design of dual-duplex system and evaluation of RAM,” in *IEEE Intelligent Transportation Systems Conf. Proc.*, Oakland, USA, Aug. 25-29, 2001, pp. 1–6.

[52] H. Kim, H. Lee, and K. Lee, “The Design and Analysis of AVTMR (All Voting Triple Modular Redundancy) and Dual – Duplex System,” *Reliab. Eng. Syst. Saf.*, vol. 88, pp. 291–300, 2005.

[53] M. A. Lundteigen and M. Rausand, “Calculation of PFD using Markov,” in *Reliability of Safety-Critical Systems: Theory and Applications*, n.d., pp. 1–33.

[54] CASCO Signal Ltd, “Addis Ababa E-W & N-S (P1) LRT Project Signaling System,” no. B4113305/3301/V1.2.0, Apr. 2014.

APPENDIX A: TERMS AND DEFINITIONS

Availability	The percentage of time that a system is able to perform its required functions at a stated instant of time or over a stated period of time. (EN50126, 1999)
Boolean	A data type that consists of either one or two values, i.e. True of False.
Error	The product state or incorrect information in the system which is liable to lead to a failure.
Fail-safe	The capability of an item of equipment or system to ensure that any failure in a predictable or specified mode will result only in that item or system reaching and remaining in a safe condition
Failure	The departure of a component's functionality targets from the specification. Termination of the ability of an entity to perform a required function under specified conditions.
Failure rate	The failure rate of a component refers to the ratio of the total amount of the independent component failure divided by the operation hour of all equipment.
Fault	A defect either in hardware, software, or in the design. A fault is an identified or potential cause of an error.
Fault-tolerant	A system can continue operation and degradation of performance may be accepted.
Hardware redundancy	Availability of additional hardware identical to the normal working hardware for taking over at the time of failure.
Hazard	Any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment, or property; or damage to the environment.
Hot standby	The main and standby subsystems are powered on. Both the subsystems take input, process it, communicate with each other and finally give one output. If any one of the two systems shuts down, there is no interruption in the output. The load is automatically taken over by the other equipment without any time delay.
Ilock	Intelligent and secure 2*2oo2 computer interlocking system with independent intellectual property and transparent interlocking logic
Line	A railway track along which trains travel.
Interlocking	A general term applied to the setting and releasing of Signals and Points to Prevent unsafe conditions arising.
Mean Time Between Failures(MTBF)	The elapsed time between two adjacent failures (including immediate failure) of a device during operation.
Signal	A visual display device that conveys instructions or provides prior warning of instructions to guide the driver's operation.
Railway	An affordable means of transportation commonly used for the transfer of passengers and freight over a long distance. A railway system consists of signaling field equipment and an electronic interlocking system. These components function collectively to ensure the safe movement of trains on a railway.

Redundancy	The provision of alternative means or parallel paths in a system for accomplishing a given task such that all means must fail before causing a system failure
Reliability	The probability that an item will perform a required function, under stated conditions, for a stated period of time (EN50126, 1999)
Safe failure	Failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that results in loss of production or service, but not the loss of safety.
Safety	The capability to guarantee the safety of traffic, human life, and equipment (EN50126, 1999).
Signals	Placed between track sections and display different aspect indications. These indications are used to inform train operators of conditions ahead on the railway line.
Station	A geographical location of signaling field elements on a railway line where crossing movements may take place.
Steady state availability	The limit of the instantaneous availability function as time approaches infinity.
System	A composite of equipment, skills, and techniques capable of performing or supporting an operational role, or both.
Train	A motorized locomotive coupled to wagons used for the transportation of passengers or goods.

APPENDIX B: FAILURE DATA OF AA-LRT INTERLOCKING SYSTEM (EW16)

Interlocking Place /Station	Failure Occurred Date	Failure Start Time	Recovered Time	Time to Repair	Reason of Failure	Effect of Failure
EW16	05-01-18	8:40	8:43	0:03	T21601、T21603 axle counter turn to red	Switch no. P11608 can't move;
EW16	05-01-18	8:50	8:58	0:08	T21603、T11605 axle counter turn to	and result in switch no.P11608、P11604 and P11602 can't move;
EW16	05-01-18	13:39	13:42	0:03	S21513 signal filament is broken	failure to the normal signal cannot be open;
EW16	10-01-18	19:30	19:35	0:05	T24602、T11607 axle counter turn red by ATS station	result P11606、P11602 can't move;
EW15	12-01-18	21:40	21:44	0:04	S21513 signal filament is broken	failure to the normal signal cannot be open;
EW16	15-01-18	12:37	12:41	0:04	T11604、T11607 axle counter turn red by ATS station	failure result in switch of P11606, P11604 don't move;
EW16	16-01-18	21:47	21:50	0:03	T11604、T11607 axle counter turn red by ATS station	failure result in switch T11604、T11607 don't move;
EW16	21-01-18	21:47	21:50	0:03	S11501 signal filament is broken	failure to the normal signal Can't be open;
EW16	21-01-18	13:10	13:14	0:04	S21513 signal filament is broken	failure to the normal signal cannot be open;
EW16	05-02-18	9:23	9:25	0:02	S21513 signal filament is broken	failure to the normal signal cannot be open;
EW16	06-02-18	8:56	9:02	0:06	T21601、T21603 axle counter turn red by ATS station	results in P11608 switch can't move
EW16	10-02-18	6:10	6:20	0:10	S21513 signal filament is broken	failure to the normal signal cannot be open;
EW16	14-02-18	11:38	11:42	0:04	S21513 signal filament is broken	failure to the normal signal cannot be open;
EW16	18-02-18	17:31	17:33	0:02	S21513 signal filament is broken	failure to the normal signal cannot be open;
EW16	23-02-18	19:09	19:17	0:08	S21513 signal filament is broken	failure to the normal signal cannot be open;
EW16	09-03-18	9:06	9:09	0:03	S21513 signal filament is broken	failure to the normal signal cannot be open;
EW16	14-03-18	7:22	7:24	0:02	T11607、T21602 axle counter turn red by ATS station	failure result in switch of P11602, P11604 and P11606 don't move;
EW16	15-03-18	7:35	7:38	0:03	S21513 signal filament is broken	failure to the normal signal cannot be open;
EW16	17-03-18	20:03	20:08	0:05	T11606、T11604 axle counter turn red by ATS station	failure result in switch of P11604 and P11606 don't move;
EW16	19-03-18	14:09	14:15	0:06	T11607、T21602 axle counter turn red by ATS station	the failure result in switch of P11602, P11604 and P11606 don't move;
EW16	20-03-18	12:39	12:43	0:04	T11606、T11604 axle counter turn red by ATS station	the failure result in switch of P11604 and P11606 don't move;
EW16	21-03-18	17:21	17:26	0:05	S21513 signal filament is broken	failure to the normal signal cannot be open;
EW16	29-03-18	18:57	19:01	0:04	S11901 signal filament is broken	failure to the normal signal cannot be open;
EW16	06-04-18	7:50	9:10	1:20	P11608, P11604, P11602 switch was failure	10603trip（110）late14'39" and 10204trip（115+120）late 15'09"
EW16	11-04-18	21:14	21:25	0:11	The signal X11608 of EW16 up line filament broke.	
EW16	14-04-18	11:35	11:42	0:07	S111608 Signal filament is broken at up line of EW16.	failure to the normal signal cannot be open;
EW16	01-05-18	21:25	22:50	1:25	EW16、EW20、EW22 & NS27 CBI signaling system has failed	P12003 don't move and from EW16 to EW20 and from EW20 to NS27; can't operate;
EW16	03-05-18	17:28	17:44	0:16	T11607, T21602 axle counter turn to red by ATS station	failure result P11606、P11604、P11602 and P12008 switch can't moves;
EW16	05-05-18	17:55	18:02	0:07	T11607, T21602 axle counter turn to red by ATS station	P11602、P11604、P11606、P11608 turnout can't move;
EW16	10-05-18	19:57	20:16	0:19	T11607 and T21602 axle counter turn red by ATS station	switch P11606, P11604&P11602 cannot move;
EW16	14-05-18	11:40	11:56	0:16	T11607 and T21602 axle counter turn red by ATS station	P11604, P11606 cannot move;
EW16	14-05-18	15:41	15:55	0:14	T11607 and T21602 axle counter turn red by ATS station	P11604, P11606 cannot move;

EW16	19-05-18	9:32	9:40	0:08	T11607, T21602 axle counter turn red by ATS station	P11606,P11602,P11604, switch can't move;
EW16	21-05-18	5:55	6:32	0:37	T11607、T21602 axle counter turn red by ATS station	P11606, P11602, P11604, switch can't move
EW16	22-05-18	19:06	19:23	0:17	T11607、T21602 axle counter turn red by ATS station	P11602,P11606 cannot move
EW16	26-05-18	17:39	18:04	0:25	T11607、T21602 axle counter turn red by ATS station	failure result in switch P11604, P11602, P11606 switch don't move
EW16	26-05-18	19:14	19:28	0:14	T11607、T21602 axle counter turn red by ATS station	failure result in switch P11604, P11602, P11606 switch don't move
EW16	27-05-18	17:46	18:05	0:19	T11607, T21602 axle counter turn red by ATS station	switch P11604, P11602, P11606 switch don't move,
EW16	31-05-18	6:50	7:07	0:17	T11607、T21602 axle counter turn to red by ATS station	affect P11604、P11602、P11606、P11608 turnout cannot move
EW16	31-05-18	8:58	9:09	0:11	T11607、T21602 axle counter turn to red by ATS station	affect P11604、P11602、P11606、P11608 turnout cannot move
EW16	05-06-18	17:38	17:44	0:06	T11607 axle counter turn to red by ATS station	failure result in switch of P11604 don't move
EW16	25-06-18	22:38	22:43	0:05	T11603、T11605 axle counter turn red by ATS station	the failure result in switch of P11608 don't move
EW16	28-06-18	14:39	15:02	0:23	T11607、T21602 axle counter turn red by ATS station	P11602、P11604 、P11606、P11608 turn out cannot move
EW16	30-06-18	11:25	11:30	0:05	T11607、T21602 axle counter turn red by ATS station	P11604、P11608 turn out cannot move
EW16	02-07-18	19:38	19:51	0:13	T11607、T21602 axle counter turn red by ATS station	P11602、P11604、 P11606、P11608 turnout don't move
EW16	06-07-18	9:56	10:15	0:19	T11607、T21602 axle counter turn red by ATS station	P11602,P11604,P11606 Switch cannot move
EW16	07-07-18	13:41	13:52	0:11	T21604、T21606 axle counter turn red by ATS station	P12001,P12003,P12005 Switch cannot move;
EW16	08-07-18	16:03	16:19	0:16	T11609、T11611 axle counter turn red by ATS station	affect P11602,P11604, Switch cannot move
EW16	09-07-18	7:21	7:24	0:03	T21602、T11607 axle counter turn red by ATS station	effect P11604,P11606,P11602,P11605 switch cannot move
EW16	09-07-18	18:16	19:40	1:24	failure in switch P11602,P11604 and P11606 don't move	
EW16	13-07-18	11:30	11:35	0:05	T11605 axle counter turn red by ATS station	the failure result in switch of ; P11608 P11604 don't move
EW16	13-07-18	12:23	12:33	0:10	T11607、T21602 axle counter turn red by ATS station	the failure result in switch of P11602 ,P11604 ,P11606, don't move
EW16	17-07-18	11:30	11:35	0:05	T11602、T11607 axle counter turn red by ATS station	P11602 ,P11604 ,P11606 switch is can't move ;
EW16	17-07-18	22:05	22:10	0:05	T11602、T11607 axle counter turn red by ATS station	P11602 ,P11604 ,P11606 switch is can't move ;
EW16	25-07-18	20:13	20:25	0:12	T11607、T21602 axle counter turn red by ATS station	P11604,P11606 ,P11608 switch is can't move ;
EW16	30-07-18	17:10	17:32	0:22	T11607、T21602 axle counter turn red by ATS station	affect P11602, P11604, P11606 switch cannot move;
EW16	08-08-18	19:50	20:05	0:15	T11607、T21602 axle counter turn red by ATS station	failure result in switch; P11602,P11604 and P11606 don't move
EW16	08-08-18	21:40	22:04	0:24	T11607、T21602 axle counter turn red by ATS station	failure result in switch; P11602,P11604 and P11606 don't move
EW16	11-08-18	7:12	7:24	0:12	T11607、T21602 axle counter turn red by ATS station	failure result in switchP11602,P11604 and P11606 don't move
EW16	13-08-18	12:43	12:59	0:16	T11619、T21621 axle counter turn red by ATS station	failure result in switchP11602,P11604 and P11606 don't move
EW16	14-08-18	7:10	7:28	0:18	T11607、T21602 axle counter turn red by ATS station	115train =11 minute late, 105+106 = 7 minute late, 121 train = 10 minute late.
EW16	17-08-18	15:07	15:29	0:22	T11607、T21602 axle counter turn red by ATS station	failure result in switch; P11602,P11604 and P11606 don't move
EW16	29-08-18	4:00	7:13	3:13	T11613 and T11611 axle counter turn to red and by ATS station	P11608,P11604,P11602 turnout Affect operation
EW16	06-10-18	15:00	15:19	0:19	T11607、T21602 axle counter turn red by ATS station	affect P11602, P11604, P11606 switch cannot move
EW16	07-10-18	18:53	19:02	0:09	T11607、T21602 axle counter turn red by ATS station	affect P11602, P11604, P11606 switch cannot move
EW16	09-10-18	19:52	19:57	0:05	T21602、T11607 axle counter turn red by ATS station	the failure result in switch No P11608 P11604 and P11606 switch don't move

EW16	11-10-18	21:45	21:49	0:04	T11604、T11606 axle counter turn red by ATS station	failure result in switch of P11606 and P11604 don't move
EW16	12-10-18	16:51	17:14	0:23	T11607、T21602 axle counter turn red by ATS station	the failure result in switch of P11606, P11604andP11602 don't move
EW16	16-10-18	9:09	9:41	0:32	T11607、T21602 axle counter turn red by ATS station	the failure result in switch of P11606, P11604andP11602 don't move,
EW16	16-10-18	18:01	18:30	0:29	T11607、T21602 axle counter turn red by ATS station	the failure result in switch of P11606, P11604andP11602 don't move
EW16	24-10-18	7:48	8:05	0:17	T21602、T11607 axle counter turn red by ATS station	switch of P11602, P11604 and P11606 cannot move
EW16	26-10-18	8:26	8:40	0:14	T11607 and T21602 axle counter turn to red by ATS station	in switch P11602, P11604,P11606 can't move
EW16	26-10-18	13:47	14:06	0:19	T11607 and T21602 axle counter turn to red by ATS station	switch P11602, P11604,P11606 can't move
EW16	11-12-18	19:21	19:24	0:03	S11501 signal filament	

T11607, T21602, etc. are the type of axle counters

S11501, S10801, etc. are the type of signal filaments

P11602, P11604, etc. are types of switches