Addis Ababa University

Addis Ababa Institute of Technology

School of Electrical and Computer Engineering

Failure analysis of signaling system of Addis Ababa-Light Rail Transit

By:

Yosef Bekele

Thesis submitted to Addis Ababa institute of Technology in partial fulfillment of the requirements for the degree of master of science in Electrical Engineering Under Railway Electrical Engineering

Advisor:

Mr. Abi Abate

April, 2015

ADDIS ABABA UNIVERSITY

ADDIS ABABA INSTITUTE OF TECHNOLOGY

FAILURE ANALYSIS OF SIGNALING SYSTEM OF AA-LRT

BY

YOSEF BEKELE

APPROVAL BY BOARD OF EXAMINERS

_____	_____
CHAIRMAN DEPARTMENT OF GRADUATE COMMITTEE	SIGNATURE
_____	_____
ADVISOR	SIGNATURE
_____	_____
INTERNAL EXAMINER	SIGNATURE
_____	_____
EXTERNAL EXAMINER	SIGNATURE

Declaration

I certify that research work titled "*failure analysis of signaling system of AA-LRT*" is my own work. The work has not been presented elsewhere for assessment. Where material has been used from other sources it has been properly acknowledged / referred.

Name: Yosef Bekele
Signature: _____
Place: Addis Ababa
Date of submission: _____

This thesis work has been submitted for examination with my approval as a university advisor.

Mr. Abi Abate _____
Advisor's Name Signature

Acknowledgement

I would like to acknowledge Mr. Abi Abate who suggested and advised me on this research, and to all who shared their precious time and ideas with me. Also I am thankful to respective ERC and CREC offices for their collaboration and support.

Abstract

Railway signaling system is one of the most important parts of the many which make up the railway system. It is the vital control system which demands the use of reliable and fault tolerant system as it directly related to the safe movement of passenger trains. Ensuring safety in railway signaling systems is considered as significant as a guarantee of the safe and efficient operation of the whole railway. In fact, one of the most important objectives of a safety analysis of the signaling system is to maintain a high degree of safety.

Therefore, to avoid these problems and provide an optimized signaling, a signaling system design should incorporate additional safety analysis. One of the safety analysis methods from design stage is failure analysis which is used to study the whole dynamic system, point out potential failure modes, failure propagation scheme and used to predict about the system.

To this end, this thesis presents the failure analysis of Addis Ababa-Light Rail Transit signaling system by employing *model-based failure analysis methods* and system fault tree, causes and effects, major failures are investigated.

Failure propagation models for the subsystems of AA-LRT signaling system are modeled on Matlab-Simulink, where signaling equipments in a main station are represented. Functional interactions between those equipments are also represented.

Hierarchically Performed Hazard Origin and Propagation Studies (HiP-HOPS) is used from the most common model-based safety analysis tools to define each signaling system equipment local failure data and to analyze failure models which are done on Simulink.

Fault trees are generated as a result for selected hazards in simulations showing the possible causes of failures.

Keywords:

- Failure modes
- Failure propagation
- Model based failure analysis
- HiP-HOPS

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

AC	Axle Counter
ATP	Automatic Train Protection
ATS	Automatic Train Supervision
CASCO	CASCO SIGNAL LTD.
CBI（CI）	Computer Based Interlocking
CC	Carborne Controller
DCS	Data Communication System
EN	Europe Standard
FHA	Fault Hazard Analysis
FMEA	Failure Mode Effect Analysis
FMECA	Failure Mode Effect & Criticality Analysis
FTA	Fault Tree Analysis
HMI	Human Machine Interface
IATP	Intermittent Automatic Train Protection
IEC	International Electrotechnical Commission
LATS	Local Automatic Train Supervision
LED	Light Emitting Diode
LEU	Line Encoder Unit
MMS	Maintenance Monitoring System
MSS	Maintenance Support System
MTBF	Mean Time Between Failures
MTTF	Mean Time To Failures
MTTR	Mean Time To Repair
OCC	Operation Control Centre
PHA	Preliminary Hazard Analysis
RAMS	Reliability, Availability, Maintainability, Safety
RAP	Radio Access Point
SCR	Signal Control Room
SDM	Diagnostics and Maintenance Subsystem
SIG	Signaling
SIL	Safety Integrity Level
TRE	Trackside Radio Equipment
ZLC	Zone Logic Computer
2oo2	2 out of 2 channel configuration

Chapter One

Introduction

1.1. Background

Railway systems have a very low tolerance for accidents, because of the potentially large numbers of injuries and deaths, huge financial losses and even worse social effects. Achieving a high degree of safety is one of the most important objectives of a railway signaling system. The safety of trains is dependent on the correct and prompt output of its signaling system.

A key concern in safety engineering is understanding the overall emergent failure behavior of a system, i.e., behavior exhibited by the system that is outside its specification of acceptable behavior. A signaling system can exhibit failure behavior in many ways, including that from failures of individual or a small number of components.

The following are some of the major reasons to why it is necessary to do failure analysis [1];

- Insure system quality
- Achieve system reliability
- Prevent safety or environmental hazards
- Prevent customer (passengers) dissatisfaction
- In addition, for easy visualization of fault propagation in case when it happens. Maintenance and troubleshooting will then be simple tasks.

Failure analysis can be done along with the system design process or after the system design is put into its implementation [2]. The later requires a historical (recorded) data of the system failure while it is in operation. Based on this data, failure rate and hazards can simply be forecasted. But this approach is of little value as compared to doing failure analysis prior to implementation, that is at design lifecycle. Different approaches are followed in the analysis of failure by different railway services which will be presented in the literature review.

1.2. Statement of the problem

The signaling system that is proposed for the AA-LRT is a new design, i.e., no recorded failure data is available. Therefore, without doing failure/safety analysis prior to implementation to study faults, their propagation and effects, the operation will exhibit the faults and may cause severe accidents. Considering this problem, it is of paramount importance to study the signaling system safety from the design stage so that catastrophic failure modes can be eliminated or reduced through the design modification.

A model based failure analysis method is used to study the safety of AA-LRT signaling system in this thesis. With this method it is also easier to visualize propagation of failures from single or multiple components to the general system output which then cause hazards to the train operation.

1.3. Objective

1.3.1. General objective:

The main objective of this research is to assess the safety of AA-LRT signaling system by doing failure analysis based on the actual design data, which includes modeling component failure propagation to the output and generating fault trees related to potential failures, and give suggestions for necessary improvements before implementation and operation of the service.

1.3.2. Specific objective:

- To determine catastrophic failure modes of the signaling system and investigate their propagation
- Precisely modeling and illustrating the system failure behavior
- Comparing the safety requirements with the results and suggesting correction

1.4. Literature Review

To cope with the increasing complexity of signaling systems, CENELEC, IEC and many countries have developed several standards and recommendations. These standards regulate the system development process (lifecycle) of signaling systems to design for safety, and also give out technical requirements, such as Safety Integrity Level (SIL).

Common traditional safety/failure analysis methods which are recommended in the safety assessment process are: Failure Modes & Effects Analysis (FMEA), Failure Modes, Effects and Criticality Analysis (FMECA), Fault Tree Analysis (FTA), Hazard and Operability Analysis (HAZOP), Preliminary Hazard Analysis(PHA), Cause-Consequence Analysis, etc **[3].**

These specific inductive or deductive methods of analysis are used to identify hazard, trace causation and evaluate their risk at different stages of the lifecycle, and the results are the main basis for design decisions. This methodology has been used by most railway equipment suppliers over the last 20 years, although they obviously lag behind the state-of-the- art engineering practice**[3].**

FMECA is mostly employed from the traditional methods **[3,4].** In extreme case, FMECA would be of little value to the design decision process if the analysis is performed after the system is built. While the FMECA identifies all failure modes, its primary benefit is the early identification of all critical and catastrophic subsystem or system failure modes so they can be eliminated or minimized through the design modification at the earliest point in the development effort. Therefore, FMECA should be performed at the system level as soon as preliminary design information is available and extended to the lower levels as the detail design progress.

These traditional qualitative methods emerge from a long expertise in building safety-critical systems. Their disadvantage is, that they mainly rely on skill and expertise of the safety engineer. A potential safety risk will only be anticipated if the engineer “foresees” it at design time. This becomes ever harder, because of rising hardware and software complexity.

A new trend is to advance the analysis methods on a model-based level **[5]**. This means, that a model of the system under consideration as well as its environment is built. The (safety) analysis is then not only grounded on the engineers skill but also on the analysis of the model. In this way some causes for hazards can be found much earlier. Errors found at early design stages are easier to remove and redesign is less costly.

One solution of model based safety analysis is extending the system development model with a fault mode. Formal languages are used to describe normal and failure behaviors of the system, and model checking tools or simulation engines are used to do automatic analysis. Some commercial safety analysis software tools/packages based on this idea are available, such as FSAP/NuSMV-SA and SCADE . However, the major portion of this kind of model is still a normal process, rather than a failure process. It is very difficult to plug in detail failure information because of the limitation of model scale from analysis tools. Another solution is to model the failure propagation behavior directly. The Failure Propagation and Transformation Notation (FPTN) described in **[6]** is the first component-based failure behavior model. Kaiser introduced modular concepts for a basic fault tree to analyze complex component-based systems. Based on early researches, Papadopoulos et al. proposed a model based semi-automatic safety and reliability analysis technique that uses tabular failure annotations as the basic building block of analysis at the component level, called Hierarchically Performed Hazard Origin and Propagation Studies (HiPHOPS) **[7, 8]**. This tool can automatically synthesis the component failure modes and generate a fault tree.

1.5. Contributions

This research lays a baseline for component based safety analysis of AA-LRT signaling system. The stored failure data of components and failure propagation model can always be checked for failures incase if a hazard is expected to happen to the actual system.

Other contributions of this study includes: suggesting improvement of the system after doing complete failure model and optimization, determination of quantitative aspects such as probability of occurrence of hazards, forecasting about the system which is important in the expansion and development of the system.

The study also initiates the use of modern model based failure analysis methods to any system (Electrical, Mechanical, ...). Hence, the same analysis can be employed for other systems of railway which Ethiopia is implementing.

1.6. Methodology

Data collection

The general architecture of the signaling system, which is employed for the case of Addis Ababa Light Rail Transit, type and placement of components and full data of each subsystems is obtained from CREC.

Corresponding failure behavior and failure modes of the components is studied and determined from corresponding equipment manufacturing companies sites. These data are the ones which are used in the system failure modeling phase. Some of them are not directly placed in the components datasheet, but the failure modes are determined through study and reference.

System modeling and simulation

Considering the advantages of HiP-HOPS study than classical methods, in this thesis failure model of the signaling system is done following procedures of HiP-HOPS . That is a failure model containing each components of the system or subsystems (grouping components with specific task as a subsystem block) is done on software such as Matlab Simulink or Simulation-X. Components failure data, after being obtained from their manufacturers specification sheets, is defined in the model using HiP-HOPS_Launcher which can work with the above softwares. Finally this model is synthesized and analyzed to generate Fault trees showing the propagation of failures.

1.7. Outline of the Thesis

This paper is organized into six chapters:

- The first chapter was the introduction part in which the background, statement of the problem, objective, literature review, methodology and applicability of the research are included.

- The second chapter discusses about system failure modeling procedures. Here the chapter focuses on the HiP-HOPS component based safety analysis method and the approaches followed to come up with a good failure model of a system and its fault trees.
- The third chapter is about the signaling system structure of AA-LRT and its sub-systems. Based on the data obtained from CREC, components employed in the design and their functional interconnection is presented for each subsystem.
- In the fourth chapter, the failure model for the signaling system is discussed. This includes the models on Matlab Simulink and failure data of each component or sub-systems.
- Fifth chapter is about the simulation results and discussions based on the models described under the fourth chapter.
- Final chapter includes conclusions and recommendations for improvements and future works.

Chapter Two

System failure modeling procedures

In this chapter, the main phases of system failure modeling using hierarchically performed hazard origin and propagation studies will be presented.

As discussed in the Literature Review, there are so many ways to model electrical systems failure behavior. The ones which are broadly mentioned was model based compositional (component based) failure analysis methods. HiP-HOPS, which is used in this thesis, is one of them.

HiP-HOPS is a compositional safety analysis tool that takes a set of local component failure data, which describes how output failures of those components are generated from combinations of internal failure modes and deviations received at the components' inputs, and then synthesizes fault trees that reflect the propagation of failures throughout the whole system**[9,10].**

From those fault trees, both qualitative and quantitative results can be generated as well as a multiple failure mode FMEA.

A HiP-HOPS study of a system design typically has three main phases:

- ✓ Modeling phase: system modeling & failure annotation.
- ✓ Synthesis phase: fault tree synthesis.
- ✓ Analysis phase: fault tree analysis & FMEA synthesis.

Although the first phase remains primarily manual in nature, the other phases are fully automated. The general process in HiP-HOPS is illustrated in Fig.1 below:

The first phase – **system modeling & failure annotation** – consists of developing a model of the system (including hydraulic, electrical or electronic, mechanical systems, as well as conceptual block and data flow diagrams) and then annotating the components in that model with failure data. This can be done on MATLAB-Simulink **[11].**

The second phase is the **fault tree synthesis process**. In this phase, paths of failure propagation are traced through the model by combining the local failure data for individual components and

subsystems. The result is a network of interconnected fault trees defining the relationships between failures of system outputs and their root causes in the failure modes of individual components. It is a deductive process, working backwards from the system outputs to determine which components caused those failures and in what logical combinations. This phase is an automated one.

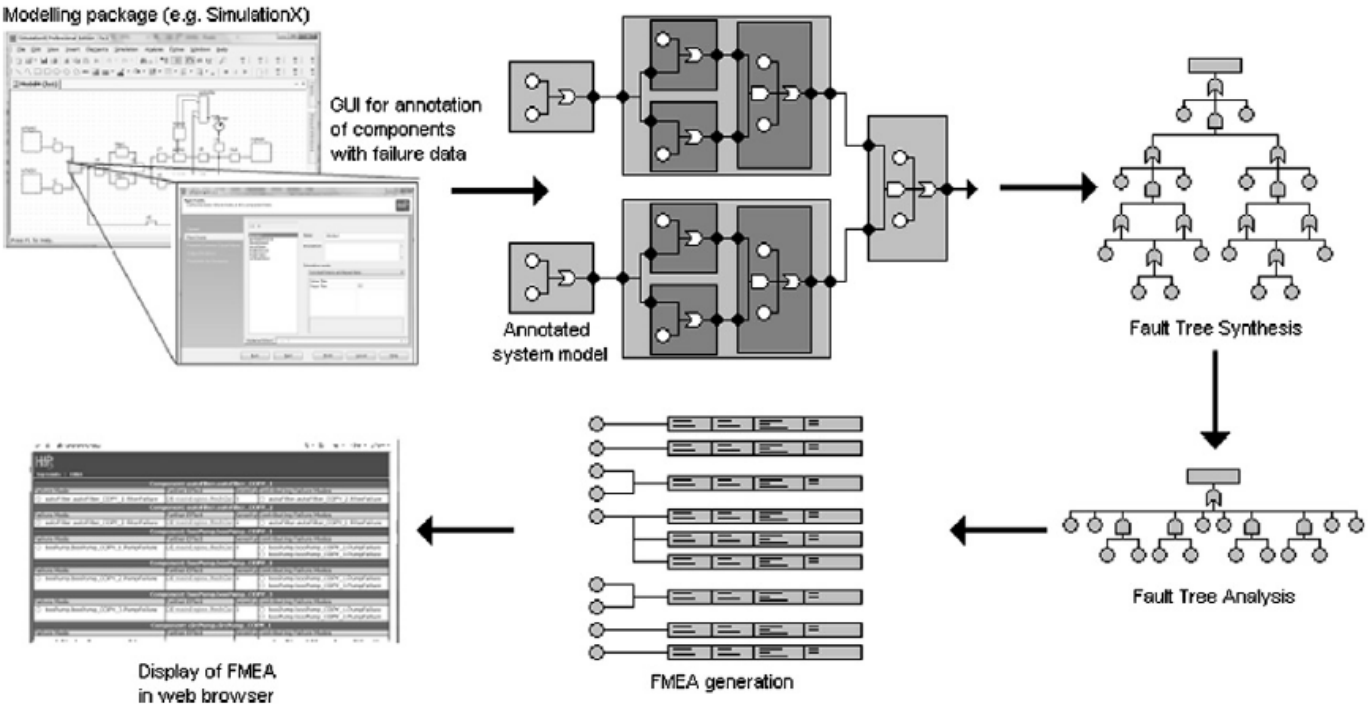


Figure 1. failure analysis process using HiP-HOPS

The final phase involves the **analysis of those fault trees and the generation of an FMEA**. The fault trees are first minimised to obtain the minimal cut sets – the smallest possible combinations of failures capable of causing any given system failure –and these are then used as the basis of both quantitative analysis (to determine the probability of a system failure) and the FMEA, which directly relates individual component failures to their effects on the rest of the system. The FMEA takes the form of a table indicating which system failures are caused by each component failure.

Each phases in the failure modeling phase are described in detail below.

2.1. Modeling phase

The system failure models are done on Simulink or other software, which illustrate components as blocks and connections are the functional data paths. These models are not supposed to be the model of the system design with every functionality and representation rather a model showing the propagation of failures from one component to the other**.**

Once a model has been obtained, it is necessary to annotate it with failure data. At its core, HiP-HOPS operates on the idea that an output failure of a component is caused by a logical combination of input failures and internal faults and that the output failure will then propagate along structural connections in the model to another component to be received as a new input failure. Thus for the purposes of the safety analysis, each component in the model needs to be annotated with its own local failure data, describing how that component can fail and how it responds to failures propagated from other components in the system.

The local failure data takes the form of a set of failure expressions relating failures at a component's outputs (known as **output deviations**) to a logical combination of internal failure modes (**basic events**) and **input deviations** (i.e. failures received at the component's inputs)**[12].**

For the specification of input and output deviations, a generic and abstract syntax was developed, consisting of two parts; the first part is the failure class, an identifier that describes the type of failure, and the second is the input or output port at which the failure is received or propagated. There are different ways of classifying failures, e.g. by relating them to the function of the component, or by classifying according to the degree of failure – complete, partial, intermittent, etc.

In general, however, the failure of a component will have adverse local effects on the outputs of the component which, in turn, may cause further effects travelling though the system on material, energy or data exchanged with other components.

Therefore in HiP-HOPS, we generally classify the effects into one of three main failure classes, all equally applicable to material, energy or data outputs:

- **Omissions**, i.e. the failure to provide the input or output;
- **commissions**, i.e. a condition in which the input or output is provided inadvertently and in the wrong context of operation;

- and finally **malfunctions**, a general condition in which the input or output is provided but in a form which deviates from the design intention, e.g. with a value that exceeds thresholds or is transmitted at the wrong time.

Since this classification adopts a functional viewpoint which is independent of technology, it could provide a common basis for describing component failures and their local effects.

In this study, failure classes are often abbreviated, e.g. O = Omission, C = Commission, V = Value, etc., and combined with the name of the port at which they occur, thus ‘‘O-input1” might be an omission of input at port ‘‘input1”. Sometimes it is useful to parameterise the failure class as well, e.g. OF for omission of flow or HP for high pressure, etc.

Standard Boolean logic operators AND and OR are used to combine input deviations and basic events and then relate these to a given output deviation, e.g. ‘‘O-out1 = O-in1 OR internalFailure” is an expression that describes how an omission of output is caused by a corresponding omission of input or some internal failure of the component itself. Internal failure modes typically depend on the domain, e.g. a blockage for a hydraulic system or a short circuit in an electrical system, etc. Note that failure classes can also be transformed from input to output; for example, if a particular component was designed to fail silent in response to input errors, it may transform value input failures into an omission of output: ‘‘O-out = V-in OR C-in”, etc.

In this way, mitigation of failures can also be represented.

The set of failure expressions for a component therefore describes all possible deviations of all outputs for that component in terms of its possible internal failure modes and any relevant deviations at its inputs (which are in turn propagated from output deviations of other components).

In addition to the logical information, it is possible to add numerical data for the failure modes of the component, detailing the probability of the occurrence each failure. Multiple different probabilistic models can be used, e.g. constant failure & repair rates, MTTF & MTTR values, Binomial and Poisson distributions, dormant failures, and Weibull variable failure rates, etc. This provides a great deal of flexibility when modelling the quantitative aspects of component failure (assuming the probability data for the failure modes are available). This data is later used to arrive at an estimate of the unavailability for each system failure.

2.1.1. Failure Rates

Entering the failure models for the basic events, allows quantitative analysis to take place. There are a number of different formulae, each with different parameters, and each will yield a different unavailability for the basic event. The current formulae **[13]** are listed below**.**

- ***Constant Failure and Repair Rate***

Parameters:

λ - Failure Rate

μ - Repair Rate

This is the currently implemented calculation method, and assumes an exponential distribution. The formula for unavailability is as follows:

$$u = \frac{\lambda}{\lambda + \mu} \times \left(1 - e^{-(\lambda+\mu)t}\right) \qquad (2.1)$$

- ***Constant Failure and Mean Time To Repair (MTTR)***

Parameters:

λ - Failure Rate

MTTR - Mean Time To Repair

Very similar to above, with the exception that the repair data is entered as the MTTR instead. This is then converted to the repair rate μ (since μ = 1 / MTTR) and the previous unavailability calculation is used.

- ***Mean Time To Failure(MTTF) and constant Repair***

Parameters:

MTTF - Failure Rate

μ - Repair Rate

Very similar to above, with the exception that the failure data is entered as the MTTF instead. This is then converted to the repair rate λ (since λ = 1 / MTTF) and the previous unavailability calculation is used.

- ***Mean Time to Failure and Repair***

Parameters:

MTTF - Mean Time To Failure

MTTR - Mean Time To Repair

Like the last, except that both the failure and the repair data are entered as mean times. These values will be converted and the unavailability formula in used.

Fixed Unavailability

Parameters:

Unavailability - The constant unavailability

This is the option to choose if the unavailability of the event is already known.

Binomial Failure Model

Parameters:

λ - Failure Rate

μ - Repair Rate

n - Number of components

m - Minimum number of components needed to fail to cause subsystem failure

T - The time of operation of the subsystem

This model is useful for representing situations where m failed components out of n will result in failure, such as in a voter. The formula is as follows:

$$u = \sum_{k=m}^{n} \left(\frac{n!}{k! \times (n-k)} \times q^k \times (1-q)^{(n-k)}\right) \qquad (2.2)$$

Poisson Failure Model

Parameters:

λ - Failure Rate

n - Number of components in operation at any one time

s - Number of spare components available

t - Time of operation of the subsystem

This method can be used to model the effects of limited numbers of replacement components.

Formula:

$$u = \sum_{k=0}^{s} \left(\frac{x^k \times e^{-x}}{k!}\right) \qquad (2.3)$$

2.2. Synthesis phase

When we examine a component out of system context, input and output deviations represent only potential conditions of failure. However, when we place the component in a model of a system, the input deviations specified in the analysis can actually be triggered by other components further upstream in the model and the specified output deviations can similarly cause more failures further downstream.

Thus by linking the output failures of a certain class from one component to the input failures of that same failure class at another component, via the architectural connections and interactions stored in the model, it is possible to map out the global propagation of failures through the system as a whole in the form of a series of interconnected fault trees **[12,13].** Thus the causes of a significant hazard or failure at the output of the system can be traced back through this propagation by simply analyzing the fault trees and determining the minimal cut sets.

This process of synthesizing fault trees from the component failure data (which are effectively mini fault trees) is automated in HiP-HOPS. The fault trees are constructed incrementally, working backwards from the outputs of the system (e.g. electromechanical actuators) towards the system inputs (e.g. material/energy resources, operators, and data sensors, etc.) and joining causes of failures in one component to their effects in another. At each stage, the mini fault trees representing the local failure data of a component are added to the tree being generated.

In this way, an overall view of the global propagation of failure in the system can be automatically captured by traversing the model and by following the causal links specified in the local safety analyses of the components. Note that the mechanically synthesized fault trees produced record the propagation of failure in a very strict and methodical way, starting from an output failure and following dependencies between components in the model to systematically record other component failures that progressively contribute to this event. The logical structure of the tree is determined only by interconnections between the components and the local analyses of those components. This logical structure is straightforward and can be easily understood, unlike the structures of many manually constructed fault trees, which are often defined by implicit assumptions made by analysts.

To manage complex hierarchical models effectively, the synthesis algorithm in HiP-HOPS will perform traversals both across the vertical and horizontal axis of the design hierarchy, allowing the annotation of the system hierarchy at all levels of the design.

HiP-HOPS is also designed to recognise and handle loops in the model that create circular references to the same failure logic (e.g. conditions such as: event A is caused by event B which in turn is caused by event A). When such circles are encountered, the failure logic contained in the circle is only incorporated once in the fault trees. At the same time, a warning note is generated in order to encourage the analyst to investigate whether or not the circular logic in the system was valid or the result of a modelling error. In general it is normally possible in the steady state to determine what the final effect on the system will be of an initiating failure further upstream.

2.3. Analysis phase

In the final phase, the synthesized system fault trees are analyzed, both qualitatively and quantitatively, and from these results a multiple failure mode FMEA is generated**[13].** Firstly, the fault trees undergo qualitative analysis to obtain their minimal cut sets, which reduces them in size and complexity. This is achieved using various logical reduction techniques, i.e. applying logical rules to reduce the complexity of the expressions and remove any redundancies. Once the minimal cut sets have been obtained, they are analysed quantitatively, which produces unavailability values for the top events of each fault tree.

The last step is to combine all of the data produced into an FMEA, which is a table that concisely illustrates the results. The FMEA shows the direct relationships between component failures and system failures, and so it is possible to see both how a failure for a given component affects everything else in the system and also how likely that failure is. A classical FMEA only shows the direct effects of single failure modes on the system, but because of the way this FMEA is generated from a series of fault trees, HiP-HOPS is not restricted in the same way, and the FMEAs produced also show what the further effects of a failure mode are; these are the effects that the failure has on the system when it occurs in conjunction with other failure modes.

Figure 2 below shows, the general process **[13].** And figure 3 shows an example of local failure data of a given component.

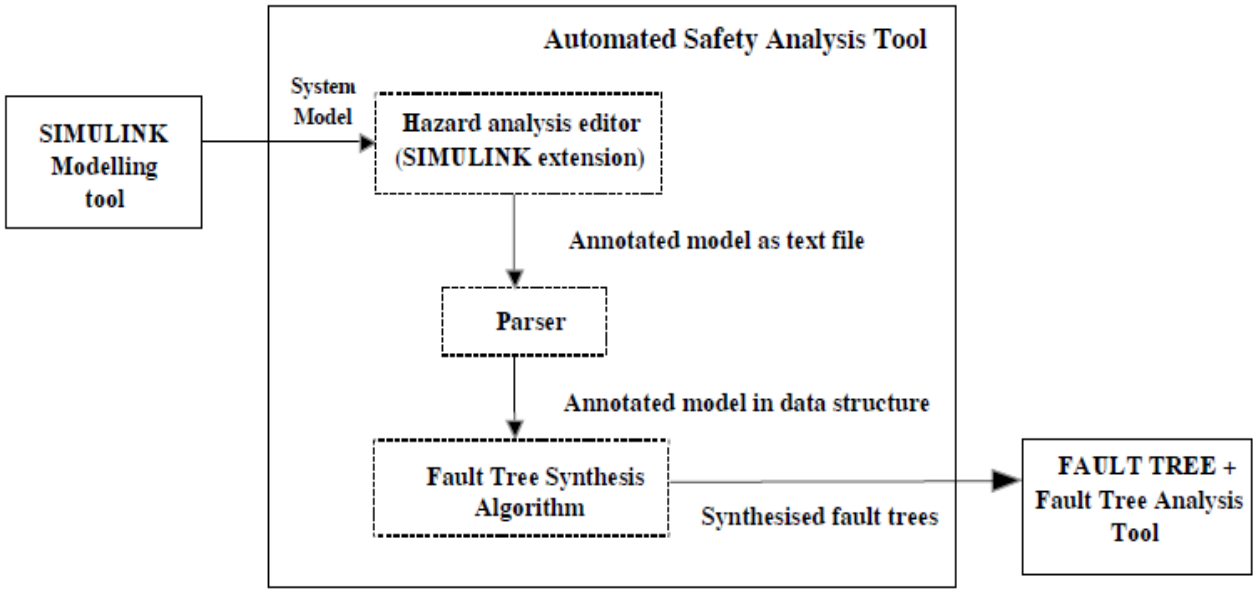
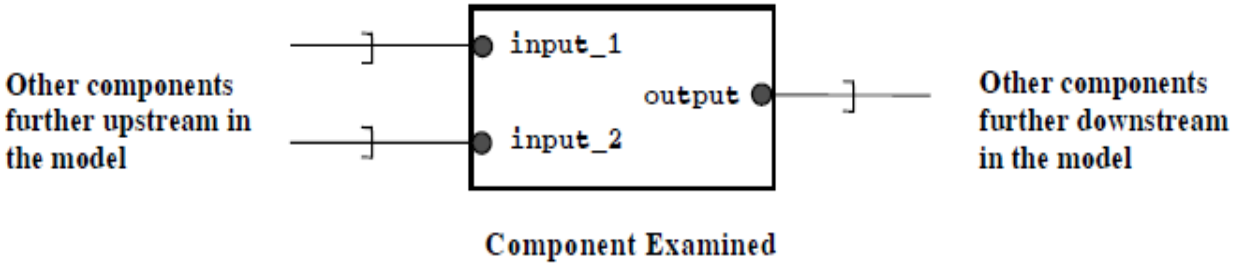


Figure 2. automated analysis using HiP-HOPS tools



Output Failure Mode	Description	Input Deviation Logic	Component Malfunction Logic	λ(f/h)
Omission-output	The component fails to generate the output	Omission-input_1 AND Omission-input_2	Jammed OR Short_circuited	$5X10^{-7}$ $6X10^{-6}$
Wrong-output	The component generates wrong output	Wrong-input_1 OR Wrong-input_2	Biased	$6X10^{-8}$
Early-output	Early output	…	…	…

Figure 3. example of failure data of component and failure catagorization

Why HiP-HOPS

Fault Tree Analysis (FTA) and Failure Modes & Effects Analysis (FMEA) are classical system analysis techniques used in reliability engineering. They are methods by which we can discover information about the potential faults in a system that we can then use to correct those faults. Both are widely used in the automotive, aerospace, nuclear, and other safety critical industries.

FTA is a deductive technique, which means it works from the top down. This is done by assuming a system failure has occurred and working backwards to try to determine what possible combinations of events might have caused it; the system failure then becomes the *top event* of the fault tree, and the individual component failures form the leaf nodes (or *basic events*), and are combined through logical gates such as OR and AND. The fault tree can then be analysed either qualitatively, to determine the smallest combinations of basic events needed to cause the system failure, or quantitatively, to obtain the probability of the top event occurring**[14-18].**

FMEA, by contrast, is an inductive technique, and works from the bottom up. It involves proposing a certain event or condition, and then trying to assess the effects of that initial event on the rest of the system. The end result is a table of failures and their effects on the system, which provide the analyst with an overview of the possible faults.

Both techniques are useful and provide valuable information about systems, but both suffer from the same flaw: they are primarily manual techniques, and the process of performing these analyses can be laborious, especially for larger and more complex systems. In such cases, it is more likely that the analyst will make a mistake, or that the results once obtained are too numerous to interpret efficiently.

This problem means that both FTA and FMEA tend to be performed only once, either after the system has been designed, in order to check its reliability, or after the system has been put into operation and has failed, in order to find out what went wrong. This is unfortunate, because both FTA and FMEA are potentially very useful when they are integrated into the design process itself, so that a system can be designed with safety and reliability in mind. By using these system analysis techniques as part of an iterative design process, it is possible to identify and remedy potential flaws and faults much earlier, thereby saving both time and effort and producing a more reliable product.

However, before FTA and FMEA can be incorporated into the design process in this way, they need to be automated in some fashion, so that they can be carried out much more quickly and

efficiently, and thus maximising their contribution to the design. The HiP-HOPS Fault Tree Synthesis (FTS) tool is intended to achieve such a goal. By including reliability annotations as part of the system model, HiP-HOPS can examine the model and automatically construct and analyse both fault trees and FMEAs. The result is a semi-automated process which takes much of the burden off the system designer and speeds up the analysis considerably, allowing the designer to quickly identify weak points in the model and take steps to remedy them.

Chapter Three

AA-LRT signaling system

In this chapter, the Addis Ababa Light Rail Transit signaling system design general structure and equipments placement is described in short. The major subsystems and functionalities are also stated. This is an important section to understand the actual layout and is necessary to model the failure propagation behavior of the system.

The signaling system design of AA-LRT project is based on iCMTC system provided by a Chinese organization "CASCO"**[19,20]**. It includes the following subsystem**:**

- iTC subsystem(IATP subsystem-);
- iLock subsystem(CBI subsystem);
- iTC subsystem(ATS subsystem);
- DCS subsystem;
- MSS subsystem.

The subsystems categorization is based on specific tasks and functions each provides. The collective tasks and functions fully addresses the requirements of a good signaling system design. The basic functions of each subsystem will be described in this section.

Each subsystem encompasses a number of signaling equipments which are localized as indoor, outdoor (trackside) and onboard. The implementation of the subsystem is in a distributed manner, i.e., some are available only in depots, in mainline stations, or central control stations, whereas some of them exists in all.

Standards such as European communication, signaling and safety standards (e.g, EN50128, EN50129, EN50159), European electric and magnetic property related standards, environmental and safety standards, Chinese technical standards, and others are checked for each equipment, system layout and testing under each subsystem.

Figure 4,**[20]** below shows all subsystems implementation in corresponding stations (depot, main station and operations control) along the general track layout. It shows that each indoor, outdoor and onboard equipment placements. It also shows signaling data communication buses between each station and redundancy of the architecture.

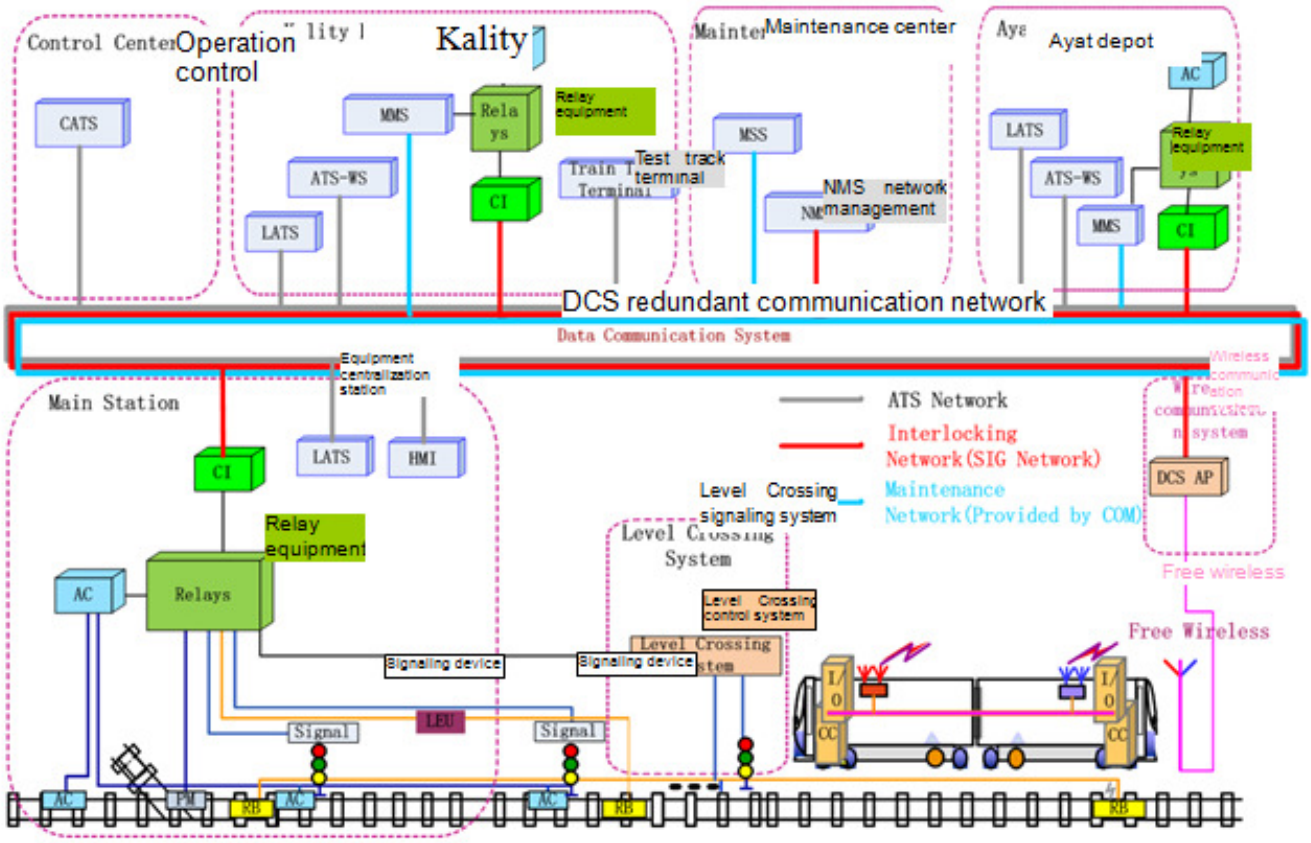


Figure 4. General Signaling System Structure for AA-LRT

3.1. The CBI system

The Computer Based Interlocking (CBI) is a system which controls railway station signal devices by using computer technology to finish transportation tasks. It is mainly composed of Man Machine Interface (MMI or display) & maintenance computer, controller (interlocking computer with redundancy), relay interface circuits and controlled signaling devices (signal, switch, axle counters, etc).

The CBI system is responsible for the following:

- Perform interlocking logical processing for corresponding station.
- Perform information exchange between Zone Logic Computers.
- Be responsible for collecting and driving the relevant wayside signal equipment, CBI interface with switch machine, signal, axle counters, etc. through vital relays;
- Interface with Automatic Train Supervision (ATS) system through the network, receive

ATS control command and send the display information to ATS.

- Interface with Line Encoding Unit (LEU), providing the signal and switch information to Carborne Controller (CC).
- Provide the friendly maintenance and diagnose function.

The CBI system of Addis Ababa Light Rail Transit includes:

- The mainline interlocking system (CBI): which is implemented in 8 Mainline Stations
- Depot interlocking: which is implemented in Depots.

The system is configured only in 8 equipment centralization stations (out of the 39 train stations) for the overall system (E-W & N-S)**[20]**. And the interlocking signaling network is done using a fiber optic cable connection.

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

Figure 5 [20], shows CBI system equipments and their communication paths within a single Mainline station. The interlocking system which is Zone Logic Computer (with redundancy) receives commands (Route set, Route release and Route lock commands) from workstations (HMI) and controls wayside signal devices through the relay interface circuit. It also gives information about the status of the signal devices to the HMI via the communication bus.

The system is configured with two set of redundancy network system for communication transmission, one is network transmission channel for information exchange between ZLC system and ATS subsystem, SDM (diagnosis and maintenance system) and HMI; Another is for ZLC and adjacent stations ZLC, also vehicle Carborne Controller (CC).

CBI is combined with the ATS system to control the train route automatically. Through ATS network, the interlocking devices provide the signal status information to ATS equipments, and receive the route control command from ATS system.

Generally, CBI system ensures the safety train-running, and control the routes, signals and switches under 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 is safe.

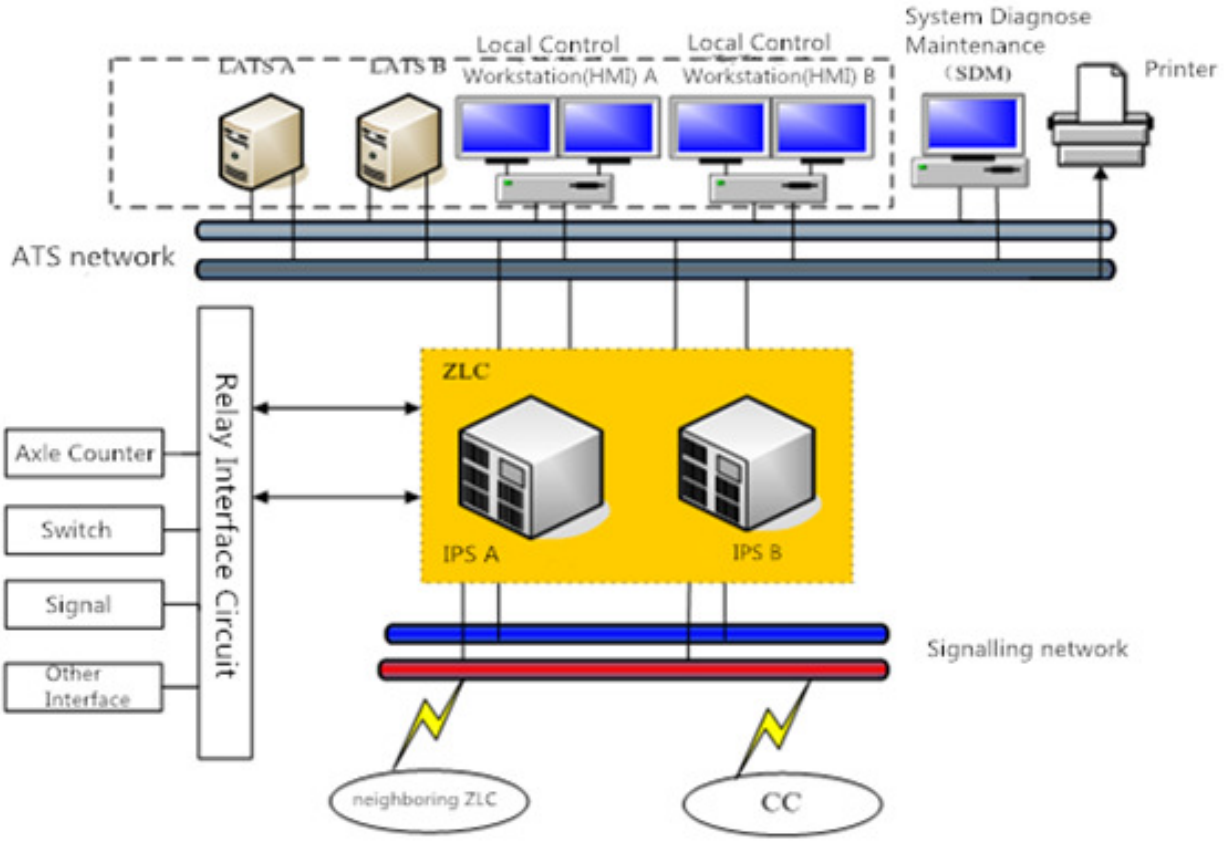


Figure 5. CBI System structure for a single mainline station

3.2. The ATS sub-system

Automatic Train Supervision (ATS) is a computer monitoring system with distribution form, which is mainly located in the operation control center, mainline equipment centralization stations, and depot.

The ATS monitors and displays the location of trains as reported from each train via the Data Communication System, automatically adjusts performance levels and dwell times, considering coasting mode, to maintain the schedule or headway, and provides for manual control of operations that includes the holding/release of one or all trains, establishment/removal of speed restrictions, and temporary zone closures/openings using data from the Zone Controller (ZC).

In **figure 6**, **[20]** it is shown how the ATS equipments are localized inside an Operations Control Center (OCC). OCC includes main central train control room, central signaling equipment control room, print and operation schedule rooms.

The central signaling equipment contains the main servers for the overall ATS system functions. It is connected to local ATS systems in each mainline station via a dedicated SDH (synchronous digital hierarchy) optical communication bus to exchange train tracking information and deliver ATS commands.

Central control room only contains train dispatcher workstations and a display panel. This is a place where train positions are displayed after tracking operation. Trains are dispatched according to the schedules from workstations.

1) Operation control center (OCC)

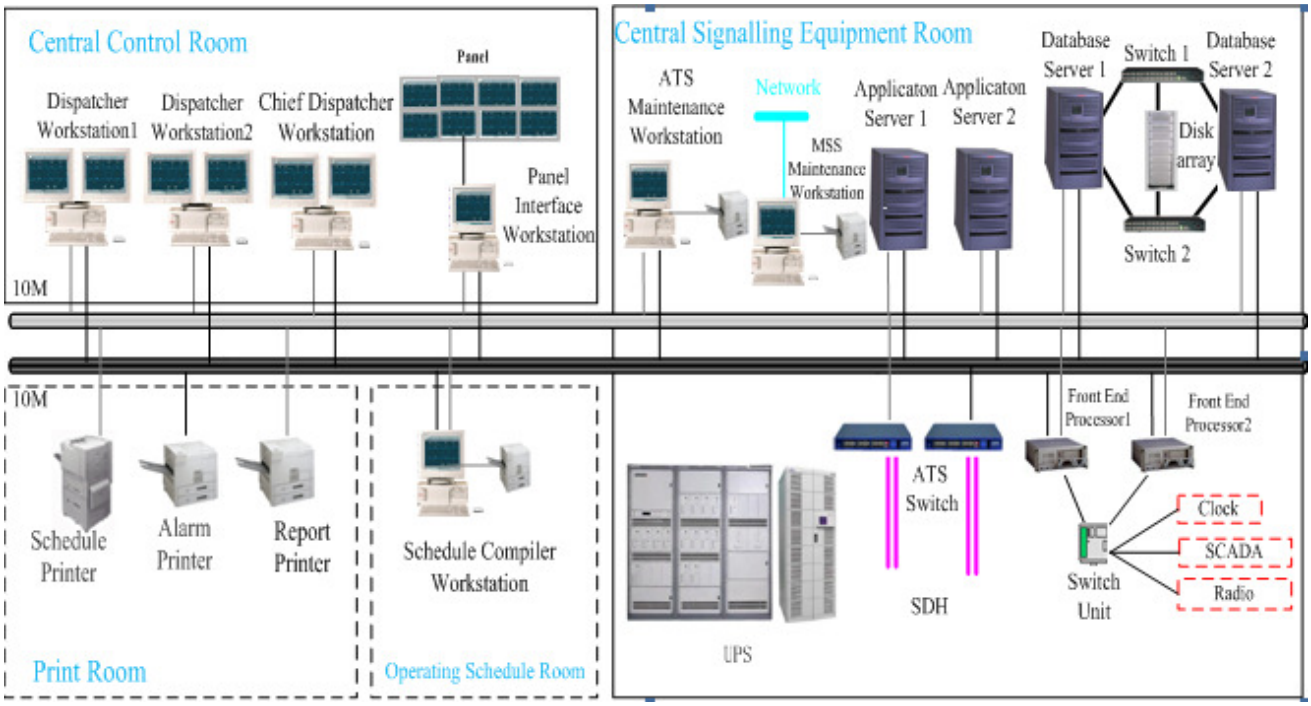


Figure 6. Architecture figure of operation control center ATS sub-system

2. Equipment centralization station

Equipment centralization stations are 8 main stations where the CBI system is configured. As shown in **Figure 7**,[20] In these stations there are local ATS (LATS servers) which are connected to the main ATS system through the optical bus and ATS switches. Also the status of wayside signaling devices is transferred to ATS system through the same path. From the workstations, if authorized, local ATS functions can be executed.

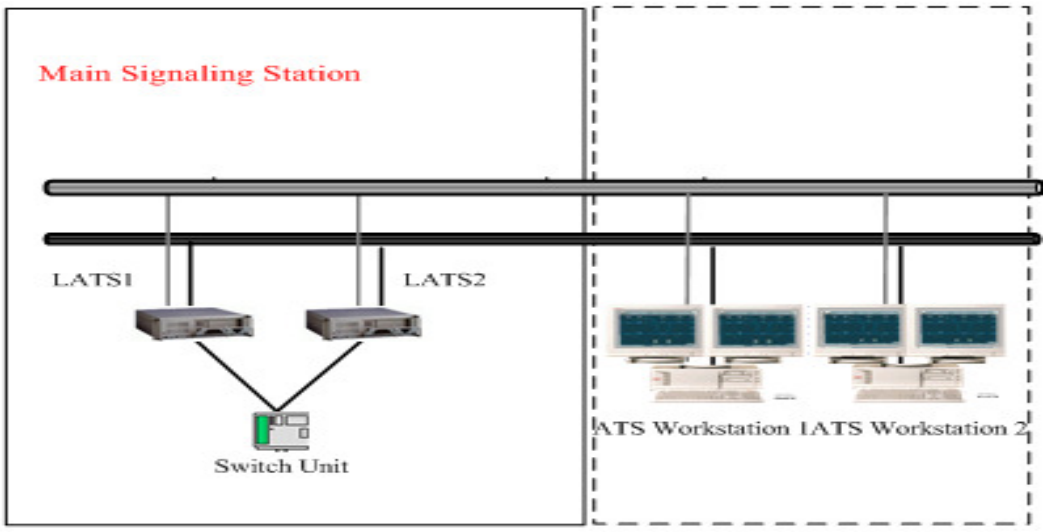


Figure 7.Architecture of main signaling stations ATS sub-system

3. Depot ATS configuration

Below in Figure 8 [20] the implementation of ATS system is a bit different from OCC. The signaling equipments are the same as previous few in number.

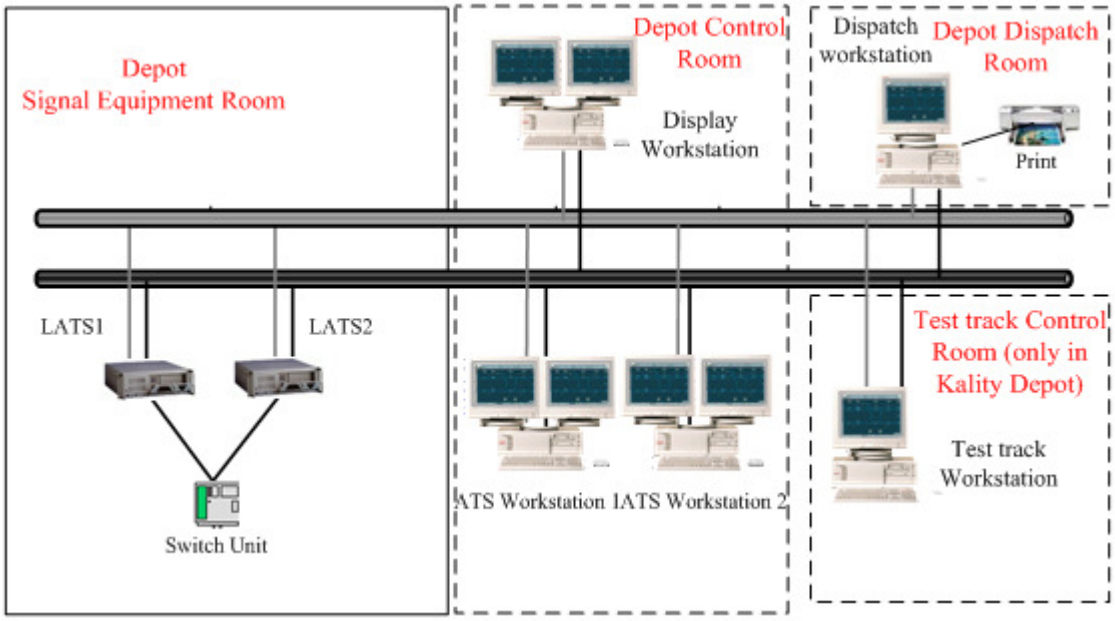


Figure 8. Ayat/Kality Depot ATS sub-system architecture

Basic functions of ATS subsystem

- Workstation authorization management
  - ✓ This authorization management ensures the reliability and uniqueness of the outputting order, which can avoid that the same function to one object are operated on two workstations simultaneously
- HMI (central dispatcher and local operator)
  - ✓ This function is used to supervise signal equipment present state and train state of the whole line, such as track layout, station control state, equipment working state, etc.
- Signal equipment management
  - ✓ ATS subsystem can supervise and control all the mainline stations signal equipments and supervise depot signal equipments
- Route operation
- Train tracking and display

3.3. The IATP sub-system

The IATP subsystem is based on trackside equipment and on on-board equipment [20]. Fig. 9 shows on-board signaling equipments. It includes the continuous communication using wireless system and an intermittent communication devices. Both systems are with a redundant structure. The intermittent communication devices are used to pick data from ballises installed on the track.

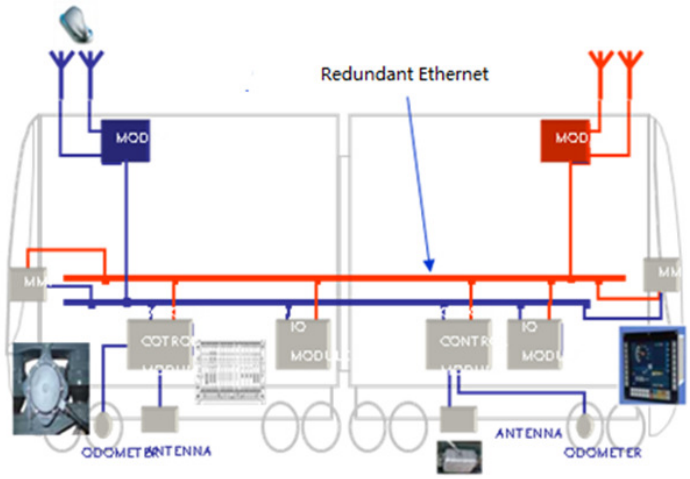


Figure 9. Onboard controller structure

IATP subsystem is a vital equipment for ensuring train safety operation, which conform to faulty-safety principle.

IATP subsystem will protect the train from overspeed and full protection according to the switch position and the train position ahead and etc, and ensure the safety travelling interval between train with interlocking system.

IATP subsystem includes the main functions as below:

- Stop the train before restrictive signal
- Over-speed protection
- Overrun red light protection
- Rollback protection
- Emergency brake control
- Train door supervision
- PSR control according to the track.

On-board display including:

- Train actual speed
- Target speed
- Target distance
- Driving mode
- Emergency brake application

3.4. MSS subsystem

MSS adopts three-tier architecture [20]:

- Center service layer: setting a suit of MSS server in Kality depot.
- MSS station layer: setting a suit of MSS station in each concentrator station (EW1,

EW7, EW16, EW20, EW22, NS27, NS10, NS6);

- MSS workstation layer: setting a suit of MSS workstations in Kality rolling stock depot and control center

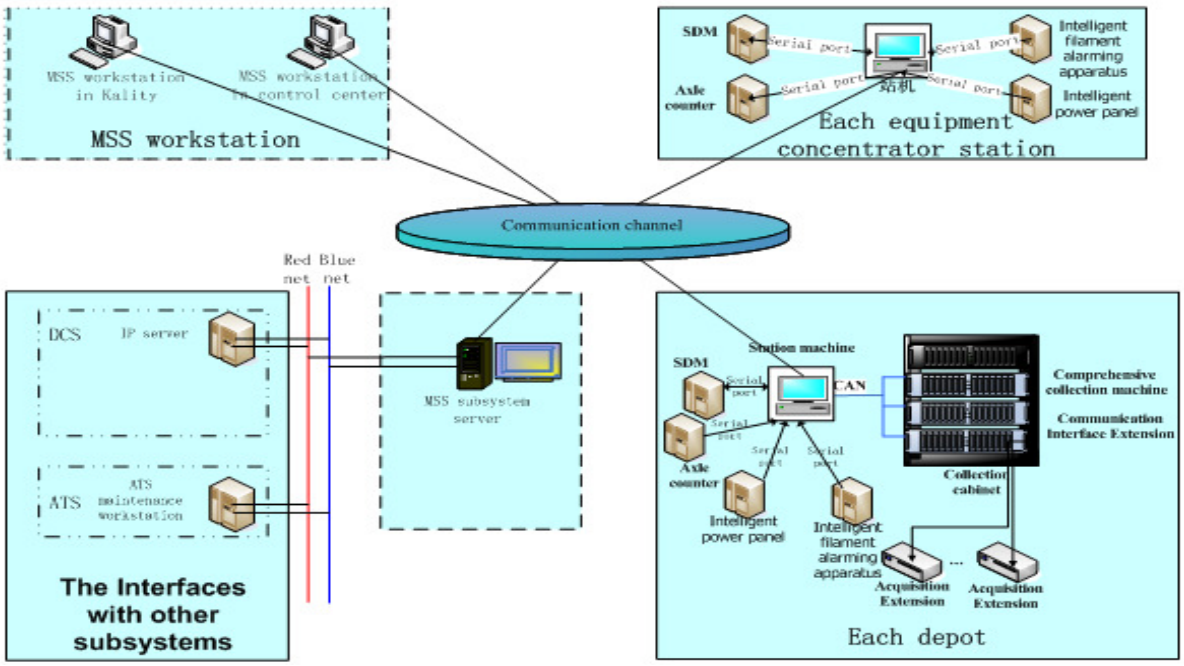


Figure 10. The overall structure of MSS signal subsystem

The main MSS function includes:

- Functional positioning of MSS is in local monitoring, fault diagnosis and remote alarm;
- MSS can complete the centralized alarm function for signal system equipment;
- ATS, IATP, CBI of main lines and depot, level crossing system equipment have the function of self monitoring and alarming, ATS, ATP and CBI can position to the replaceable unit.
- Monitoring and alarm equipment of MSS has the functions of receiving, statistic and processing the signal systems, and it can generate alarms of all signaling devices, daily tables, weekly tables and monthly tables of each individual device.

3.5. The DCS subsystem

According to communication way and function, DCS subsystem is composed of the following 3 parts:

- Wired network, mainly composed of Ethernet Switches.
- Wireless network, composed of:
  - Trackside Wireless Network: main equipments are trackside APs, Power Splitter and directional antenna. The trackside wireless network equipments are deployed before the signals with IATP function, to fulfill the communication requirements of ATP function;
  - On board Wireless Network: main equipments are on board radio modem and antenna.
- Network Management System: NMS IP.

Signaling Safety related data of AA-LRT

Below are quantitative data taken from the signaling system design [20].

1) Availability

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

2) Safety

- The safety integrity level (SIL) of safety-related equipment in the signaling system reaches the level 4 .
  - International Electromechanical Commission's (IEC) standard IEC 61508 specifies SIL assignment. SIL is defined as a relative level of risk-reduction provided by a safety function or to specify a target level of risk reduction. SIL is a measurement of performance required for a safety instrumented function. SIL assignment has only 4 levels and SIL level 4 is the highest safety integrity

Subsystem	Safety integrity level
IATP system	Level 4
CBI system of mainline and depot	Level 4
Train position detection equipment	Level 4

Table 1 . Safety Integrity Levels for signaling equipments

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

3) Reliability

- ATS system: MTBF$\geq 2.0\times 10^5$ 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 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;
- 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

Chapter Four

Failure Model of AA-LRT signaling system

In the previous chapters, failure modeling process and signaling system of AA-LRT are discussed in detail. In this section, the models for main subsystems and local failure data of components are presented.

Assumptions and details in the modeling and analysis

A railway signaling system is a large and basic subsystem of a railway system. It is the result of interactions of many highly sensitive electronic devices. Hence, too many failures can be pointed out and studied. But, most simple failures can be easily handled by employing equipments with high safety standard. Therefore, it is of great importance to study the ones which can be hazardous or catastrophic causing the overall system failure and put the operation at risk.

The failure analysis here is component based safety analysis using HiP-HOPS tools and Matlab. And the failure models encompasses functional interaction of equipments from **each signaling sub-system** within **only a single mainline station or depot.**

The modeling phase requires understanding of the whole system operation and signaling equipments specific functions. The general topology and equipments localization of signaling system design of AA-LRT is the major input to the modeling phase. This will lead to models of subsystems on Simulink as shown in **Figures 11, 12 and 13.**

In this study, failures related to power loss, manual errors, communication and power cable damage, station to station communication problems, Train onboard signaling equipments etc. are not covered. It is not because these failures are hazardous rather to limit the complexity of the analysis. For further research, this study can be a baseline. Therefore, it is assumed that the system perfectly addresses them.

For each component, failure modes, output deviations and input failures are studied. And hazardous failures which propagates in the system are tabulated and presented in the final fault-tree of the given system. Tables 2 and 3, shows the studied failure modes for CBI and ATS system equipments

4.1. CBI system indoor and outdoor equipments

1. ILOCK 2*2OO2 CBI system
   - ✓ Intelligent safety type double 2-vote-2 computer interlock system platform
   - ✓ Compared with prior art, this provides a novel safe hardware platform providing high safety, high reliability, high stability, high operational speed and easy expansion.
   - ✓ MTBF $\geq 2.0\times10^5$h.

2. System maintenance workstation (SDM)
3. CBI and ATS Ethernet switches
4. Relay interfacing unit
5. SDM
6. MSS
7. Axle counter
8. Signal
9. Turnout

COMPONENT or SUBYSTEM	BASISC EVENTS or INTERNAL FAILURES	INPUT FAILURES with their failure classes
ILOCK 2*2OO2 CBI SYSTEM	✓ Failure to provide correct route setup (Logic Error) ✓ Failure to collect and drive relevant wayside equipments	✓ No data received from signal machine, axle counter or switch machine [Omission] ✓ Erroneous data from axle counter [Value failure]
HMI WORKSTATION IPC-610H	✓ Failure to show station indication obtained from CBI system (including signal, switch, failure alarms)	✓ Omission of route related data from zone logic computer as an input to HMI ✓ Commission failure from ZLCs

CBI & ATS ETHERNET SWITCHES H3C_S3600V2-28TP-EI : Three level electrical switches	✓ No failure modes available	✓ Input data absence or wrong information
RELAY INTERFACING UNIT CASCO	✓ Relay contact failures	✓ Omission of data from signal, axle counter or turnout (switch machine) ✓ Value error from axle counter
SDM and MSS workstations and Maintenance Servers IPC-610H HP Workstation z620 HP DL388p Gen8	✓ MSS server to station MSS workstation communication failure	✓ No system failure related data received at inputs, [Omission] ✓ Wrong failure information and interpretation, [Commission]
AXLE COUNTER Frauscher	✓ Wheel sensor failure ✓ Evaluation board inconsistency ✓ delay	✓ RESET command failure in case flushing AC count value
SIGNAL MACHINE	✓ LEDs failure	✓ Omission of signal display commands
SWITCH MACHINE	✓ Switch mechanical failure, (stuck at a position or slowness of shifting) ✓ Or switch motor problem	✓ Omission of Switch set signal ✓ Wrong switch position command [value failure]

Table 2. CBI system equipments failure modes and catagorization

In Figure 11, failure propagation model of CBI system for a main station is modeled on Simulink. Here, some components such as switch machine enclose many equipments. For the modeling simplification, these components are represented as a single block in the models. Thus, input-output failures can be defined for the block. The same is done for the other signaling subsystems (ATS, IATP) as shown in Figures 12 and 13.

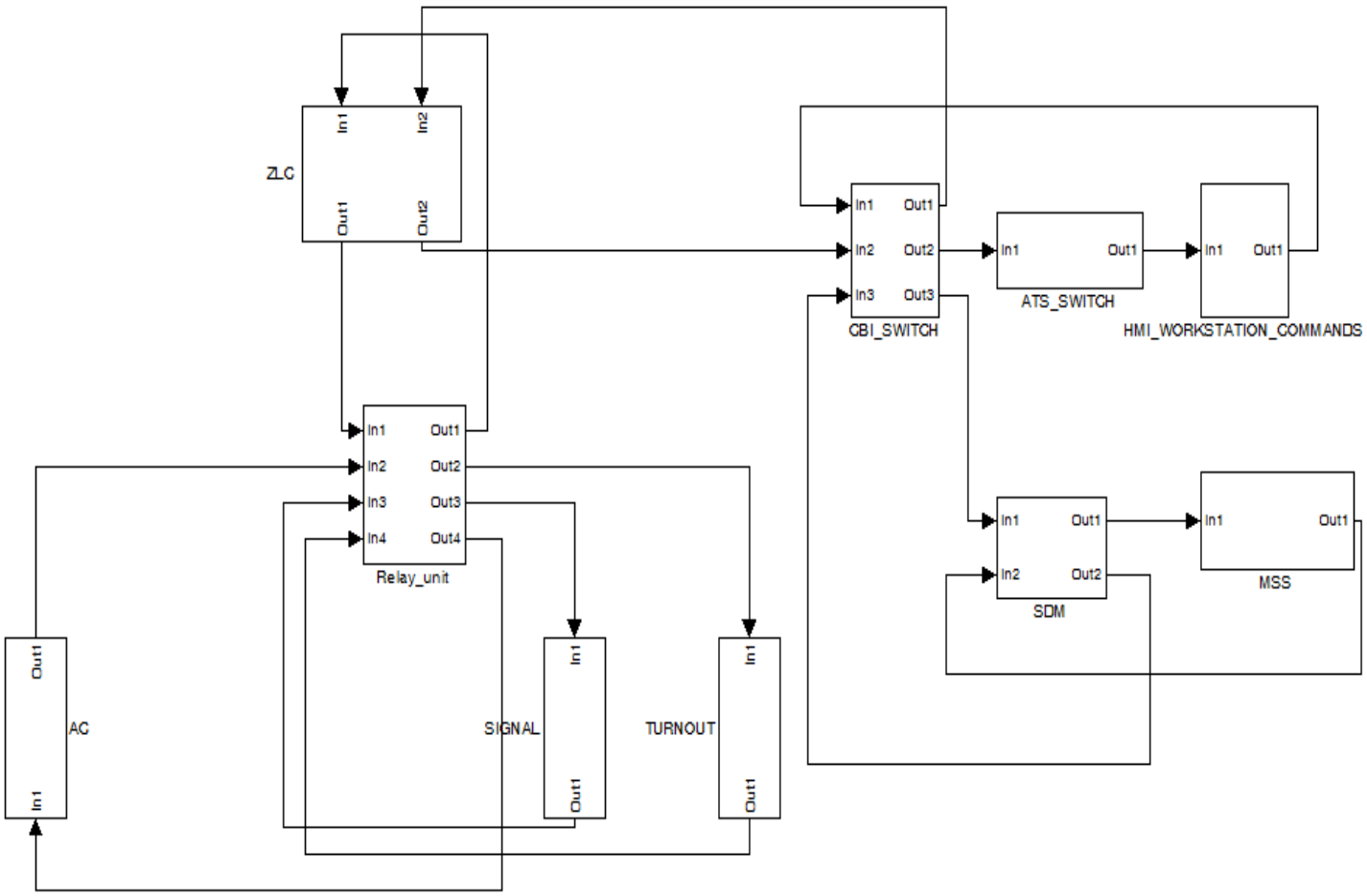


Figure 11. Functional structure and failure propagation model of CBI and MSS system within a single Mainline Station (indoor and outdoor equipments)

4.2. ATS system Mainline-station and OCC equipment configuration

COMPONENT or SUBYSTEM	BASISC EVENTS or INTERNAL FAILURES	INPUT FAILURES with their failure classes
ATS SERVER (application & database) HP ProLiant DL 580 G7	✓ Software error ✓ Viruses ✓ ATS functions incorrect operations	
ATS WORKSTATION	✓ Failure to show station train schedule and history	✓ Input control command error

	✓ Failure to show the system equipment state, track layout equipment state, time, alarm and etc, ✓ Unable to run operations relevant to track layout like interlocking control, train running control user responsibility and authorization, report and etc.	
LOCAL HMI WORKSTATION	✓ Failure to show station indication obtained from CBI system (including signal, switch, failure alarms) ✓ Interlocking control failure	✓ Omission of route related data from zone logic computer as an input to HMI ✓ Commission failure from ZLCs
ATS & CBI ETHERNET SWITCHES H3C_S3600V2-28TP-EI : Three level electrical switches	✓ No failure data	✓ No data present at inputs or wrong data input
OPTICAL SWITCHES	✓ Light - electric conversion interface failures	✓ Wrong data from CBI
LOCAL ATS SERVERS (LATS) LiRC-2	✓ Interlocking controlfailure ✓ Track indication failure	✓ No control data to change control mode
SDM and MSS workstations and Maintenance Servers IPC-610H HP Workstation z620 HP DL388p Gen8	✓ MSS server to station MSS workstation communication failure	✓ No system failure related data received at inputs, [Omission] ✓ Wrong failure information and interpretation, [Commission]

Table 3. ATS system equipments failure modes and catagorization

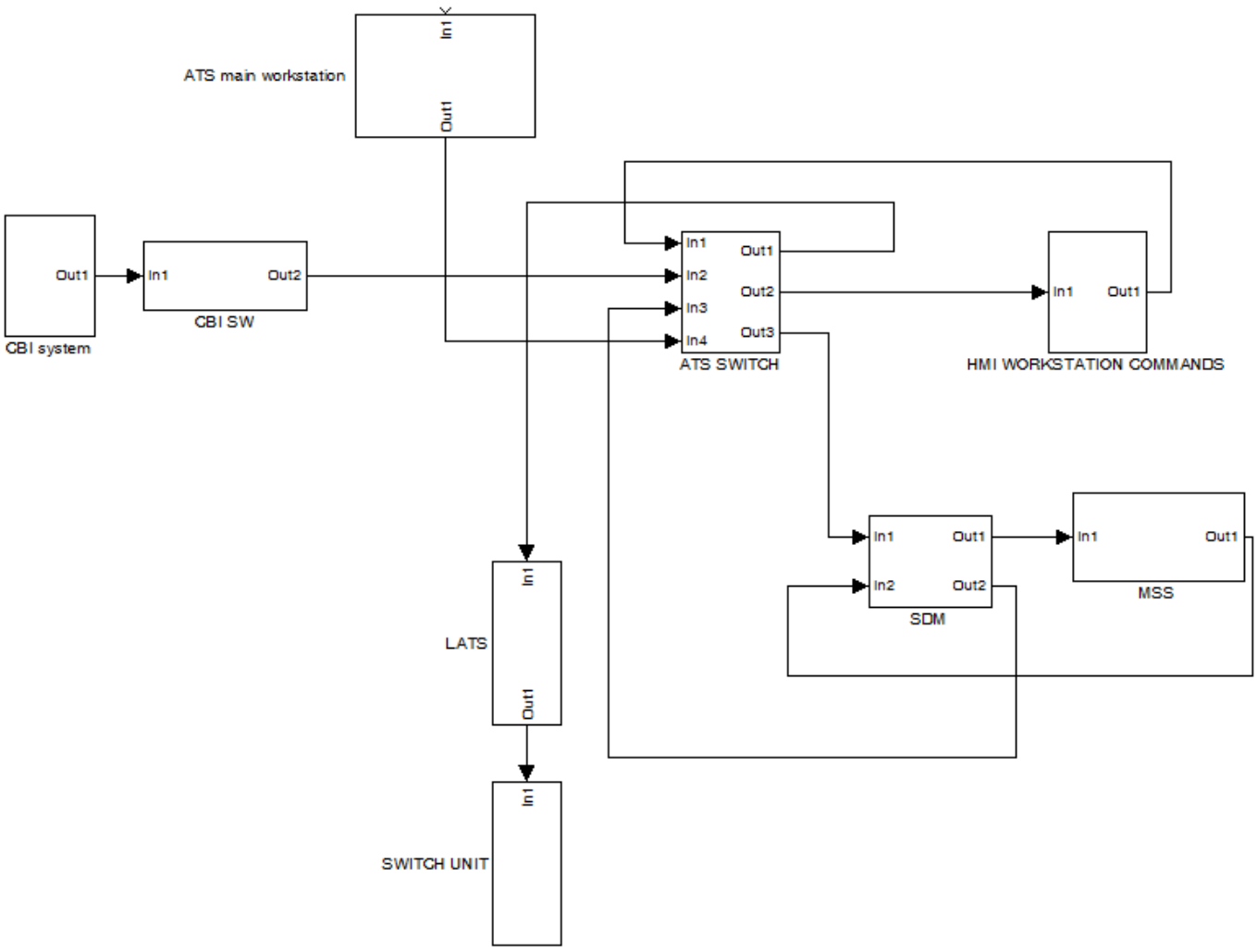


Figure 12. Functional interconnection and failure propagation model of mainline station ATS system

4.3. IATP system

The IATP subsystem equipment localization is classified as; on-board equipments configuration, trackside equipments and configuration. In this section only trackside equipments and functional flow is modeled.

The IATP subsystem is based on trackside equipment and on on-board equipment

Trackside equipment includes:

- Beacon (Ballise)
- LEU (Line Encoder Unit or Line side Electronics Unit)
- Trackside radio equipment

On-board equipment includes

- Carbone controller
- Odometer
- Beacon antenna
- DMI
- On-board radio equipment
- On-board switch

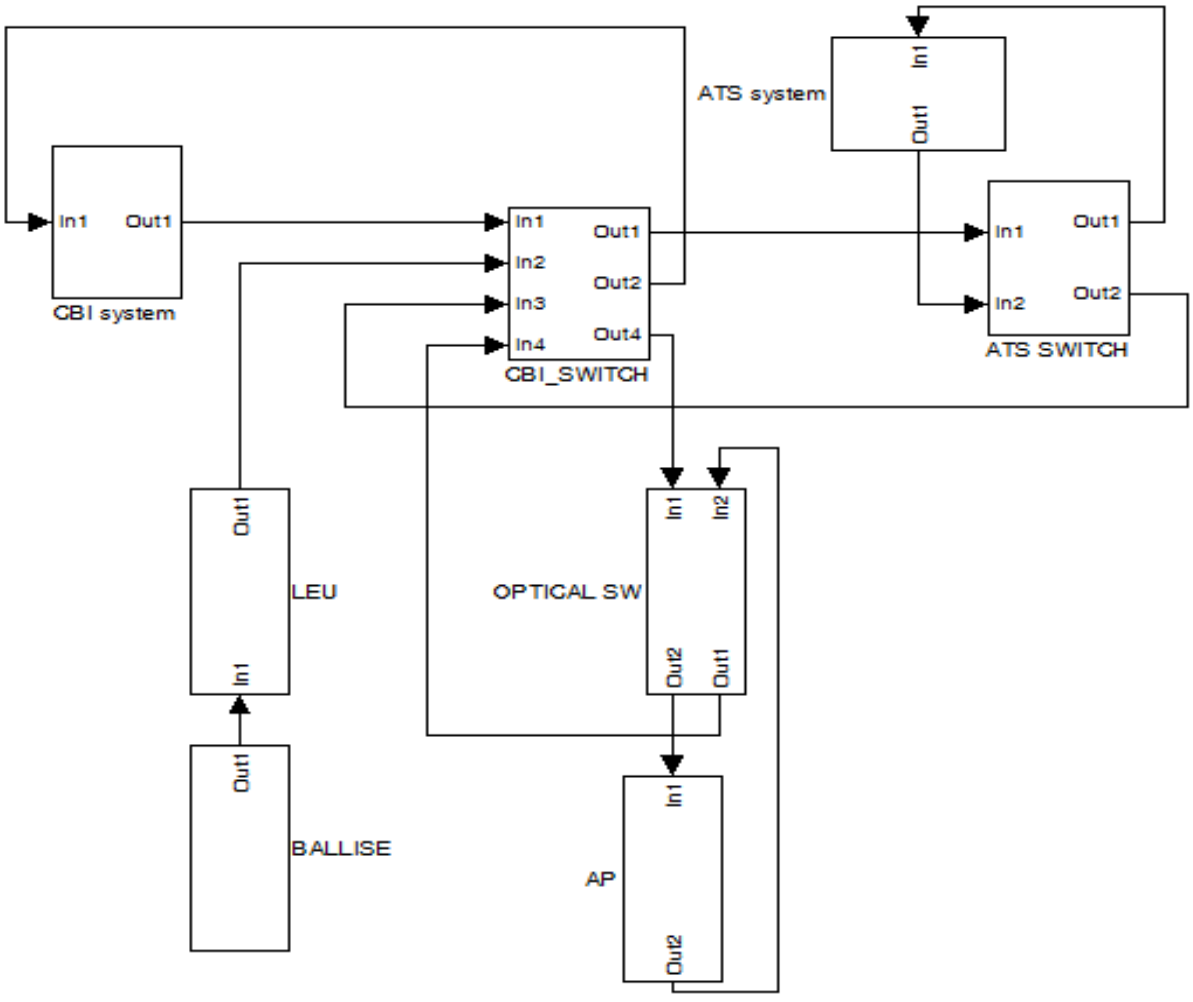


Figure 13. Trackside and indoor connection of IATP sys, its failure propagation model

Chapter Five

Simulation results and Discussions

This chapter presents the results and captures of simulation of failure models which are discussed in Chapter 4. Descriptions of results is stated here and in the succeeding chapter

Simulations are done with the Help of HiP-HOPS tool taking models from Matlab Simulink. Tests are done by defining a top level hazard and a fault tree is generated as a result showing the propagation of a failure for the event. According to this model based safety analysis, once components failure data is added to the models, every hazard fault tree can be automatically generated. The fault trees here are obtained after solving minimum cutsets.

Quantitative results can also be generated by entering components MTTF and MTTR **[21]**. In this section unavailability of few components are calculated by using the simple formula described in chapter 2.

1. CBI sub-system for a single mainline station- failure model fault tree generation

To generate fault trees showing the propagation of failure from originating device to the top level, defining hazards with specified SIL is necessary. Then with the aid of HiP-HOPS tools this hazard is feed to the Simulink model. Figure 14, shows fault tree corresponding to a SWITCH failure hazard. From bottom to top it displays possible causes for this event.

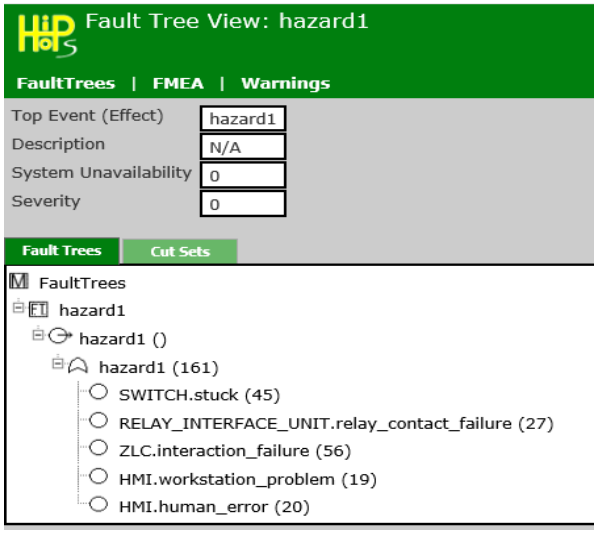


Figure 14. fault tree for switch failure hazard

Hazard definitions on MATLAB is as shown in the figure below. It shows a failure expression defined as Omission output for a switch device, which is a case when the switch device fails to execute the switching task.

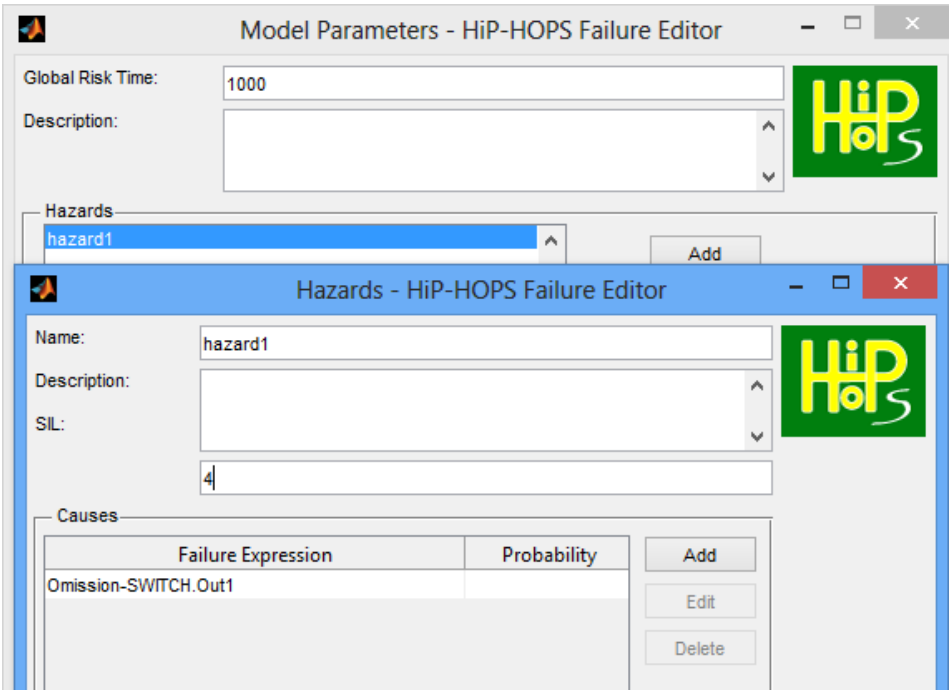


Figure 15.Hazard definition for the previous Fault Tree

Failure propagation related to Relay interface unit output failure is shown in Figure 16 below.

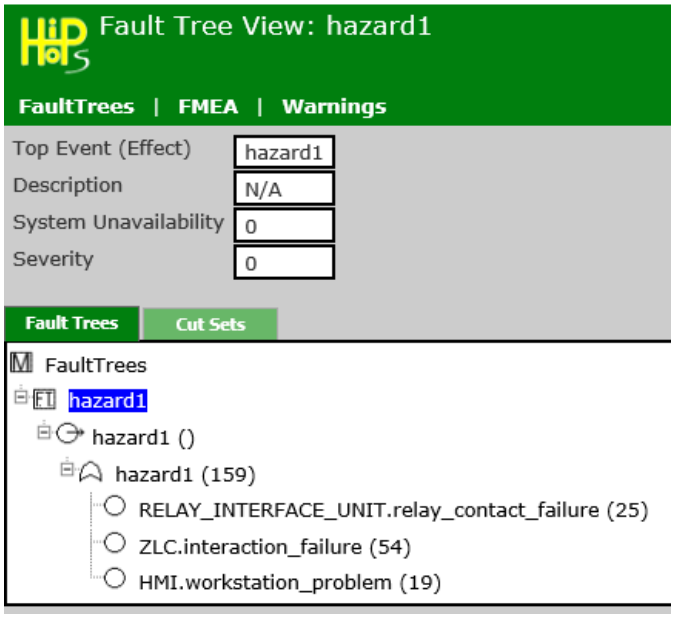


Figure 16. Fault Tree for Relay interface unit output failure.

Figure 17, displays the scenario of the signal device not showing the signaling lights.

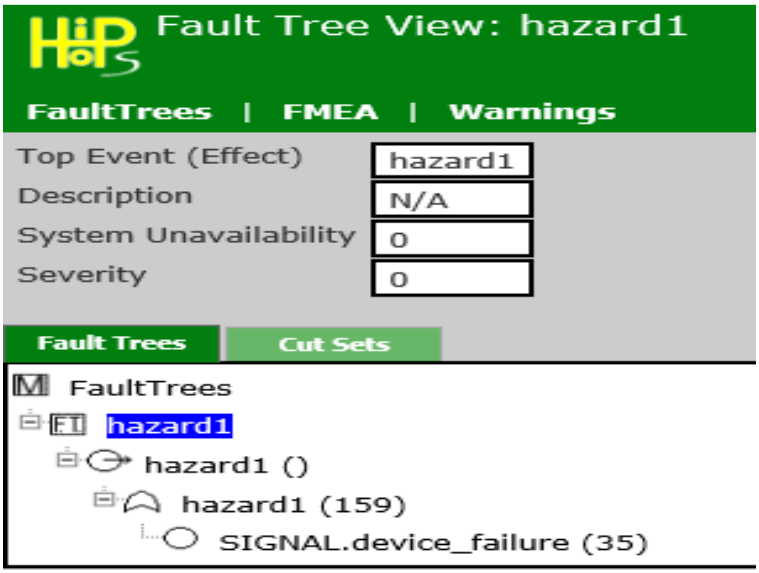


Figure 17. fault tree for signal device failure

Zone logic computer failure to provide correct route operations is as shown in figure 18. Here possible causes are no route set commands from HMI or internal failure of ZLC itself.

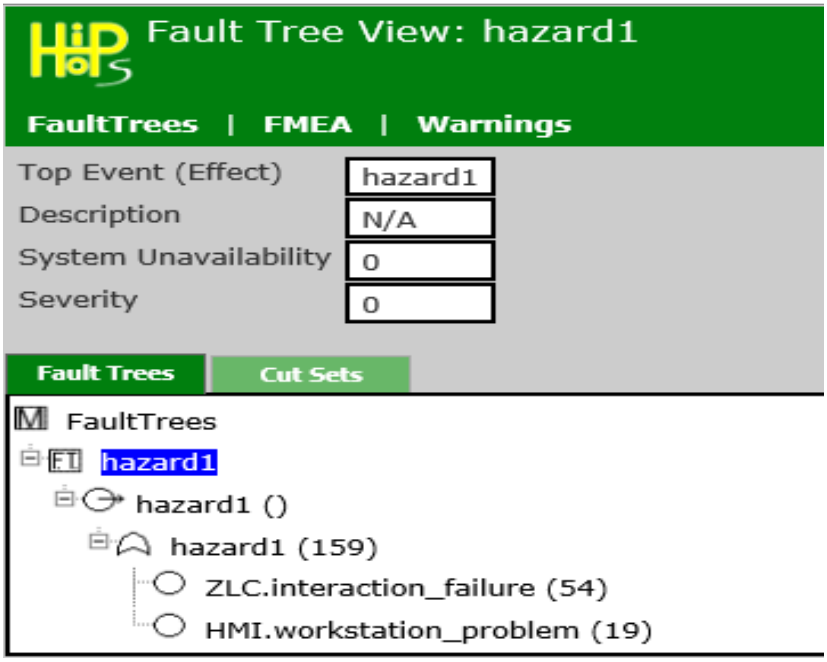


Figure 18. fault tree related to ZLC failure

The above figures are fault tree display mode in HiP-HOPS analysis tool. Another display mode is failure modes and effects analysis view. In this mode, all failures with corresponding severity value (if internal failures are specified with quantitative values such as MTTF) is shown. See figure 17.

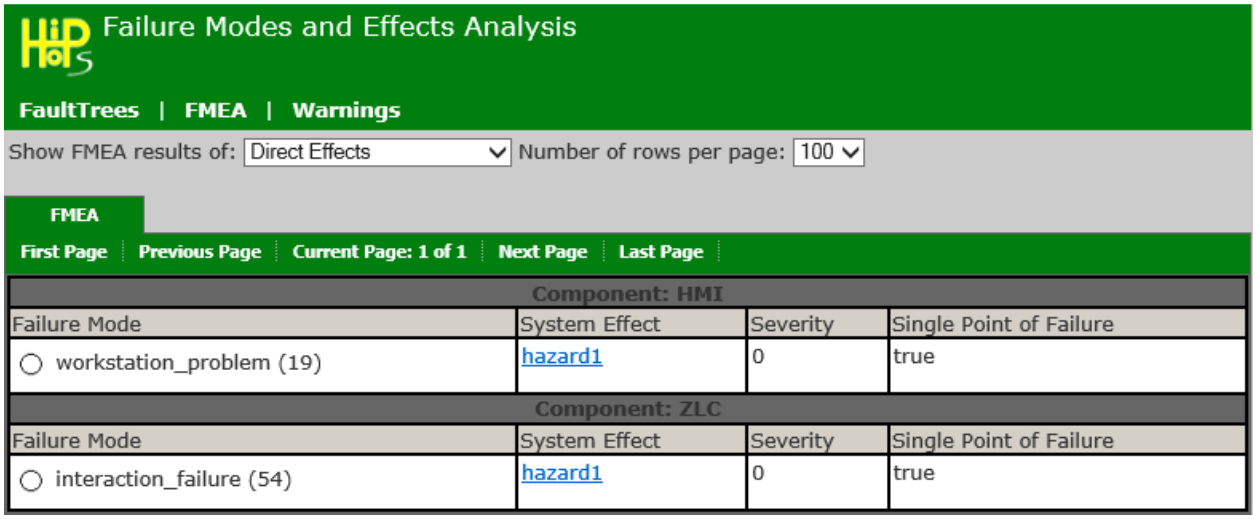


Figure 19. Failure Mode and Effects Analysis view of ZLC failure

2. ATS sub-system for a single mainline station- failure model fault tree generation with hazard definitions

Local ATS system failure (no output) is as shown in the fault tree below. As it is displayed, possible causes for this failure are only its internal failures.

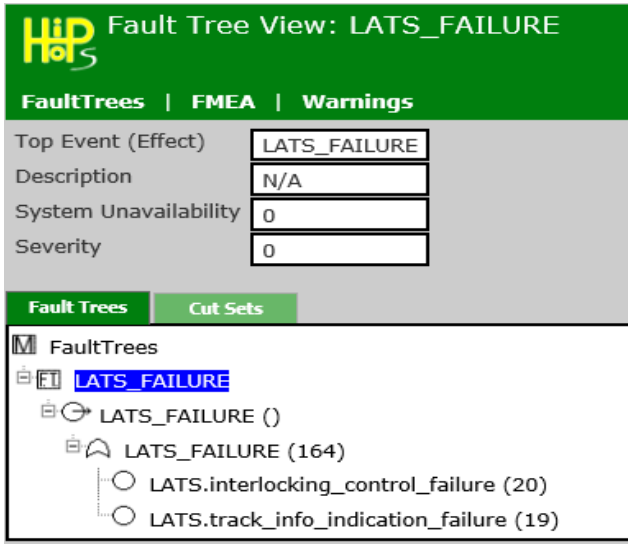


Figure 20. LATS equipment failure hazard FTA

Other subsystems Fault Trees are also done in such a way after defining each components failure modes in the Simulink models

Generally, after identifying each components failures as it was done in the previous chapter (as shown in tables 11, 12 and 13) and defining the failure modes for all components in the overall signaling system by employing HiP-HOPS tools, failure propagation throughout the complex signaling system can be illustrated. The above FTAs can be used for system maintenance easy operation.

Unavailability of components of some components

- Station equipments: most station signaling equipments have the following Mean Time To Failure and Mean Time To Repair rates as obtained from CREC signaling system design.
  - ✓ MTTR = 30 Min = 0.5Hr. , MTTF = 2 x 10^5Hr.

By using equation (2.1), the unavailability of basic events for the components can be calculated as;

$$\lambda = \frac{1}{MTTF} = \frac{1}{200000} = 5x10exp - 6$$

$$\mu = \frac{1}{MTTR} = \frac{1}{0.5} = 2\ /1\text{Hr.}$$

$$u = \frac{\lambda}{\lambda+\mu} * (1 - e^{-(\lambda+\mu)t}) \approx 2.49\text{e-}6$$

The same result will be obtained if all failure rates are specified for all failure modes in the Simulink models.

Chapter Six

Conclusion, Recommendation and Suggestion for future work

CONCLUSION

Railway signaling system generally is complex. Therefore, instead of direct implementation and troubleshooting from the beginning it is much easier to once define every equipment, components and subsystems failure data in a model. And test the system with hazards to find how failure propagates and which source is the root cause. This is the basic concern of model based safety analysis methods.

For the design of AA-LRT signaling system, a model based failure analysis is not done and failure propagation and fault trees are not generated. But safety analysis is done using classical methods such as PHA and HAZOP. If modern methods were used it is also possible to calculate and determine each basic events unavailability by using equipments MTTF and MTTR values.

In this thesis, a study is done to generate fault trees corresponding to few subsystems of signaling system of AA-LRT. But, absence of significant data related to failure modes for the equipments used in the design, makes the analysis process difficult. Hence, a number of assumptions and study based data are taken into consideration.

To generalize about the safety of the system design, the overall signaling system design needs to be modeled perfectly with each equipments failure modes. Most equipments used in the design belong to Chinese Manufacturers and very important data about components cannot be simply obtained from internet sources.

RECOMMENDATION

Each equipment selection and system design was based on acceptable standards. And safety integrity level for all Major Subsystem is SIL 4. Based on this data the systems safety can be easily identified. But it will be more essential if the general system failure model is done perfectly, which will be helpful in case of Maintenance, future operation troubleshooting, and determining the system life.

Using HiP-HOPS safety analysis methods a number of systems are modeled and tested for hazardous failures. These systems are fail safe and determined after being implemented. Using this analysis for AA-LRT electrical and also mechanical systems is appropriate and advantageous.

In the future, this study can be expanded to include other subsystems, every component and their failure modes. This will be put in a database and can be assessed every time when a hazard is probable to occur.

References

[1] J. Glancey, Failure Analysis Methods What, Why and How, Special Topics in Design, Spring 2006.

[2] FMEA, http://www.wikipedia.org/wiki/Failure_Modes_and_Effects_Analysis

[3] A model-based framework for the safety analysis of computer-based railway signalling systems, R. Niu & T. Tang, research paper, state key laboratory of rail traffic control and safety, Beijing Jiao Tong University, China

[4] R.J. Mikulak and R.E. McDermott, the basics of FMEA, 2nd edition, CRC Press

[5] Matthias Gudemann & Frank Ortmeier, Probabilistic Model Based Safety Analysis, Otto-von-Guericke University of Magdegurg, research paper, p 114

[6] Xiaocheng Ge, Richard F. Paige, and John A. McDermid, Probabilistic Failure Propagation and Transformation Analysis, research paper, University of York, UK

[7]. Lars Grunske, Bernhard Kaiser, and Yiannis Papadopoulos, Model-Driven Safety Evaluation with State-Event-Based component failure annotations, School of Information Technology and Electrical Engineering ITEE, University of Queensland, Australia

[8] Jong-Gyu Hwang and Hyun-Jeong Jo, Hazard Identification of Railway Signaling System Using PHA and HAZOP Methods, On-demand Transit Research Team, Korea Railroad Research Institute, International Journal of Automation and power Engineering (IJAPE), February 2013, V2 Issue 2

[9] Engineering Failure Analysis, Yiannis Papadopoulos, Martin Walker, David Parker, journal 18(2011), p590-608

[10] Papadopoulos YI, McDermid JA. Hierarchically performed hazard origin and propagation studies. In: 18th International conference in computer safety,

reliability and security, Toulouse, France; 1999. p. 139–52.

[11] ITI Gmbh. SimulationX 3; 2010. <http://www.simulationx.com>.

[12] Rausand M, Oien K. The basic concepts of failure analysis. Reliab Eng Syst Safety 1996;53:73–83.

[13] HiP-HOPS automated fault-tree, FMEA and optimization tool, www.hiphops.net

[14] Papadopoulos, Y., Maruhn M.: Model-based Automated Synthesis of Fault Trees from Simulink models, Int'l Conf. on Dependable Systems and Networks, (2001), pp. 77-82

[15] Grante C, Andersson J. Optimisation of design specifications for mechatronic systems. Res Eng Des 2003;14(4):224–35.

[16] Sharvia S, Papadopoulos YI. Non-coherent modelling in compositional safety analysis. In: IFAC 17th world congress, Seoul, South Korea; 2008.

[17] Papadopoulos, Y., McDermid, J. A.: Hierarchically Performed Hazard Origin and Propagation Studies, SAFECOMP '99, 18th Int. Conf. on Computer Safety, Reliability and Security, Toulouse, LNCS, 1698 (1999) 139-152

[18] Deb K. Evolutionary algorithms for multi-criterion optimisation in engineering design. Evolutionary algorithms in engineering and computer science. John Wiley & Sons; 1999. p. 135–61.

[19] Addis Ababa E-W & N-S (Phase I) Light Rail Transit Project Preliminary Design EPC(ET/ERC/CREC/0901), China Railway Group Limited (CREC) Chapter XIV Signaling System, V1

[20] Signaling System detailed design, Addis Ababa E-W & N-S (Phase I) Light Rail Transit Project, Part I Technical Specification, Version: ET/AA/LRT/CREC/EPC/DD/XH-01/A

[21] Hamann R, Uhlig A, Papadopoulos Y, Rüde E, Grätz U, Walker M, et al. Semi-automatic failure analysis based on simulation models, paper no. In:OMAE2008-57256, proceeding OMAE 2008, Estoril, Portugal; 2008.

APPENDIX

A. TERMS AND DEFINITIONS

Overspeed protection	The onboard ATP system guarantees train running under safety speed restriction.
Train detection device	Train detection device is a device installed on the track on which the train runs in order to detecte if a train occupies a block of the line.
Train identification	Train identification is a method to indentify train by information as ‘train ID’, ‘destination area’, etc. for the purpose of route setting and dispatch.
Failure	Failure is a state when system fails to complete required function.
Out of operation	The system loses the ability to complete required function.
Failure rate	Failure rate of a component refers to the ratio of the total amount of the independent component failure devided by the operation hour of all equipment.
Mean Time Between Failures(MTBF)	Mean time between failure is the elapsed time between two adjacent failures (including to immediate failure) of a device during operation.
Mean time between right side failure(MTBRSF)	Mean time between right side failure is the elapsed time between two adjacent failures which lead to the right side.
Mean time between wrong side failure(MTBWSF)	Mean time between wrong side failure is the elapsed time between two adjacent failures which lead to the wrong side.
Failure complete recovery time	Failure complete recovery time is the duration from the moment a fault is reported to the moment the faulty equipment fully recovers its design features (maintance job is completely finished).
Failure recovery time	Failure recovery time is the duration from the moment maintainance personnel reaches the faulty equipment to the moment the faulty equipment fully recovers its design features (maintainance job is completely finished).
Safety	Safety is the capibility to guarantee the safety of traffic, human life and equipment. Safety is characterized as the probability of system to maintain safety features at a certain time.
Reliability	Reliability is the capibility of a product to complete required function under specified conditions and within specified time.
Availability	For a repairable product, availability is the possibility of maintaining its function in a certain moment or the ratio of maintaining its function during a certain period. Availibity is a intergrated indicator of product reliability, maintainability and maintainance assurance.

Maintainability	When product is under prescript condition of usage and is maintained according to prescript procedure and means, Maintainability is the capability of product to recover its performance for the purpose of maintaining the product at normal operation condition or restoring product failure and defect.
Life cycle	Life cycle is the minimal time period that regular operation of a project is guaranteed under normal maintaince condition.
Safety assessment	Safety assessment is a process to evaluate whether system hazards can be reduced to an acceptable level.