Department of Advanced Energy
Transdisciplinary Sciences
Graduate School of Frontier Sciences
The University of Tokyo

2020

Master's Thesis

New Safety Analysis Method as a Combination of STAMP & FTA
(STAMP と FTA を組み合わせた新しい安全性解析手法)

Submitted July 22, 2020
Adviser: Project Professor Takeshi MIZUMA

47186146　Upvinder SINGH

Acknowledgement

First & foremost, I would like to thank God, The Almighty in whose omnipresence & blessings I started, conducted & completed my work successfully.

I consider myself fortunate enough for getting an opportunity to work under the kind guidance and supervision of Prof. Takeshi MIZUMA, who with his dynamic personality & immense depth of knowledge not only devoted generous efforts to provide excellent advice but also remained the abundant source of knowledge, encouragement & constructive criticism throughout the study period.

I am very thankful to prof Hideo NAKAMURA, who held regular discussions on various topic related to the field of my study. His vast knowledge helped me in to get an in-depth insight into my research. I am profoundly grateful to Ms Yukari KATAGIRI for helping in my all kind of problems and special thanks for her support in learning Japanese.

I extend my special gratitude to prof Hiroyuki OHSAKI for his valuable suggestion during lab meetings and for allowing me to use the lab resources. I am very thankful to assistant prof Yutaka TERAO for his support in all kind of situation during the last two and a half years. Further, I extend my sincere thanks to all the member of prof. Mizuma laboratory and prof. Ohsaki laboratory for their continuous support and encouragement.

I am very thankful to all the faculty members of Advanced energy department and all other departments of GSFS, whose cooperation made my work successful.

I express my heartful thanks to the MEXT for supporting my studies in Japan without which this wouldn't have been possible. I express my sincere thanks to the Ministry of Railways for providing this opportunity to me.

Last but not the least, I am indebted to my late parents, whose untiring efforts made me capable enough to reach this point. I show my heartful thanks to my beloved wife, Dr Sheetal Singh and my whole family whose continuous motivation and emotional support provided me with enough strength to complete this endeavour.

Abstract

The safety evaluation method used for railway industries, i.e. FTA has limitations concerning time-delay hazard and completeness of fault tree and missing of hazardous events. STAMP has the capability of covering all the risks, including time-delay hazards. However, it cannot do the quantitative analysis, and that makes it not compliant to international standard IEC 62278 and EN 50126, which require qualitative and quantitative analysis of all safety-critical systems.

This study proposes a new method as a combination of STAMP and FTA, in which STAMP is used for qualitative analysis and fault tree is constructed taking the input from the STAMP table. FTA quantitative analysis is applied in the last. Both methods compensate for the limitations of each other, and the proposed method covers all kind of hazards, including the time-delay hazard. The procedure of the proposed method ensures the completes of fault tree without skipping any hazardous event. Also, its quantitative analysis capabilities make it compliant to international standard. Moreover, its defined procedure makes it easier to analyse complex systems. This study covers the application of the proposed method on two target systems from the railway signalling industry.

Application of the proposed method on both the target system successfully demonstrated the superiority of the proposed method over the conventional method as both qualitatively and quantitatively. The case studies confirmed that the proposed method made the complete hazard prediction by covering all the hazards identified by the traditional method along with time-delay hazard. The result comparison from both methods showed that the proposed method could predict a higher number of hazard event than the conventional method. Also, the occurrence probability of the top hazard was higher in the case of the proposed method.

List of Acronyms

1. IEC International Electrotechnical commission.
2. EN European Norm.
3. FTA Fault Tree Analysis.
4. SFTA Software Fault Tree Analysis.
5. FMEA Failure Mode and Effect Analysis.
6. SFMEA Software Failure Mode and Effect Analysis.
7. STAMP System Theoretic Accident Model and Process.
8. STPA System Theoretic Process Analysis.

Table of Contents

List of Figures

List of Tables

1. Introduction

Railway signalling systems are safety-critical and need compliance to the international standards that include IEC (International Electrotechnical Commission) 62278 and EN (European Norm) 50126. This compliance needs both qualitative and quantitative safety analysis of each system. IEC 62278 mentions the use of FMEA (Failure Mode and Effect Analysis) and FTA (Fault Tree Analysis) safety analysis methods as both are capable of qualitative as well as quantitative analysis and comply to the standard's requirements. However, both approaches are quite old and have their limitations.

FTA is being used for a very long time and can do both qualitative and quantitative analysis as per the standard's requirement. However, it often misses the events leading to the fatal failure due to absence of any systematic procedure; and analysis result depends entirely on the analyst's skills only. Though it can be reviewed and updated later, on the occurrence of any incident, yet the drawback of missing events in new systems, raises the concerns about its effectiveness, especially in case of time-series failure events where FTA has remained incapable. For examples, a relay stuck temporarily for few seconds while changing the position can cause serious hazard due to delayed field status to interlocking. Though methods of compensating the drawbacks of FTA were studied, yet an effective solution is not available.

On the other hand, recently developed STAMP (System Theoretic Accident Model and Process) is excellent in predicting the time-series failure. In a recent paper, Sugimoto [1] highlighted the inability of FTA in predicting the time-sequence hazards that were identified by the STAMP. However, STAMP has another drawback of not having the quantitative analysis capability what makes it non-complaint to IEC 62278 and EN 50126.

Therefore, this research is proposing a new safety analysis method as a combination of STAMP and FTA to compensate for drawbacks of both approaches. This method incorporates the STAMP's qualitative analysis capability that can predict time-series hazards and doesn't skip any hazardous event. It also includes the FTA's quantitative analysis capability, which makes it compliant to international standards.

As a result, a new safety analysis that enables both qualitative and quantitative analysis and doesn't miss any hazardous event shall be established. The proposed method shall contribute to improvement in the safety of railway signalling systems by providing a comprehensive safety analysis as per international standards.

2. Survey of Safety Analysis Methods

A large number of safety-evaluation methods, including FTA and FMEA, that also find mention in IEC 62278 and EN 50126, are in use for a long time. This chapter covers a brief of these two traditional methods, along with some of their improved versions. The last section shall also include a brief about the STAMP.

2.1 Fault Tree Analysis (FTA)

FTA is one of the prominently used methods in reliability and safety engineering to identify the possible system failures, determining the rate associated with faults and reducing the risk arising from those failures. It was developed in 1962 by Bell laboratories for U.S. Air Force. After a lot of changes and improvement, it is still in use in aerospace, nuclear power, transportation and other safety-sensitive industries.

It is a top-down, deductive approach of failure analysis which uses the Boolean logic to represent the way various lower-level events in different combinations, lead to the undesired top events. Basic events are identified mainly in the form of component failures, software failures and human errors.

2.1.1 Basic Concept

Fault tree uses different events such as primary, conditioning, gate, transfer event to meaningfully represent the cause and effect relationship from bottom to top. Some of the important events related to FTA are as follows [2] [3]

- **Top Event**: it is an undesired event that usually represents a system failure or accident.
- **Basic Event**: It represents a primary cause for the undesired event and needs no further deliberations.
- **External Events**: It's an event that usually occurs irrespective of the system working.
- **Conditioning Event**: A specific condition or restriction that can apply to any gate.
- **Transfer Event**: Indicates a transfer continuation to a subtree.
- **Intermediate Event**: An intermediate event can be used immediately above the other events to provide more room to type the event description.

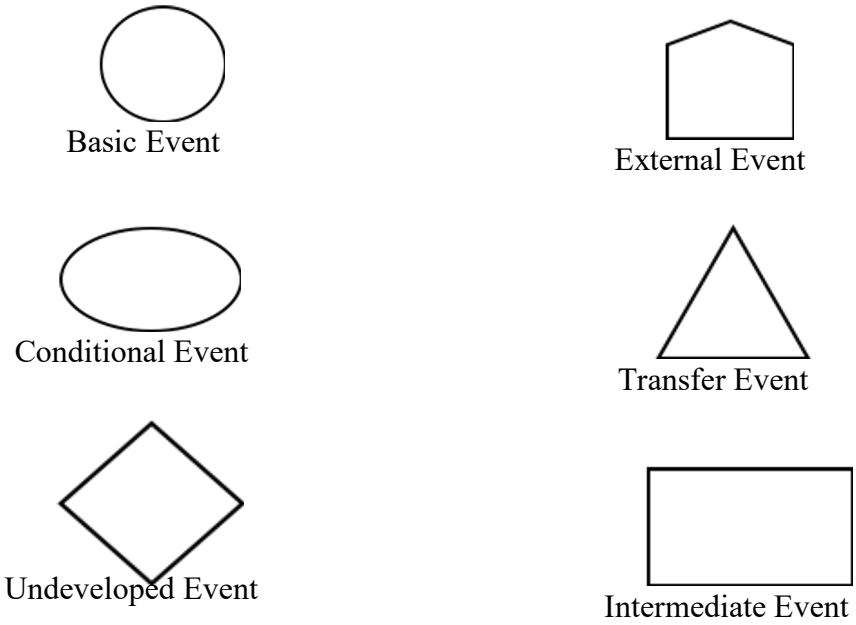


Figure 2-1 Various Events used in FTA

Various gates used in FTA are as follows [3]

- **OR gate**: The output occurs if any input occurs.
- **AND gate**: The output occurs if all Input occurs (inputs are independent).
- **Exclusive OR gate**: Th output occurs if precisely one Input occurs.
- **Priority AND gate**: The output occurs if the Input occurs in a specific sequence specified by a conditioning gate.
- **Inhibit gate**: The output occurs if the Input occurs under am enabling conditioning specified by a conditioning event.

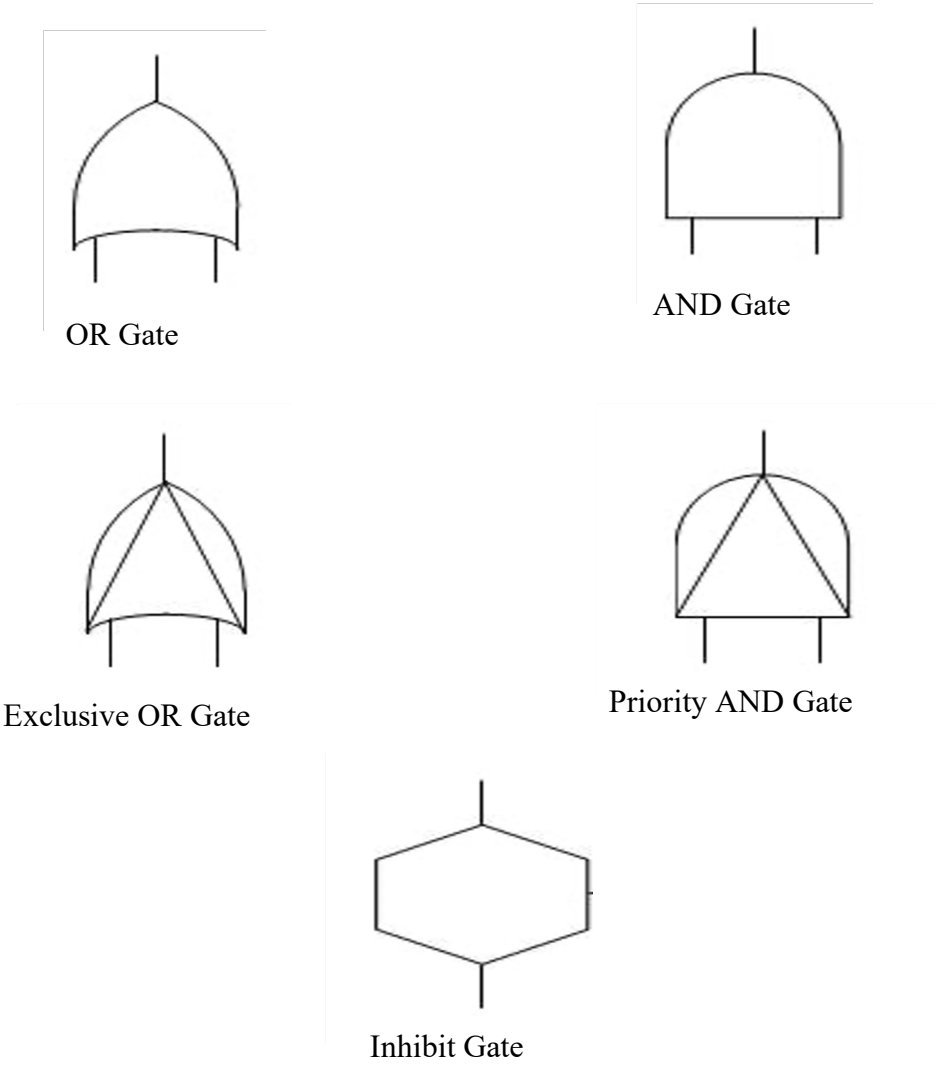


Figure 2-2 Various Gates used in FTA

2.1.2 Fault tree creation Procedure:

The necessary procedure for creating a fault tree is as follows. [4]

I. Define the system: This includes defining failure and scope of analysis. This step becomes essential when a system can operate with a fault in any one or more component.

II. Define top event/hazard: The top event is defined either for the entire system or a single block depending upon the scope of analysis.

III. Top event cause identification: It covers identifying the underline reasons behind the top event and using the logic gates to organize to show the required association with other events.

IV. Identify the next level of events: Each event leading to the top-level failure may also have precipitating events.

V. Identify root causes: For each event above continue to identify precipitating events or cause to identify the underlying cause of the sequence of events leading to failure.

VI. Add probabilities to events: Where possible, add the actual or relative probability of occurrence of each event.

VII. Analysis the fault tree: Look for the most likely events that lead to failure, for single events the initiate multiple paths to failure, or patterns related to stresses, use, or operating conditions. Identify means to resolve or mitigate paths to failure.

2.1.3 Analysis Types:

Depending upon the requirement FTA can serve two purposes;

1 Qualitative Analysis.

2 Quantitative Analysis

2.1.3.1 Qualitative Analysis:

Qualitative analysis involves determining reliability characteristics of the top event from primary event characteristics. Quantitative analysis includes determining (a) the system modes of failure and (b) the component of the system that share an alliance such that they are candidates for a common cause failure; for example, two components that are both subject to failure due to moisture and are in close vicinity are common cause candidates. A system mode of failure, called a minimal cut set, is a group of basic component failures, called primary events, that are collectively sufficient to cause the top event to occur. [5]

The purpose of qualitative analysis is usually to find minimal cut sets. One of the most common fault tree algorithms for generating CSs is the MOCUS (Method of obtaining the cut-sets) algorithm.

The algorithm starts at the top gate representing the top event of the fault tree and constructs the set of cut sets by considering the gate at each lower level. [6]. AND gate means that all the inputs must occur to activate the gate. Thus, AND gate is replaced at the lower level by a list of all the inputs. OR gate means that the occurrence of any input can activate the gate. Thus, the cut set being built is split into several cut sets, one containing each Input to the or

gate. Based on minimal cut sets, it is possible to get all the unique combinations of primary events that may result in the top event. A minimal cut set represents each of them.

2.1.3.2 Quantitative analysis [7]

Reliability analysis is probabilistic; therefore, a complete quantification of the system is required to be able to assess a meaningful value for the reliability of the system. In the fault tree analysis, since the system structure logic is composed of a series of negative (failure) logic, the term reliability is always replaced by the term "unreliability." In a quantitative sense, unreliability is a complement value of reliability. As discussed in the previous section, generating minimal cut sets is the first step in any FTA. The second step in FTA is to find the Top event unreliability by proper assignment of probability values (data) to each basic event (components failure). The assignment of data described above depends on the type of results required. For example, if a point estimate of the Top event failure probability is to be determined, then the point estimates for the component failure probabilities (or data allowing their computation) needs to be assigned. Similarly, if a distribution is to be found for the Top event unreliability, then one or more of the component characteristics needs to be assigned in terms of distribution. Given the above data, the following quantitative evaluations are generally useful in assessing system reliability.

2.2 Improved Fault Tree analysis

2.2.1 Conditional Fault Tree

CFT is an extension of FTA that aims to include uncertainties in the fault tree. As per Zhen Xu Zhou [8], sometimes the causalities can be uncertain. Considering that some of the causal relationships in the FTs may be uncertain or non-deterministic, CFT introduces a new parameter U. It illustrates the random mechanism of how parent event can cause child event and probability of this parameter U is used to measure the uncertainty between parent event and child event. Since CFT is an extension of traditional FT, it can cover both qualitative and quantitative analysis. For qualitative analysis, one can simplify a given CFT into the most comfortable form with some defined rules and properties. With the purest form of CFT, one can then get the minimum cut-set with uncertainties.

2.2.2 Software Fault Tree Analysis (SFTA)

SFTA derives from safety -system analysis technique, and it can verify the safety aspect of the software [9]. This method considers the undesired events originating from software failure and faults. [10]. SFTA can identify failures related to software systems, and also the sub-events that might have triggered the top events. Similar to FTA, it arranges the failure events in a tree structure. The top event usually represents a system-wide undesired event which potentially may inflict the danger of becoming an accident leads to a catastrophe. [10]

Some of the advantages of SFTA are as follows [11]

1. Identify contributing circumstances to an unsafe state.
2. Demonstrate that a system cannot reach an unsafe state.
3. Demonstrate the probability of going to an unsafe state is very low.

SFTA provides a backward analysis from the root node to the necessary preconditions for the undesired event to take place. The required conditions include the failures that triggered the hazard, and faults which triggered the failures. [10]

2.3 FMEA: Failure Mode and Effect Analysis

FMEA is a widely used hazard analysis method to evaluate the system safety across a wide range of industries. Initially, it was developed for the U.S military to study the problems arising from the system's malfunctioning, but later of its use expanded and now it is used extensively in aerospace, automobile, product design and process and various other industries. The basic idea in FMEA is to identify possible failure modes in a subsystem or component using the experience from similar product use or using basic science logics and then to analyze its effect on effect on the entire system. In this method, the system is divided into subsystems or components, and then each subsystem or component is taken one by one for anticipating the potential failure associated with them. Then each failure is analyzed for its impact at the system level, and a table is prepared to depict each failure and its effects. Based on this, the analyst can recommend measures to eliminate the failure or mitigation of its impact on the system. It's a lifelong process for any system that starts from systems conception till its decommissioning. This method is capable of doing both qualitative as well as quantitative analysis, and it uses an Inductive or bottom-up approach as it starts investigation from the primary component failure and then analyzes its effect at the system level.

2.4 Improved FMEA

2.4.1 AFMEA: Advanced FMEA

AFMEA is a level analysis based on behaviour modelling, and it incorporates the behaviour analysis with FMEA. Opposite to the FMEA, AFMEA is a deductive or top-down approach. AFMEA is further development of FMEA, and this development showed a way to make FMEA more structured and systematic. [12] FMEA provides a framework for control and hardware developer to discuss and understand the relationship between sub-systems, controls, and overall system performance. It provides a systematic approach to identify a comprehensive set of failure modes early in the design phase. AFMEA uses behaviour modelling to link desired behaviour with the components, operating environment, related systems and control logics and qualitative behaviour simulation provides the framework for identifying failure modes and estimating their effects. AFMEA defines three kinds of failures. [12]

1 Non-behaviour failure.
2 Unexpected behaviour failure.
3 Mis-behaviour failure.

2.4.2 Software FMEA

SFMEA is a bottom-up software reliability technique that identifies the potential software failure modes and helps in improving the safety of the control system. process of SFMEA is as follows: [13]

1. Confirmation of software functions: In this step, the analyst identifies all software-intensive units of the system, their functions and structures; and draws out the software flow charts.
2. Identification of software failure mode: Identification of software failure mode is one of the most challenging tasks as there is no physical component to predict the failure. The analyst predicts all these possible failures based on the requirement and functions to be performed by the unit. Identifying software failure modes require expertise.
3. Assessment of failure mode effect: After identification of failure modes, the analyst analyses the impact of each failure on the entire system.
4. Assessment of failure cause: In this step, the analyst analyses the reason behind each failure mode to identify the steps to eliminate or reduce the impact of failure. All the above information is recorded in SFMEA table.
5. Reassessment in the new iteration: depending upon the result of SFMEA software requirement and specifications are repeatedly modified until the results obtained by SFMEA in respect of safety and reliability are up to the standard.

6. SFMEA applies to the components including software, commercial off the shelf, firmware component, free, open-source software.

2.5 STAMP: System Theoretic Accident Model and Processes

STAMP is the newest safety analyses methodology developed by MIT academic Ms Nancy Leveson, and it is based on system theory. Ms Leveson stresses that system theory is a useful way to analyze the accidents, particularly system accidents. In this conception of safety, accidents occur when the control system does not adequately handle external disturbances, component failures, or dysfunctional interaction among system components. i.e. accidents result from inadequate control over safety-related constraints in the development, design, and operation of the system. [14]

She emphasizes that safety is a control problem, and one should use the control structure to enforce constraints during system development and its operation to ensure safe behaviour. In this model purpose of the accident's analysis is to determine the control ineffectiveness and based on the result, to enforce the necessary constraints for safety. She further advocates that instead of focusing just on preventing component failure events, the focus should be on constraint imposition to limit system behaviour to safe changes and adaptions. The motive of accident analysis should be to look for the ineffective controls that failed to prevent or detect maladaptive changes, i.e. to identify the safety constraint's violation and to determine why the controls were inadequate in enforcing them. [14]

She stressed that the system is not a static design, but a dynamic processed that adapts and reacts to changes to itself and its environment. So, the system is a dynamic equilibrium of interrelated components that using feedback loops of information and control.

This model follows the following three principles. [14]

I. Safety constraints.
II. Hierarchical safety control structure.
III. Process models.

2.5.1 System Theoretic Process Analysis (STPA)

STPA is STAMP based analysis method used for hazard analysis

STPA has two main steps: [14]

1. Identify the inadequate controls that can cause hazardous state. Hazardous states are the results of
   a. Absence of control action required for safety.
   b. Unsafe control action.
   c. Potentially safe control actin applied at the wrong time.
   d. A required control action provided for an inappropriate time duration.
2. Determine the cause of hazardous control action described above.
   a. Examine control loops for probable cause of each unsafe control action and recommend controls or mitigation measures if required.
   b. Considering age-related degradation in control including
      I. Replacement management to ensure enforcement of safety constraints in planned replacement activities.
      II. Performance audits where the assumptions underlying the hazard analysis are the preconditions for the operational checks and controls so that unplanned changes that violate the safety constraints can be detected.
      III. Trace of anomalies to the system design and the hazard by incident and accident analysis.

3. Research Objective

The disadvantage of FTA is that it is difficult to predict the time-delay failures. For example, in case of a dual system, it is difficult to express the failure of both systems in a time sequence manner, i.e. one after another with some time gap. It is also tricky for conventional FTA to represent a time series hazard event in which the present action depends upon the time duration of previous steps. Furthermore, FTA has no systematic procedure for analysis due to which chances of missing some critical events are high and the chances of losing the event increase with the increase in complexity of the system. Therefore, improved FTA was proposed to overcome these difficulties. However, it has its challenges, such as using state transition diagrams for devising the tree and chance of misses the event is still there.

On the other hand, events in STAMP are predicated based on four guide words for control action, i.e. (1) hazard if not provided, (2) Hazard if wrongly provided, (3) hazard if provided at wrong time (too early or too late), (4) hazard if applied for the wrong duration (used too long or stopped too soon). So, it covers all possible risks through guide words and ensures the completeness of the analysis. Furthermore, guide word (3) and (4) covers all time-delay and time sequence hazards. Though STAMP is suitable for qualitative analysis, but it doesn't include the quantitative analysis required for compliance with international standards.

Therefore, this research's objective is to make a new safety analysis method that can do comprehensive qualitative analysis as well as quantitative analysis and comply with the international standard. It shall be covering all the times-series hazards, along with all the hazards predicted by conventional methods.

4. Proposed Method

Going through many deliberations, we decided to go for a combination of STAMP and FTA to make the new method. We aimed at creating a STAMP based fault tree, means. It means to carry out safety analysis using STAMP procedure and then generate the fault tree taking inputs from the STAMP analysis. The reason behind this logic is that FTA focuses mainly on component failures, and there is no defined set of rules for predicting the top hazard or intermediate event of the tree. It makes the results dependent on the knowledge and expertise of the analyst, and that's why FTA result from different analyst may be different. Additionally, the likelihood of missing various intermediate events, in the absence of a defined set of rules, is very high.

On the other hand, STAMP can easily predict component failures as well as component interaction failures. Besides, STAMP is capable of predicting the time-sequence hazards, which is one of the significant issues for embedded systems working based on clock synchronization. Moreover, the use of defined procedure and guide words make the STAMP procedure streamlined and results in variation from the different analyst is comparatively less. At the same time, this streamlined procedure eliminates the chances of omissions and helps in preparing a comprehensive hazard list. As STAMP covers all the hazards predicted by FTA in addition to other hazards like component interaction, time-sequence hazards., creating a fault tree from results of STAMP shall serve the following purpose.

1. It covers all the possible events predicted by FTA.
2. It has additional probable events such as component interaction hazard, time sequence hazards that are difficult to be predicted by FTA.
3. A defined set of procedure eliminates chances of omission of any events.
4. It's challenging to comprehend the STMAP result due to its presentation in extensive spreadsheets. The transformation of this result in a fault tree makes it much easier to understand as a fault tree depicts the relationship among different events using logic gates.

Figure 4-1 shows a conceptual block diagram for the new propose method that depicts how it first uses the STAMP for qualitative analysis and then transforms STAMP results in a fault tree,

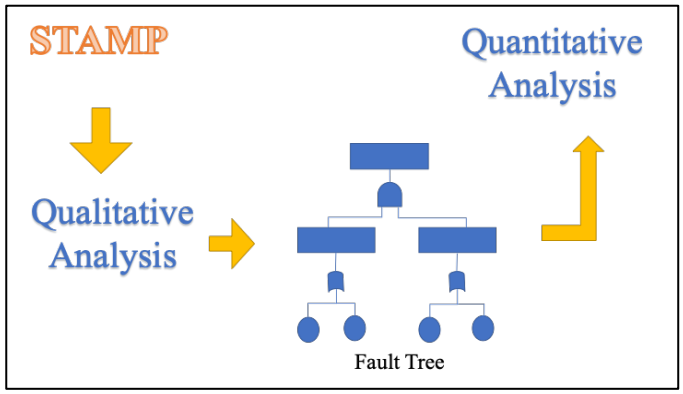


Figure 4-1 Combining STAMP and FTA

and finally uses the FTA method for quantitative analysis. Following sections give a brief insight into implementation steps of the proposed method.

4.1 System selection

The first requirement to test any approach is identifying the right target system. This research used two target systems for application and result-analysis of the newly proposed method. Reason to go for two target system was to gain more confidence in the implementation of the proposed plan and to try to find a way to overcome limitations faced during its usage. Though any system can be analyzed using this method, this research targeted the systems that are used in the railway's signalling only, as this study was conducted specifically for that purpose. The first target system is "On-Board ATP" system used for train control, and the second target system is "Electronic interlocking" system used to ensure safety in routing trains.

4.2 STAMP Application

STAMP application has four main steps (Nancy Leveson)

1. Defining Accidents, Hazards and Safety constraints for the system.
2. Construction of Control structure.
3. Extraction of unsafe control actions (UCA).
4. Extraction of hazard causal factors (HCF).

4.3 FTA application

FTA is a top-down approach that starts with the identification of top hazardous event and tracing down the system components to find the primary events that caused the trigger of top hazard. Identification of top event is a big challenge because of no defined set of procedures. FTA application involves following main steps.

1. Identification of top hazard.
2. Tracing the system down to find intermediate and basic events
3. Representation of events in a tree form using logic gates.
4. Quantitative analysis.

Though, performing FTA analysis at this point is not the requirement of the system yet we covered this step to compare the result of FTA and newly proposed method because the proposed method is targeting various limitations of FTA, such as its inability to predict time-sequence hazards.

4.4 STAMP to Fault tree Mapping

We considered two methods for transforming the STAMP result into the tree form. The first proposal was not successful because of its limitations, but the second method proved useful and was finally adopted. In the first method, As STAMP, similar to FTA, is a top-down approach, which has the sequence of Accidents, Hazards, UCA and HCFs, where HCF lead to UCA and UCA leads to hazards and hazard ultimately transforming into an accident if specific conditions fulfil. Straightforwardly, we decided to keep Accidents as the top event of the fault tree, Hazards 2^{nd} level, followed by all the UCAs at 3^{rd} level and the 4^{th} level consisting of HCF as shown in Figure 4-2. However, while considering the practical application, it was observed that UCAs identified by STAMP were not independent and many of them were directly or indirectly related to each other. This relationship made it impossible to keep all the UCAs at the same level. Similarly, it was not possible to keep all HCFs at the same level. Further, it was also observed that UCA is caused by HCF, different combination of HCFs and combination of HCFs and UCAs along with other events that create the right scenario for HCFs propagation to the higher level. Based on this, the first idea was abandoned, and a new possibility was considered.

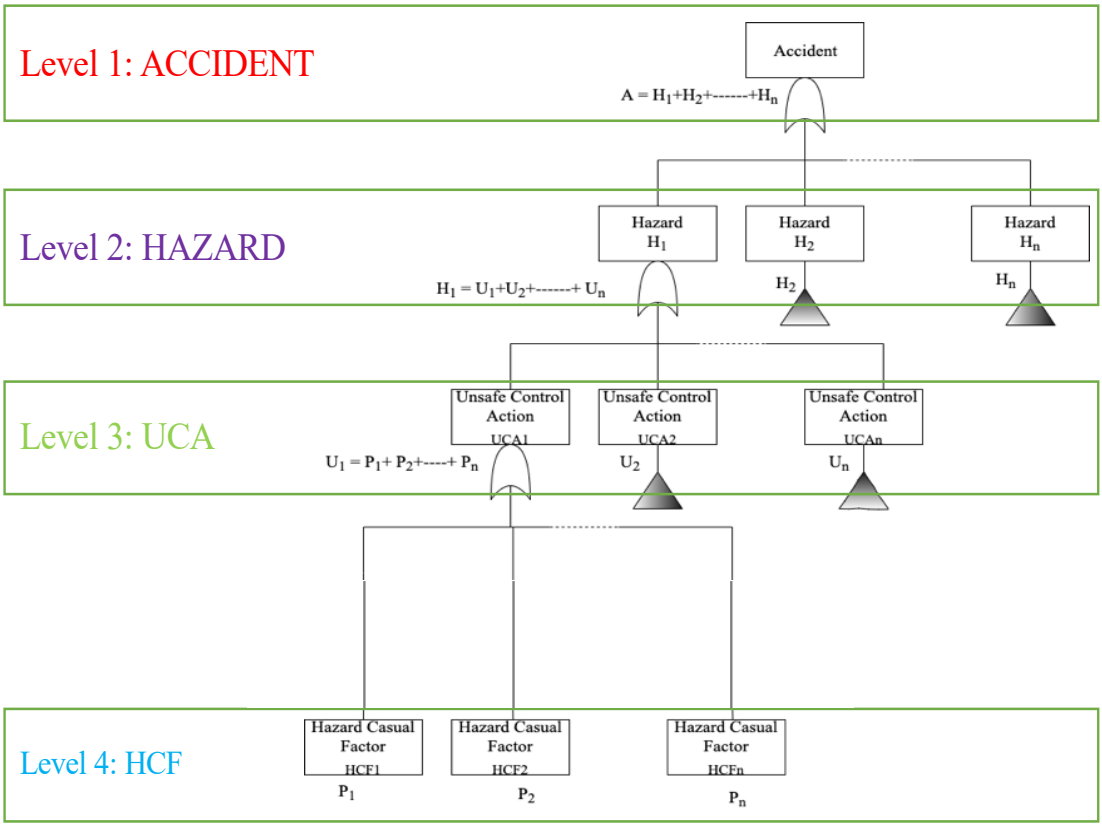


Figure 4-2Considered Method for STAMP and FTA combination.

In the second approach, or finally adopted method, we proposed to keep various UCAs and HCFs at fixed levels. However, system knowledge and FTA application expertise are still required to decide the position of different events. In this procedure, the first step is to arrange UCAs at different levels showing some relationship among the related UCA, as shown in Figure 4-3, (not all the UCAs need to be connected. Usually, UCAs generated only from similar functions are connected). The second step is to place all HCFs at an appropriate position showing the relationship of each HCF with other HCFs and UCAs. In most of the cases, HCFs get dispersed at different levels, similar to the UCAs, as shown in Figure 4-4. Some HCFs may need to be repeated in a fault tree to make a clear explanation of tree structure. The final step is to map scenarios to the fault tree to create a better understanding, as shown in Figure 4-5.
In the last, an FTA expert review is needed to suggest any other event that is required to make tree explanation more rational.

No.	Control Action	From	To	CA Providing Condition	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
1	Alarm Initiation	On Board ATS System	Alarm System	When Signal is RED operate the warning alarm	(UCA1-N-1) Alarm system doesn't Initiate alarm. [SC1]	(UCA1-P-1) No Alarm actuation when signal is RED [SC2]	(UCA1-T-1) Late Alarm actuation when signal is RED [SC1]	x
2	Audio Visual Alarm	Alarm System	Train Operator	[illegible] when signal is RED.	[illegible]	x	[illegible]	x
3	Manual Brake command	Train Operator	Brake Controller	[illegible] Braking signal is [illegible]	[illegible]	x	[illegible]	(UCA3-D-1) Brake time too small to stop the train. [SC1]
4	AUTO Brake command	On Board ATS System	Brake Controller	AUTO brake initiation when driven not reponding to warning	(UCA4-N-1) No Brake command when inaction by Operator. [SC1]	x	(UCA4-T-1) Delayed Brake command when no action by Operator. [SC1]	x
5	Brake Process	Brake Controller	Brake Mechanism	Braking when brake initiation cammand is received	(UCA5-N-1) No Braking [SC1]	(UCA5-P-1) Usuccessful Braking [SC1]	(UCA5-T-1) Braking when train alredy inside minimum braking distance. [SC1]	(UCA5-D-1) Braking not for enough duration to stop the train [SC1]

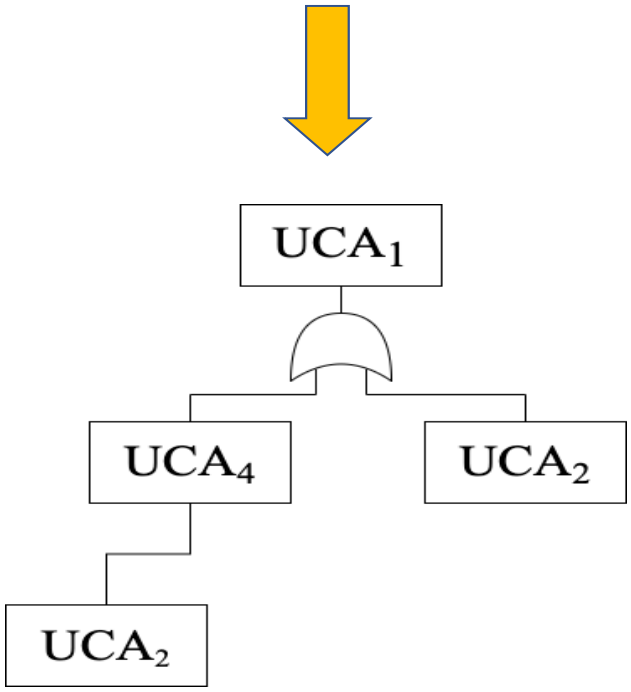


Figure 4-3 UCA Transformation to Fault Tree

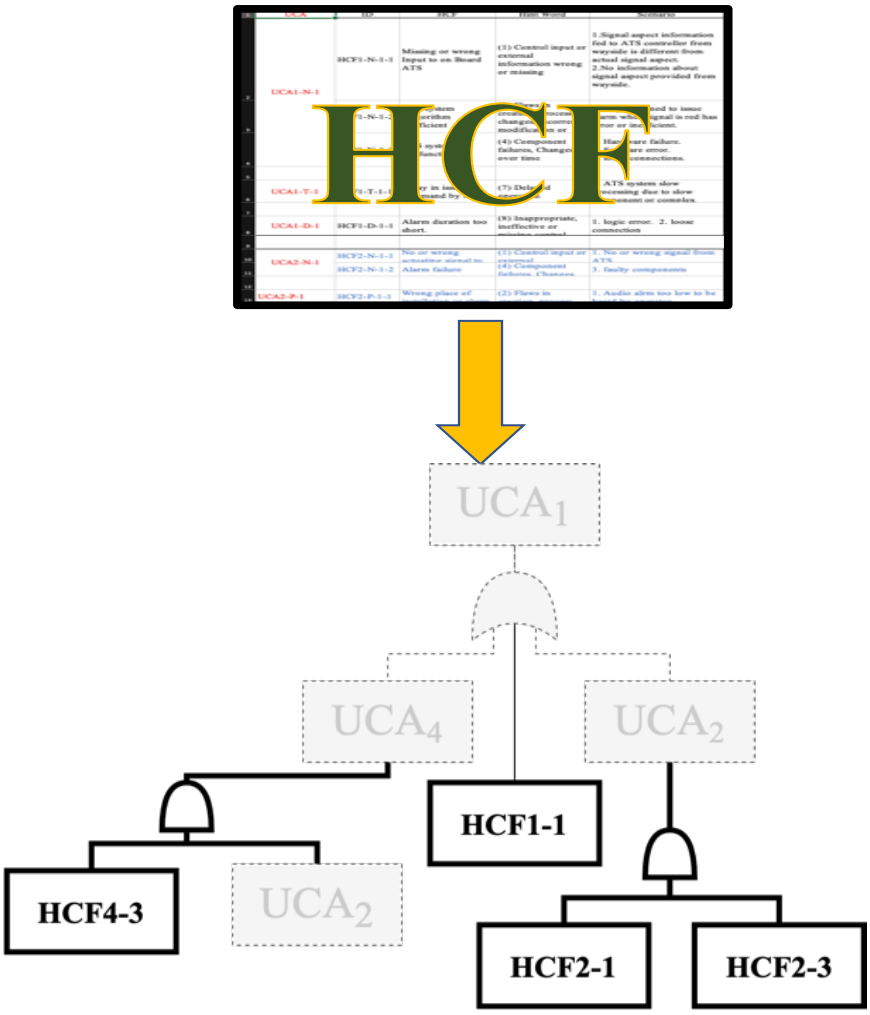


Figure 4-4 HCF Transformation to Fault Tree

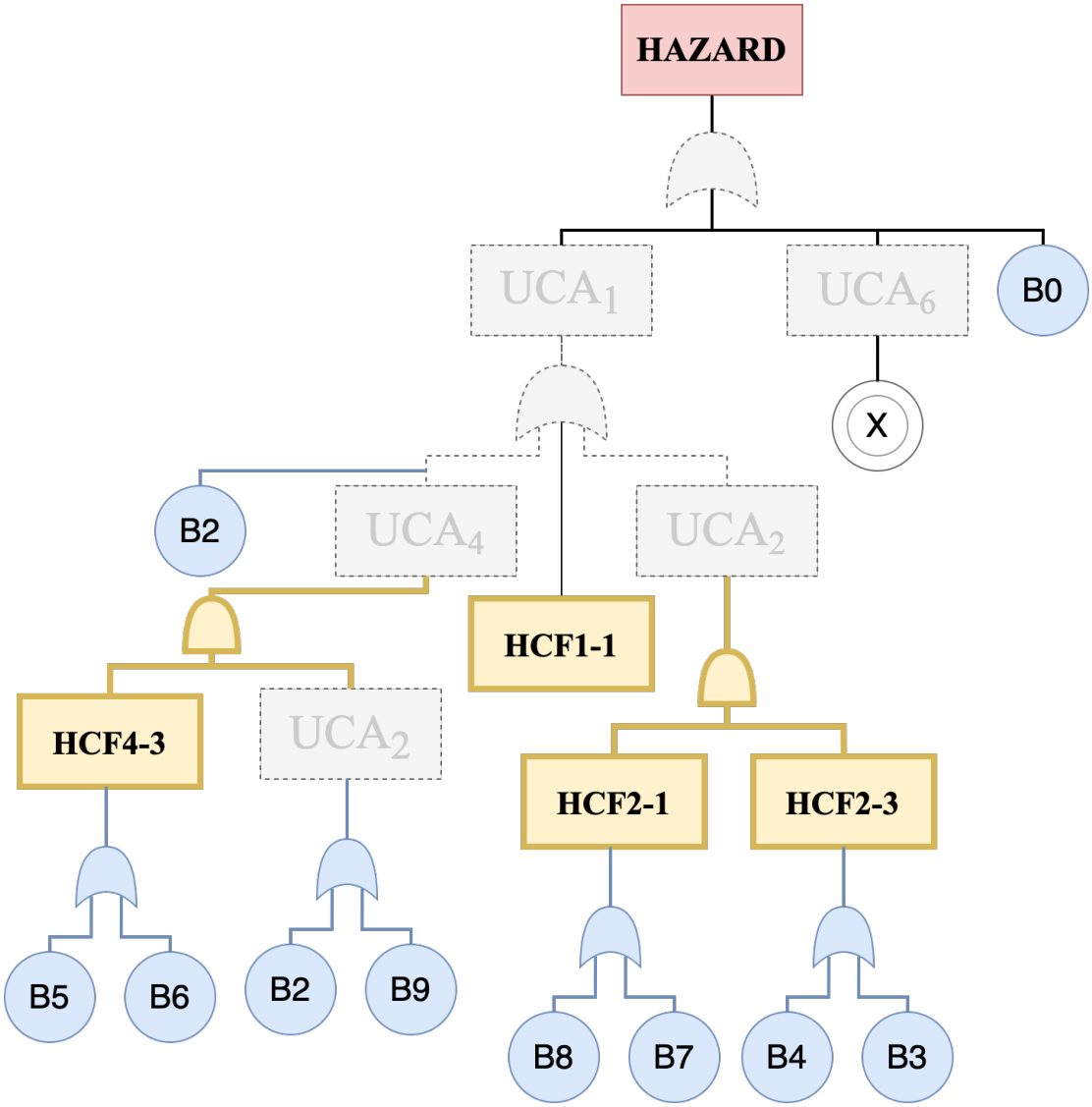
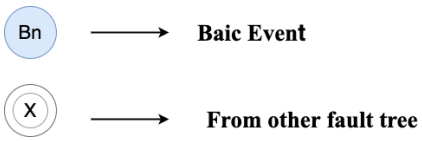


Figure 4-5 Complete Fault Tree from STAMP



4.5 Quantitative analysis

For quantitative analysis, this method uses the quantitative method used for FTA quantitative analysis approach. In addition to covering all types of research, this approach shows that quantitative analysis is possible for STAMP result on its transformation in a fault tree. To keep things simple, we used the simple quantitative analysis method of FTA.

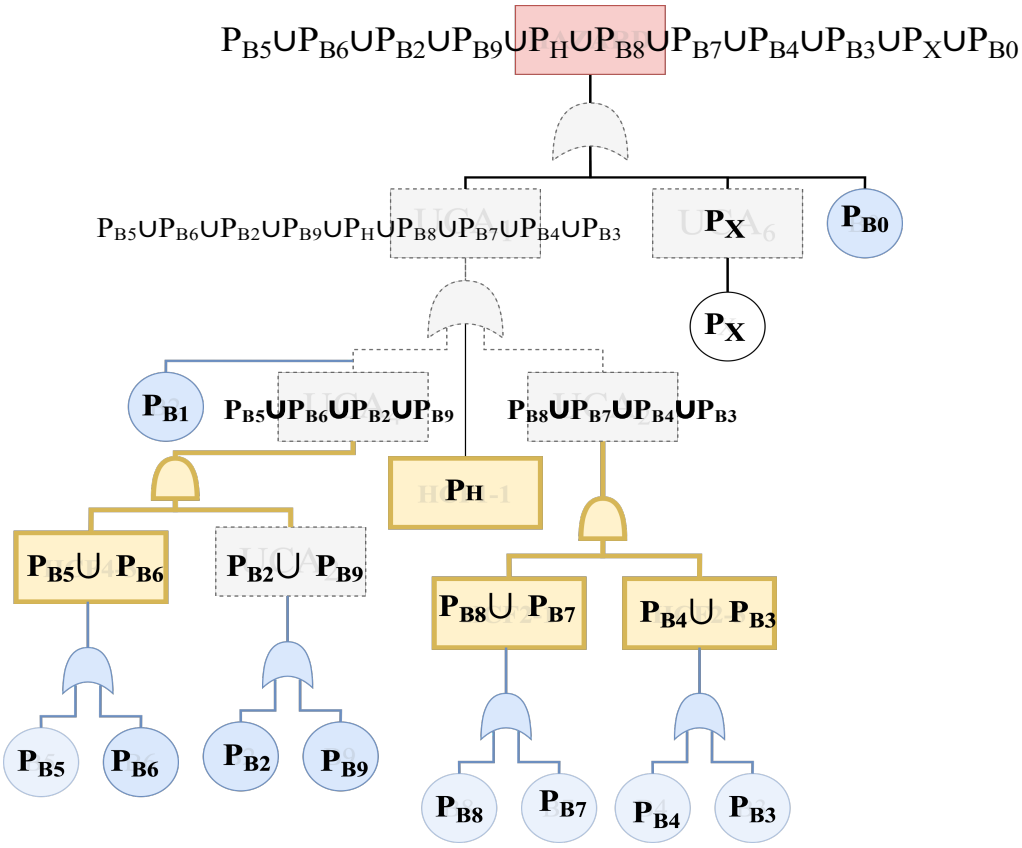


Figure 4-6 Quantative Analysis

Events in fault tree are associated with statistical probabilities. Usually, convention logic gate's Input and output are in binary form, i.e. 0 and 1, however, in FTA, outputs probabilities are related to the set operations of Boolean logic, and output probability of gate event depends on the Input of the gate. Figure 4-6 depicts the calculation of the probability of various events using Boolean logic.

In the fault tree, independent events are represented by AND gates and output probability of AND gate is given as

$$P(A \text{ and } B) = P(A \cap B) = P(A)\,P(B) \qquad (4\text{-}1)$$

OR gate corresponds to the set union

$$P(A \text{ or } B) = P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

Failure probability in FTA is minimal; usually, less than .001 and in that case, $P(A \cap B)$ becomes even smaller and can be avoided. So, OR gate output can easily be approximated to

$$P(A \text{ or } B) = P(A) + P(B) \qquad (4\text{-}2)$$

1. Assigning the probabilities to the primary events:

The quantitative analysis starts with mapping the occurrence probability to the basic events. Some designated organizations maintain the failure and reliability data of various components. This kind of data includes manufacturing defects, random failures, testing errors, calibration error, maintenance error.

In this research, we didn't have access to factual data, and this Quantitative analysis was done only to explain the probability calculation procedure. So, we decided to go for imaginary data, taken randomly, for all primary events.

2. Probability calculation for intermediate and top events:

On completion of probability assignment to primary events, Equation 4-1 and Equation 4-2 were used to calculate the probabilities of all the intermediate and top events. Figure 4-6 explains the probability calculation of various events.

4.6 Research Flow chart

Figure 4-7 shows the steps followed in conducting the proposed method implementation.

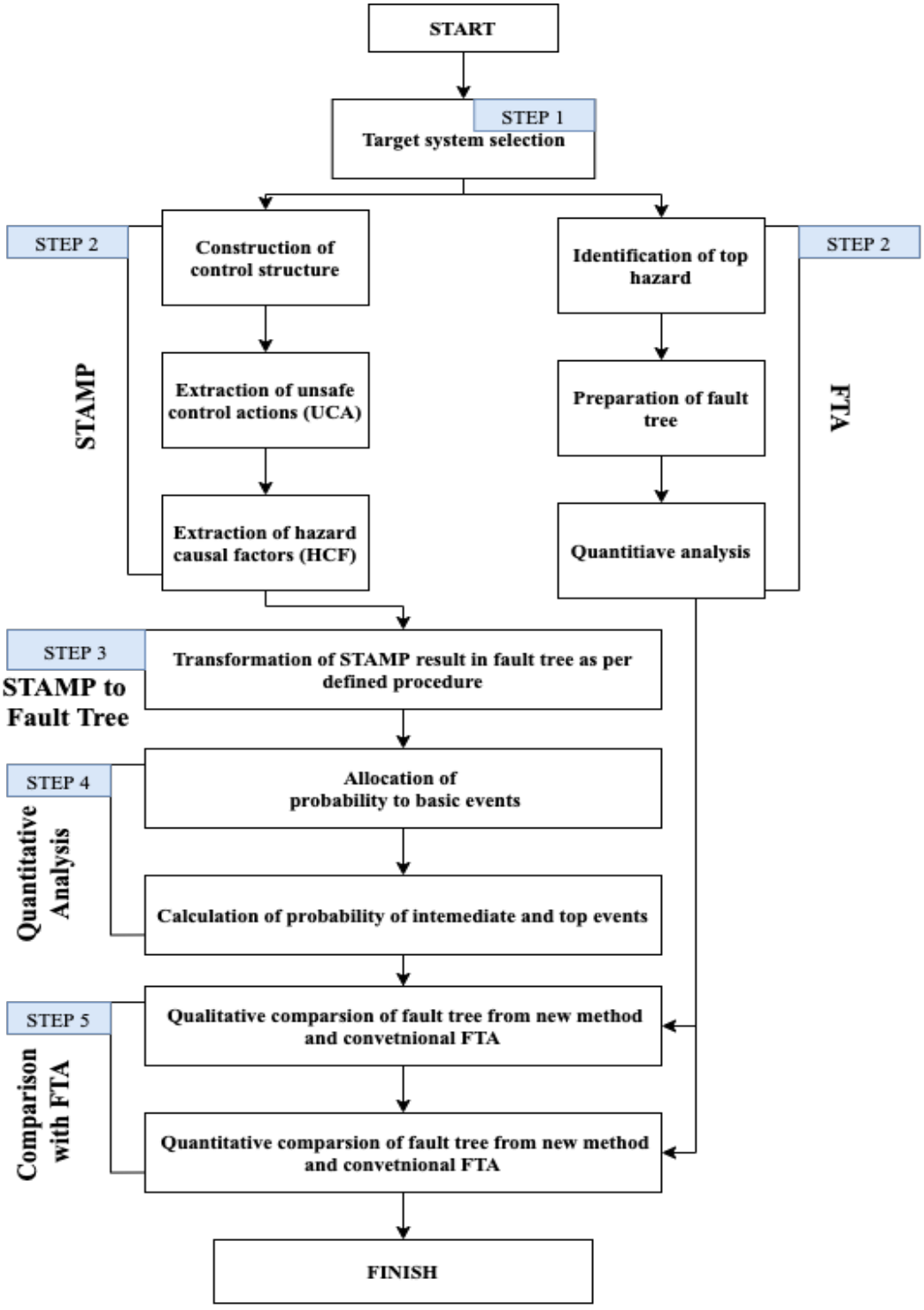


Figure 4-7 Research Flowchart

5. Comparison of the proposed method with various other methods

FTA has been excellent in predicting and presenting various events, either alone or in association with other events, that can propagate through a system and result in a hazardous situation. This method uses a to down deductive approach that is very convenient in presenting the direct and indirect reason and a combination of these reasons causing top hazardous events. This method has many advantages and has served good in safety analysis in various industries. Besides its benefits, this method has shortcomings also and still has the room for improvements. Among the disadvantage, the prominent one is the uncertainties in covering all the failure modes. There is no formal control against the overlooking of events due to the absence of a systematic procedure. The second one is that the analysis depends on analysis expertise, and there is a good chance of inaccuracies or human error in the investigation of complex systems.

Further, this method considers the component failure as the underlying cause behind various hazardous events. However, some temporal failure and delay in execution, in case of time-dependent sequential operations, might be the severe safety concerns. As these kinds of failures are not the result of component failure, these are difficult to be identified by the FTA. Over time many improvements in FTA has been proposed focusing on different points.

Towhidnejad and Hilburn [7] pointed out that identifying the top events is one of the first steps in FTA and gave the idea of borrowing this from the FMEA or HAZOP analysis. But they also mentioned that this is a very subjective activity and gets influenced by the analyst bias. Sugimoto [6] has pointed out that it is not possible to identify the time hazard failure in FTA. That is why she advocated the STAMP analysis to determine the time-sequence hazard use of state transition diagrams to present these hazards. However, borrowing the top event from the FMEA still doesn't solve the issue of missing event as FMEA is also dependent on analysis expertise only. Also, using the STAMP only for identifying the time-sequence failure and representing these hazards in the form of state transition diagram makes the analysis complex. So, improved version of FTA also has the drawbacks such as not easy to identify the top events, doubts over the completeness of analysis, the chance of missing events, smooth presentation of time -sequence hazards.

So, from the review of FTA and its improved versions, it can be established that FTA still has two significant drawbacks. First is, it's difficult to confirm the completeness of the analysis, and second is, it's is challenging to identify the time-delay events.

On the other hand, FMEA is a bottom-up inductive approach. Using FMEA, it's easy to analyse the impact of individual failure and degree of its influence on the system. However, it is difficult to explain the impact of two overlapping failure as FMEA considers one component failure at a time. Also, there may be variance in the result produced by two different analysts because FMEA analysis also depends on the expertise of the analyst.

Furthermore, Nancy Leveson pointed out the traditional methods focuses on individual component failure for the hazard analysis. She gave the new method 'STAMP' based on system theory. She described the systematic procedure to conduct the analysis using the STAMP. It uses the guide words to identify unsafe control actions and then cause behind these unsafe control actions called HCF (hazard Causal Factor) can be identified using another set of guide word provided with the method. These guide words ensure to cover all hazardous event and help in a comprehensive qualitative safety analysis. But it has another limitation of having no quantitative analysis.

The proposed method covers all the above limitations. The proposed method does the comprehensive qualitative analysis with the help of STAMP method and includes all the defect of FTA. All the time-sequence or time-delay failure gets easily covered with the help of guide word such as 'control action applied too late or too early' and 'control action applied too long or too short'. Also, top hazards for FTA can easily be predicted with the help of the UCA table. Furthermore, it covers the limitation of STAMP by doing the quantitative analysis with the help of FTA. Hence this proposed method complies with IEC 62278 and EN 50126 standards which is essential for safety-critical systems of railways. Table 5-1 shows a brief comparison of various methods

Table 5-1 Comparison of various methods

Features	**FTA**	**Improved FTA**	**FMEA**	**STAMP**	**New method**
Completeness of Analysis	✗	✗	✗	✓	✓
Quantitative Analysis	✓	✓	✓	✗	✓
Easily covers time sequence hazards	✗	✓	✗	✓	✓
Result in easy to be understood form.	✓	✗	✗	✗	✓
Defined process for analysis	✗	✗	✗	✓	✓

6. Case Study

Aim of this research was the inclusion of STAMP's qualitative analysis capabilities in safety evaluation of railway signalling systems to make it more comprehensive compared to existing methods. So, the case study was conducted to check the practical implementation of the proposed method and its advantage over the conventional way while applied to the same system. In this case study, two systems named On-board ATS and Electronic Interlocking were examined, which are essential systems in railway signalling, using both newly proposed method and conventional FTA. The analysis results were later compared with each other to check the effectiveness of the proposed method. This chapter covers the following items.

1. System description.
2. Block diagram.
3. Conventional FTA application to the target system.
4. New Proposed method analysis of the target system.
5. Comparison of analysis result from both methods.

6.1 On-Board ATS

On-board ATS ensures safe train operation that continuously supervises the train operation and takes necessary action if an unsafe situation arises. On-boards system is a part of ATS that operates in association with 'wayside ATS'.

6.1.1 System description

ATS stands for "Automatic Train Supervision" and this system assists in safe train operation and provides various features such as a warning to the operator and brake initiation if required. As can be inferred from its name, this system only supervises the train operation, and all the operational activities are the reasonability of the train the operator. However, it takes over control to bring the train to a standstill if the operator fails to initiate the necessary safety steps such as speed reduction or brake application. ATS system has two main subsystems a shown in Figure 6-1.

1. On-board ATS.
2. Wayside ATS.

On-board ATS is installed in the operator cab and has dedicated interfaces for speed monitoring, audio and visual alarms, acknowledgement from the operator, and brake control. It has inbuilt

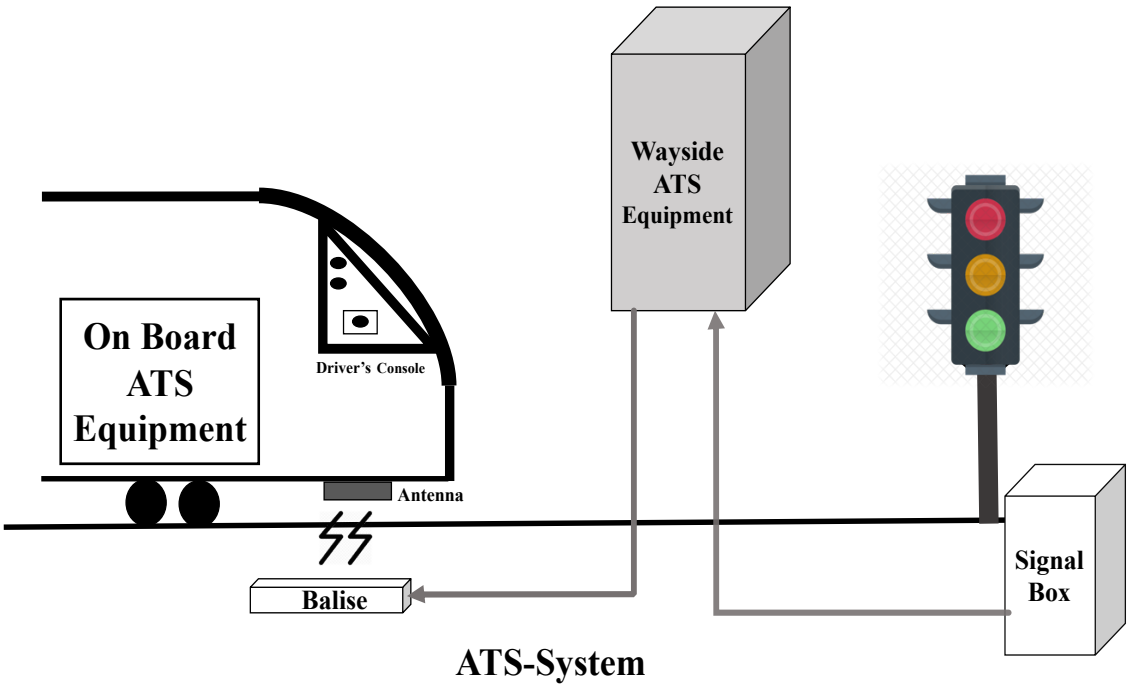


Figure 6-1 ATS system

software that determines the actions to be executed based on the data received from wayside ATS and its interfaces with the train. For, receiving wayside data, it uses radio antenna installed under the cab that collects data from Balise/transponder installed at track centre at defined locations.

6.1.2 Block diagram

Figure 6-2 shows the functional block diagram for the on-board system. It has five main sub-systems that include On-board controller, the alarm system, train the operator, brake controller and brake mechanism. A controller connected to the antenna receives the wayside signal present aspect from wayside ATS unit. Based on this information, it generates an audio and visual alarm to the operator, if the signal aspect ahead is Red, to make him alert to control the speed and stop the train before the signal. The operator needs to acknowledge the alarm using a push-button on the operator console within five seconds of alarm generation. If the operator fails to acknowledge the alert within five seconds, then controllers issues the auto brake initiation command to the brake controller, which in turn activates the brake mechanism to stop the train before the Red signal.

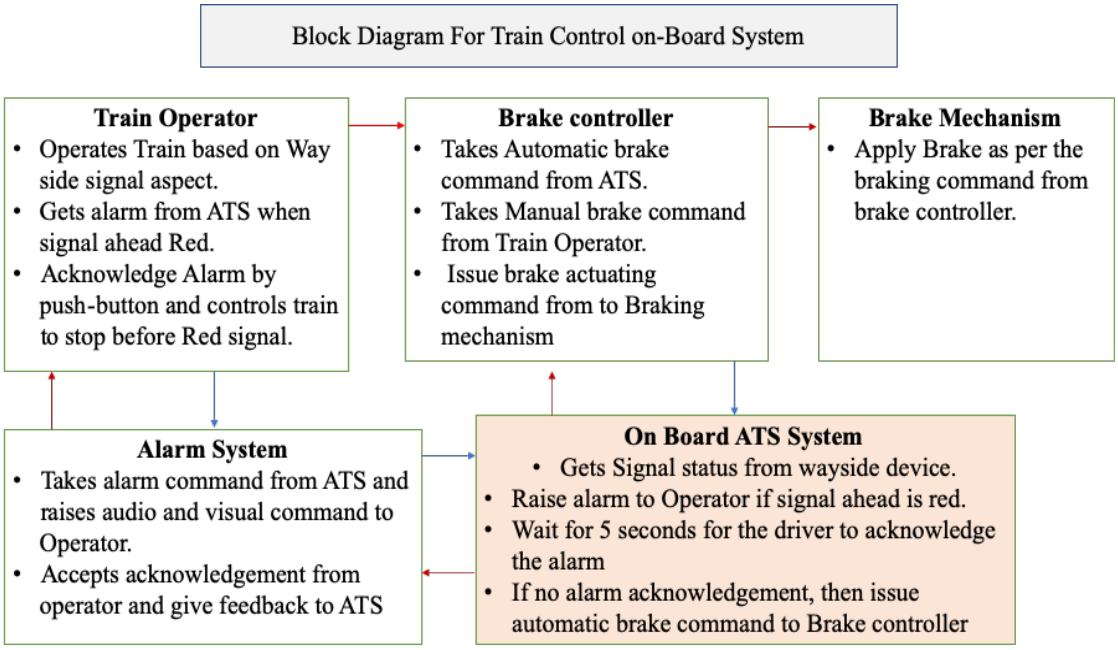


Figure 6-2 Onboard ATS

6.1.3 Conventional FTA analysis of ATS

FTA needs a detailed understanding of the system. On-board ATS ensures safe train operation that continuously supervises the train operation and takes necessary action if an unsafe situation arises. On-boards system is a part of ATS that operates in association with 'wayside ATS'.

System description and Block diagram section of this chapter has covered the details of the system working. The first step in the construction of a fault tree is the identification of top hazardous events. This system prevents an incident of a train crossing the red signal that has the potential to cause a disastrous event if another train is present immediately ahead of the jumped signal. So, the top event for this system is "Train passes the signal when it is red". A system can have more than one hazardous event as top events depending upon the various condition. However, for ease of application, we restricted the scope to one top event only.

On identification of top events, immediate faults or hazardous events leading to top event were identified. This deductive approach continued until we were able to identify the initial triggering fault or the primary events. Figure 6-3 shows the fault tree for the on-board system. All the circles represent the basic events, and rectangle boxes represent the intermediate events,

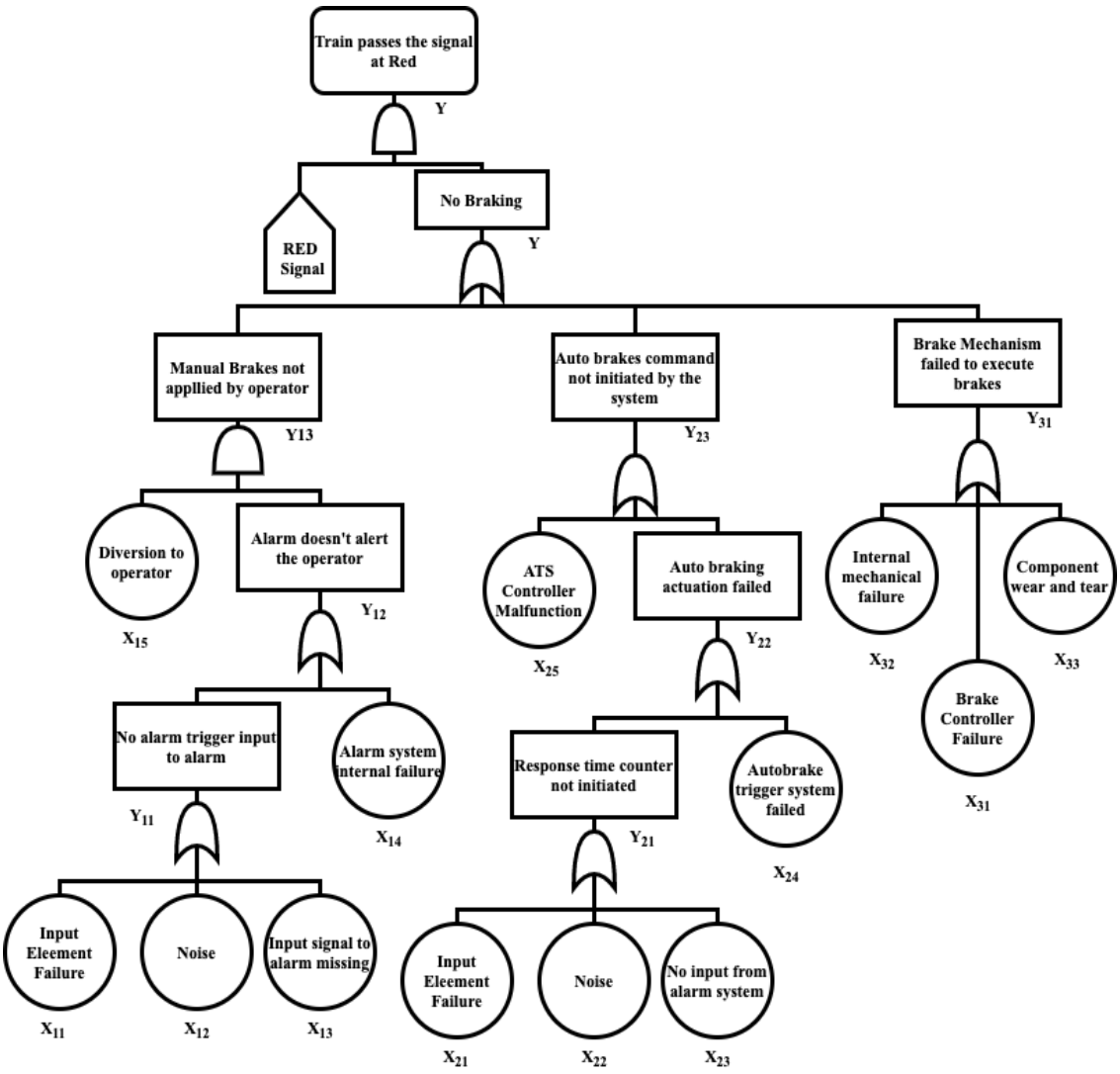


Figure 6-3 Conventional FTA of Onboard ATS

or the fault event resulted from a combination of other faults through logic gates. External events are shown as a pentagon shape.

6.1.4 Quantitative analysis

For quantitative analysis, we randomly assigned the probability of occurrence to each event and calculated the probabilities of the intermediate and top event using the Boolean logic of gates, as explained in section 4.5. For ease of understanding, each event in a tree got a unique code number based on the following convention.

Event code X_{mn}: Basic events.

Y_{mn}: Intermediate events.

Y: top event.

Where 'm' is the sub-tree number and '**n**' represents the n^{th} event in m^{th} sub-tree.

Table 6-1 presents the detail of all the basic events along with code number and probability assigned. The third column represents the code of the corresponding events in the new fault tree generated using the proposed method.

Table 6-1 probability of occurrence assigned to basic events in conventional FTA.

Sr. No.	Event's code in conventional FTA	Equivalent Event's code in New Fault Tree	Event description	Occurrence Probability
1.	X_{11}	$A_{13} + A_{14}$	Alarm input component failure	1.5×10^{-9}
2.	X_{12}	A_{11}	Noise	-
3.	X_{13}	A_{12}	Input Signal to alarm missing	5.2×10^{-10}
4.	X_{14}	A_{15}	The alarm system internal failure or alarm hardware failure	2.3×10^{-10}
5.	X_{15}	A_{16}	Diversion to the operator	1.3×10^{-8}
6.	X_{21}	$A_{22} + A_{23}$	Counter input component failure	3.1×10^{-9}

Sr. No.	Event's code in conventional FTA	Equivalent Event's code in New Fault Tree	Event description	Occurrence Probability
7.	$X_{22} = X_{12}$	-	Noise to counter	-
8.	$X_{23} = Y_{11}$	A_{21}	No input from the alarm system.	
9.	X_{24}	-	Auto Brake Trigger system failure	1.3×10^{-10}
10.	X_{25}	A_{25}	ATS controller malfunction	2.1×10^{-11}
11.	X_{31}	A_{31}	Brake controller failure	4.2×10^{-10}
12.	X_{32}	A_{32}	Brake mechanism internal failure	1.7×10^{-10}
13.	X_{33}	A_{33}	Brake mechanism component wear and tear	2.2×10^{-9}

Probability of intermediate events was calculated using the following formulas derived from the fault tree events and logic gates.

$Y_{11} = X_{11}+X_{12}+X_{13} = 1.5 \times 10^{-9} + 0 + 5.2 \times 10^{-10} = 2.02 \times 10^{-9}$

$Y_{12} = Y_{11}+X_{14} = 2.02 \times 10^{-9} + 2.3 \times 10^{-10} = 2.25 \times 10^{-9}$

$Y_{13} = Y_{12} * X_{15} = 2.25 \times 10^{-9} * 1.3 \times 10^{-8} = 2.93 \times 10^{-17}$

$Y_{21} = X_{21}+X_{22}+X_{23} = 3.1 \times 10^{-9} + 0 + 2.02 \times 10^{-9} = 5.02 \times 10^{-9}$

$Y_{22} = Y_{21}+X_{24} = 5.02 \times 10^{-9} + 1.3 \times 10^{-10} = 5.15 \times 10^{-9}$

$Y_{23} = Y_{22}+X_{25} = 5.15 \times 10^{-9} + 2.1 \times 10^{-11} = 5.17 \times 10^{-9}$

$Y_{31} = X_{31}+X_{32}+X_{33} = 4.2 \times 10^{-10} + 1.7 \times 10^{-10} + 2.2 \times 10^{-9} = 2.79 \times 10^{-9}$

$Y = Y_{13} + Y_{23} + Y_{31} = 2.93 \times 10^{-17} + 5.17 \times 10^{-9} + 2.79 \times 10^{-9} =$ **7.97×10^{-9}**

Y is the probability of occurrence of the top event in the conventional fault tree, and that came out to be 7.97×10^{-9}.

6.1.5 New Proposed method analysis of onboard ATS system

The proposed method is a combination of STAMP and FTA, where firstly STAMP is applied on the system and then fault tree is constructed using STAMP result. For STAMP application, the analyst used the 'STAMP workbench' tool developed by IPA japan. This procedure includes the following five steps.

1. Identifying Hazards
2. Construction of control structure.
3. Extraction of unsafe control actions (UCA)
4. Extraction of hazard causal factors (HCF).
5. Transformation of STAMP result into fault tree.

First four steps are the procedure of STPA and last step it the main idea of this research.

6.1.5.1 Identifying hazards

A hazard is a state of a system that, together with a particular set of worst-case environmental condition leads to a loss. For the considered system, the identified hazard is 'Train crosses the signal when it is red' and in a worst-case scenario, when another train is present immediately ahead of the signal, leads to a collision that can cause huge losses.

6.1.5.2 Construction of control Structure

A control structure is a system model that is composed of feedback control loops. Figure 6-4 Shows the control structure constructed for onboard ATS where square boxes represent subsystems or components. All red arrows indicate the control and its direction, whereas the blue line is for feedbacks. Each arrow has a description attached either above or below it, that explains the control or feedback associated with it.

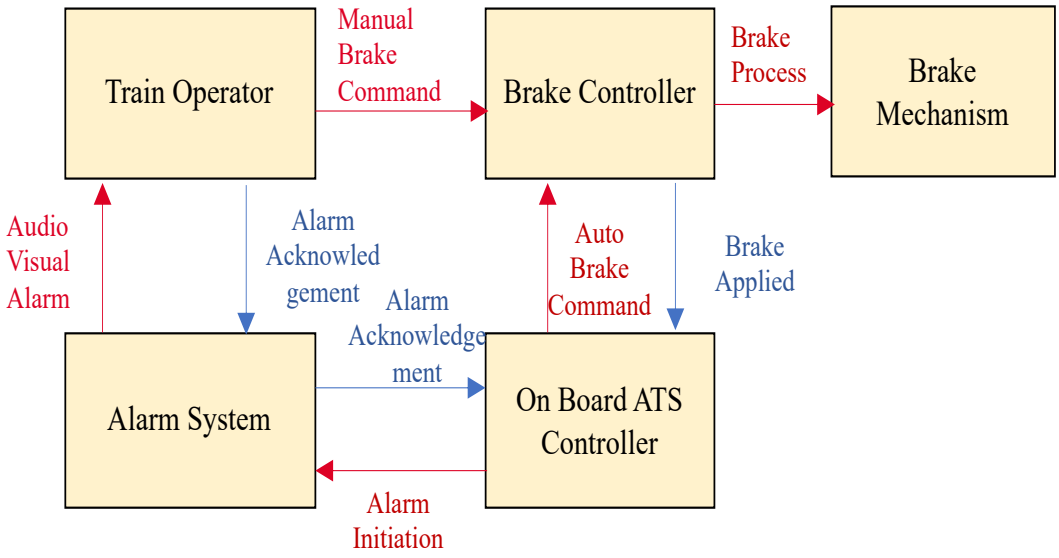


Figure 6-4 Control structure for o board ATS

6.1.5.3 Extraction of UCA

An unsafe control action is control action that, in a particular context and worst-case environment, leads to hazard [14]. UCA table is generated considering all the control action in the following manner that can lead to an unsafe situation.

1. Not providing a control action lead to a hazard.
2. The control provided in an unsafe way leads to hazard.
3. Safe control provided at the wrong time.
4. Safe control provided for the inappropriate duration.

Table 6-2 shows the UCA table for onboard ATS. Column named 'Control action' contains the control action present in the control structure. Each of these control actions is examined against the four guide words, not provided, provided caused hazard, too early/too late; and stopped too soon/applied too soon, as shown in last four columns. Total 14 UCAs were identified in this case and all UCAs are written in red colour in the table along with specific UCA number.

Table 6-2 UCA for on board ATS

No.	Control Action	From	To	CA Providing Condition	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
1	Alarm Initiation	On Board ATS System	Alarm System	When Siganl is RED operate the warning alarm	(UCA1-N-1) Alarm system doesn't Initiate alarm. [SC1]	(UCA1-P-1) No Alarm actuation when signal is RED [SC2]	(UCA1-T-1) Late Alarm actuation when signal is RED [SC1]	x
2	Audio Visual Alarm	Alarm System	Train Operator	Alert driver when Signal is RED.	(UCA2-N-1) No alarm to operator when signal is RED [SC2]	x	(UCA2-T-1) Late warning to Operator when signal is RED [SC1]	x
3	Manual Brake command	Train Operator	Brake Controller	Mnaual Braking when signal is RED	(UCA3-N-1) No Braking [SC1]	x	(UCA3-T-1) Braking when signal already inside Tain minimum stopping distance. [SC1]	(UCA3-D-1) Brake time too small to stop the train. [SC1]
4	AUTO Brake command	On Board ATS System	Brake Controller	AUTO brake initiation when driven not reponding to warning	(UCA4-N-1) No Brake command when inaction by Operator. [SC1]	x	(UCA4-T-1) Delayed Brake command when no action by Operator. [SC1]	x
5	Brake Process	Brake Controller	Brake Mechanism	Braking when brake initiation cammand is received	(UCA5-N-1) No Braking [SC1]	(UCA5-P-1) Usuccessful Braking [SC1]	(UCA5-T-1) Braking when train alredy inside minimum braking distance. [SC1]	(UCA5-D-1) Braking not for enough duration to stop the train [SC1]

6.1.5.4 Extraction of HCFs

Hazard causal factor or HCF describes the reason along with scenarios that leads to unsafe control actions. Following two types of loss-scenarios are considered in HCF table preparation. [14]

1. Why would unsafe control action occur?
2. Why would control action be improperly executed, or not executed, leading to hazard?

Table 6-3 shows the HCF table prepared for onboard ATS system.

Table 6-3 HCF for on board ATS

UCA	ID	HCF	Hint Word	Scenario
UCA1-N-1	HCF1-N-1-1	Missing or wrong Input to on Board ATS	(1) Control input or external information wrong or missing	1. Signal aspect information fed to ATS controller from wayside is different from the actual signal aspect. 2.No information about signal aspect provided from the wayside.
	HCF1-N-1-2	ATS system algorithm inefficient	(2) Flaws in creation, process changes, incorrect modification or adaption	1. Logic defined tan o issue the alarm when the signal is red has error or inefficient.
	HCF1-N-1-3	ATS system malfunction	(4) Component failures, Changes over time	1. Hardware failure. 2. Software error. 3. loose connections.

UCA	ID	HCF	Hint Word	Scenario
UCA1-T-1	HCF1-T-1-1	Delay in issuing command by ATS	(7) Delayed operation	1. ATS system slow processing due to the slow component or complicated procedure. 2. Delayed Input to ATS system 3. Larger Response time of ATS system
UCA1-D-1	HCF1-D-1-1	Alarm duration too short.	(8) An inappropriate, ineffective or missing control action	1. logic error. 2. loose connection
UCA2-N-1	HCF2-N-1-1	No or wrong actuating signal to the alarm system	(1) Control input or external information wrong or missing	1. No or wrong signal from ATS 2. Loose connection
	HCF2-N-1-2	Alarm failure	(4) Component failures, Changes over time	3. faulty components
UCA2-P-1	HCF2-P-1-1	Wrong place of installation or alarm	(2) Flaws in creation, process changes, incorrect modification or adaption	1. Audio alarm too low to be heard by the operator. 2. Audio too loud to cause inconvenience the operator. 3. Visual alarm not in continuous sight of the operator.
UCA2-T-1	HCF2-T-1-1	Longer response time of the alarm.	(2) Flaws in creation, process changes, incorrect modification or adaption	1. The alarm system is taking a long time to raise the alarm after receiving signal, overaged components.
	HCF2-T-1-2	Delayed operation of the alarm	(7) Delayed operation	1. The delayed output from ATS. 2. Temporary loose connection.
UCA2-D-1	HCF2-D-1-1	Insufficient command duration	(8) An inappropriate, ineffective or missing control action	1. Time of command pulse too small to be sensed by the system.
	HCF2-D-1-2	Intermittent disconnection	(4) Component failures, Changes over time	1. Loose connection over time and causing disconnection.
UCA3-N-1	HCF3-N-1-1	Considering no braking required	(1) Not Providing (forgetting the operation)	1. Lack of Knowledge.
	HCF3-N-1-2	Overlooking the brake alarm	(1) Not Providing (forgetting the operation)	1. Ignorance
UCA3-P-1	HCF3-P-1-1	Unable to understanding required braking power.	(2) Providing causes hazard (failure)	1. Lack of Training.
	HCF3-P-1-2	Faulty Instruction to the brake controller.	(4) Commission Error	1. Inadequate algorithm.
	HCF3-P-1-3	Faulty instruction to the brake controller.	(5) Instructions (Operation: switches, keyboard.)	1. Transmission error. 2. wrong calibration.
UCA3-T-1	HCF3-T-1-1	Delayed Response by the operator.	(5) Instructions (Operation: switches, keyboard.)	1. the operator's reaction time is longer due to some Physical/Mental health issue.
	HCF3-T-1-2	Delayed Instruction.	(5) Instructions (Operation: switches, keyboard.)	1. Switch operation time or response time longer. 2. Long and complicated procedure.
UCA3-D-1	HCF3-D-1-1	Braking for the insufficient duration.	(2) Providing causes hazard (failure)	1. Lack of system knowledge/training

UCA	ID	HCF	Hint Word	Scenario
UCA4-N-1	HCF4-N-1-1	Wrong feedback from the alarm system.	(1) Control input or external information wrong or missing	1. ATS gets alarm acknowledgement feedback from the alarm system even when alarm not acknowledged by the operator.
	HCF4-N-1-2	No instruction from ATS	(8) An inappropriate, ineffective or missing control action	1. Control logic inefficient.
	HCF4-N-1-3	No Instruction from ATS	(4) Component failures, Changes over time	1. Hardware failure. 2. Software error. 3. loose connection over time.
UCA4-T-1	HCF4-T-1-1	The delayed output from ATS controller	(8) An inappropriate, ineffective or missing control action	1. Complex decision making process. 2. inefficient logic error.
	HCF4-T-1-2	Delayed Input to ATS controller	(7) Delayed operation	1. Delayed Input from the timer. 2. Timer error.
UCA4-D-1	HCF4-D-1-1	Brake command duration from ATS too small.	(2) Flaws in creation, process changes, incorrect modification or adaption	1. Control Logic error.
UCA5-N-1	HCF5-N-1-1	No or wrong input to Brake controller.	(1) Control input or external information wrong or missing	1. Brake lever Sensor failure. 2. The wrong command from ATS
	HCF5-N-1-2	No output or wrong output from Brake controller.	(8) An inappropriate, ineffective or missing control action	1. Inefficient or flawed logic.
	HCF5-N-1-3	Brake mechanism failure.	(4) Component failures, Changes over time	1. component failure.
	HCF5-N-1-4	Brake Mechanism failure.	(2) Flaws in creation, process changes, incorrect modification or adaption	1. Faulty braking mechanism.
UCA5-T-1	HCF5-T-1-1	The delayed output from Brake controller.	(7) Delayed operation	1. design flaw. 2. Temporary loose connection
	HCF5-T-1-2	Delayed operation by the Brake mechanism	(7) Delayed operation	1. Slow Brake mechanism. (Design flaw)
UCA5-D-1	HCF5-D-1-1	Inefficient braking due to short time.	(8) An inappropriate, ineffective or missing control action	1. inefficient or flawed logic.

6.1.5.5 Transformation of STAMP result into fault tree

As described in chapter 4, the fault tree was constructed taking the input from the tables generated by the STPA application on the system. In the first step, all the UCAs from the UCA table of STAMP were mapped in tree form, illustrating the relationships among various UCAs events. In the next step, HCFs from HCF table were inserted at the appropriate position, using the knowledge of FTA and system working, showing the relationship of each HCF with other HCF and UCAs. Advantage of following this procedure is that it covers all possible hazardous events as all the events are identified by STAMP using a systematic procedure, and this tree formation is just manipulation of result from one format to another format. If required, scenarios can be added to the fault tree for a better understanding of event flow. Figure 6-5 and Figure 6-6 shows the fault tree constructed using this transformation.

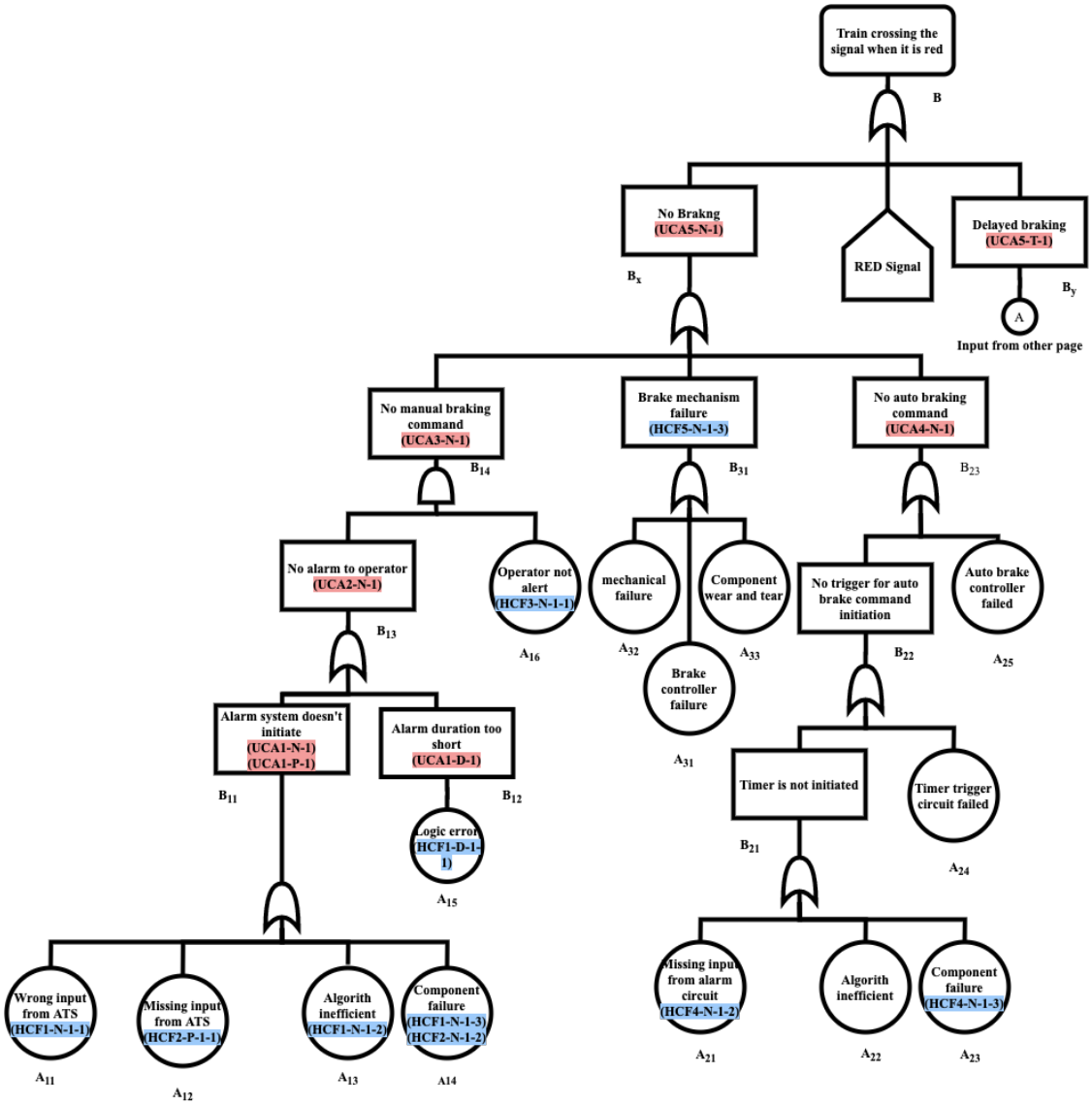


Figure 6-5 Fault Tree for on-board ATS using Newly Proposed Method (i)

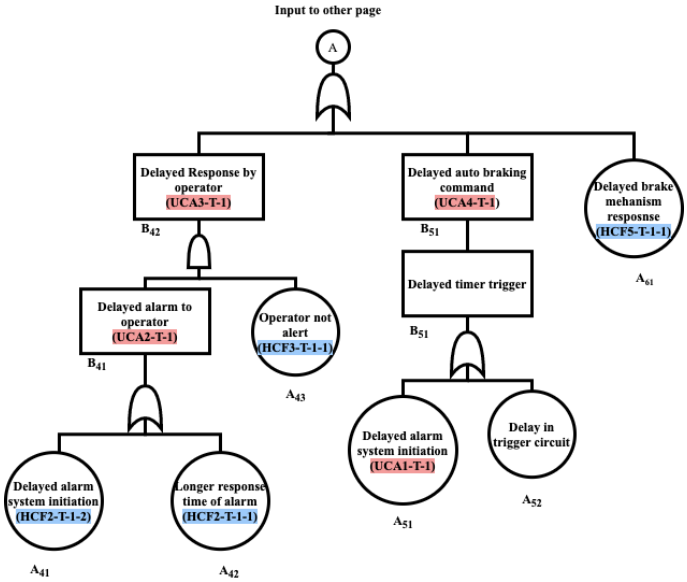


Figure 6-6 Fault Tree for on-board ATS using Newly Proposed Method (ii)

6.1.5.6 Quantitative analysis

Similar to the conventional method, quantitative analysis was done for the fault tree prepared using the proposed method. We used a similar nomenclature scheme to assign code numbers to events. However, to avoid any confusion in event identification, A and B alphabets were used in place of X and Y. The coding scheme is as follows.

Event code A_{mn}: Basic events.

B_{mn}: Intermediate events.

B: top event.

Where 'm' is the sub-tree number and '**n**' represents the n^{th} event in m^{th} sub-tree.

Table 6-4 shows the basic events for new fault tree along with event code and the probability of occurrence assigned to each basic event. For making the quantitative more reliable, the probability of any event in new fault tree has been kept the same as of the equivalent event in the conventional method, if the same exists.

Table 6-4 probability of occurrence assigned to basic events in the new method

[15]	**Event's code in New Fault Tree**	**Equivalent Event's code in conventional FTA**	**Event description**	**Probability**
1.	A_{11}	X_{12} or another event	Wrong Input from ATS	1.9×10^{-11}
2.	A_{12}	X_{13}	Missing Input from ATS	5.2×10^{-10}
3.	A_{13}	X_{11}	Alarm Algorithm Inefficient	1.5×10^{-9} (Together for both)
4.	A_{14}		Alarm Component failure	
5.	A_{15}	X_{14}	The alarm system Logic error	2.3×10^{-10}
6.	A_{16}	X_{15}	the operator not alert	1.3×10^{-8}
7.	$A_{21} = B_{11}$	X_{23} or another event	Missing Input from alarm circuit	1.9×10^{-11}
8.	A_{22}	X_{21}	Timer Algorithm Inefficient	3.1×10^{-9}
9.	A_{23}		Timer component failure	
10.	A_{24}	-	Timer trigger circuit fail	1.3×10^{-10}
11.	A_{25}	X_{25}	Auto Brake controller failed	2.1×10^{-11}
12.	A_{31}	X_{31}	Brake controller failure	4.2×10^{-10}
13.	A_{32}	X_{32}	Brake mechanism mechanical failure	1.7×10^{-10}

[15]	Event's code in New Fault Tree	Equivalent Event's code in conventional FTA	Event description	Probability
14.	A_{33}	X_{33}	Brake mechanism component wear and tear	2.2×10^{-9}
15.	A_{41}	-	Delayed the alarm system initiation	1.6×10^{-10}
16.	A_{42}	-	Longer response time of the alarm	2.1×10^{-9}
17.	$A_{43} = A_{16}$	X_{12}	the operator not alert	1.3×10^{-8}
18.	A_{51}	-	Delayed the alarm system initiation	1.6×10^{-10}
19.	A_{52}	-	Delay in the trigger circuit	1.7×10^{-9}
20.	A_{61}	-	Delayed brake mechanism response.	3.1×10^{-10}

The probability of the intermediate and top events was calculated by the formulas generating with events and logic gates. Details are as follows.

$B_{11} = A_{11} + A_{12} + A_{13} + A_{14} = 1.9 \times 10^{-11} + 5.2 \times 10^{-10} + 1.5 \times 10^{-9} = 2.03 \times 10^{-9}$

$B_{12} = A_{15} = 2.3 \times 10^{-10}$

$B_{13} = B_{11} + B_{12} = 2.03 \times 10^{-9} + 2.3 \times 10^{-10} = 2.26 \times 10^{-10}$

$B_{14} = B_{13} * A_{16} = 2.26 \times 10^{-10} * 1.3 \times 10^{-8} = 2.94 \text{ X } 10^{-18}$

$B_{21} = A_{21} + A_{22} + A_{23} = 1.9 \times 10^{-11} + 3.1 \times 10^{-9} = 3.12 \times 10^{-9}$

$B_{22} = B_{21} + A_{24} = 3.12 \times 10^{-9} + 1.3 \times 10^{-10} = 3.23 \times 10^{-9}$

$B_{23} = B_{22} + A_{25} = 3.23 \times 10^{-9} + 2.1 \times 10^{-11} = 3.25 \times 10^{-9}$

$B_{31} = A_{31} + A_{32} + A_{33} = 4.2 \times 10^{-9} + 1.7 \times 10^{-9} + 2.2 \times 10^{-9} = 2.79 \text{ X } 10^{-9}$

$B_{41} = A_{41} + A_{42} = 1.6 \times 10^{-9} + 2.1 \times 10^{-9} = 2.26 \text{ X } 10^{-9}$

$B_{42} = B_{41} + A_{43}$ $= 2.26 \text{ X } 10^{-9} * 1.3 \text{ x } 10^{-8} = 2.94 \text{ X } 10^{-17}$

$B_{51} = A_{51} + A_{52}$ $= 1.6\text{x}10^{-10} + 1.7\text{x}10^{-9} = 1.86 \text{ X } 10^{-9}$

$B_x = B_{14} + B_{23} + B_{31}$ $= 2.94 \text{ X } 10^{-18} + 3.25 \text{ x } 10^{-9} + 2.79 \text{ X } 10^{-9} = 6.04 \text{ x } 10^{-9}$

$B_y = B_{42} + B_{51} + A_{61}$ $= 2.94 \text{ X } 10^{-17} + 1.86 \text{ X } 10^{-9} + 3.1\text{x}10^{-10} = 2.17 \text{ x } 10^{-9}$

$B = B_x + B_y$ $= 6.04 \text{ x } 10^{-9} + 2.17 \text{ x } 10^{-9} = \mathbf{8.21 \text{ x } 10^{-9}}$

'B' is the probability of occurrence for the top event as per the new method. This probability using the newly proposed method came out higher than the one using the conventional method. Chapter Result and Discussion covers the detailed discussion about this.

6.2 Electronic Interlocking

Interlocking is said to be the backbone of the safe train operation. It is an arrangement of signal apparatus that ensures prevention of conflicting movement of trains through an arrangement of tracks such as the junction of stations [15]. It ensures that signal doesn't show the proceed (green) aspect unless all the safety conditions, such as no conflicting signal is down, no conflicting route is set, all the tracks in a proposed route are unoccupied, all the switches are set and locked in required direction and route is set and locked; are met. Interlocking also ensures that the movement of trains succeeds each other in a proper sequence. [16]

Interlockings have a long history of use as mechanical interlockings, electro-mechanical interlocking and relay interlocking. Relay interlocking has been very popular and is still in use over vast networks around the world. However, in recent decades, due to development in software, most of the new installations are using the Electronic interlocking, where software running over special-purpose control hardware replaces the wired networks of relays. Use of Electronic interlocking have significantly reduced the installation space requirement and efforts needed in case of alterations.

6.2.1 System description

Figure 6-7 shows a typical illustration of Electronic Interlocking. The logic unit is the central processing unit that contains all the logic that does the soft realization of relays and its wiring used in relay interlocking. This unit is responsible for all the decision making for the operation of all signal apparatus. It takes the Input from operation panel as a command to operate the switch, level crossing, set or release the route, and other operations. It also gathers the real-time status of all field gears that include all track circuit status, switches position, level crossing status, current aspect of all signal. Based on this information, the logic unit decides on the execution of a command request from the interlocking panel. The remote unit acts as a mediator between the central logic unit and signalling apparatuses installed in the field. The central logic unit can have multiple the remote units attached to it. Signalling apparatuses are usually installed at various remote locations and connected to the remote unit through copper cables. Operating panel is provided with the operator to control the train movement.

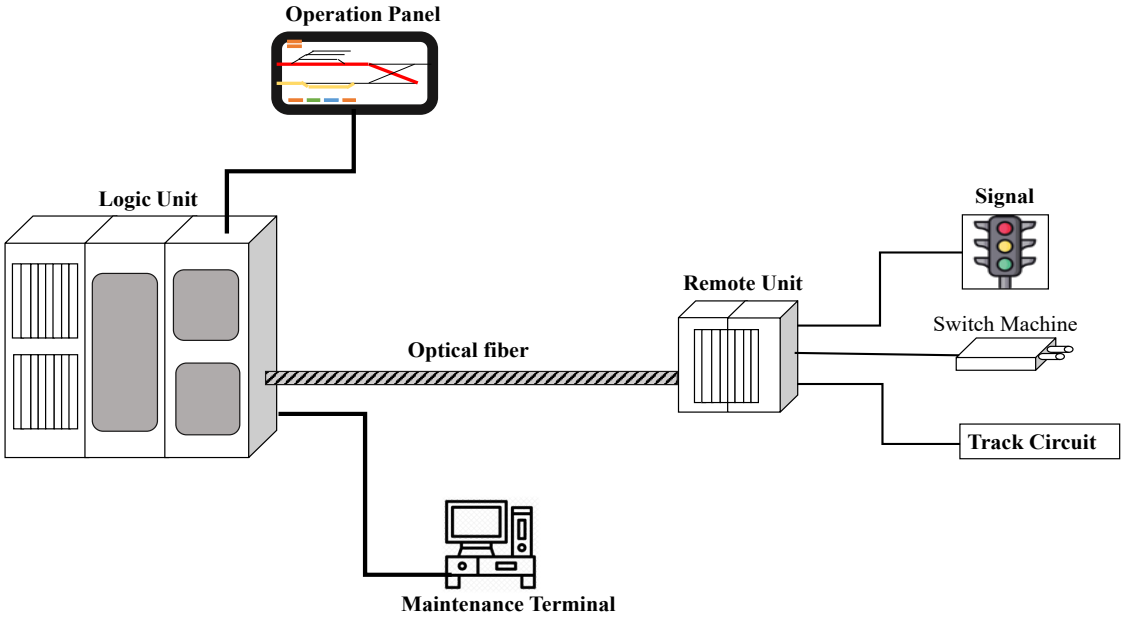


Figure 6-7 Electronic Interlocking

Maintenance terminal collects all the status and diagnosis data from the logic unit for system monitoring and maintenance purpose.

6.2.2 Block diagram

Figure 6-8 shows the block diagram of the electronic interlocking. Software inside the logic unit implements all the required restrictions per railways signalling principles. Some of the basic principles of the signalling are as follows.

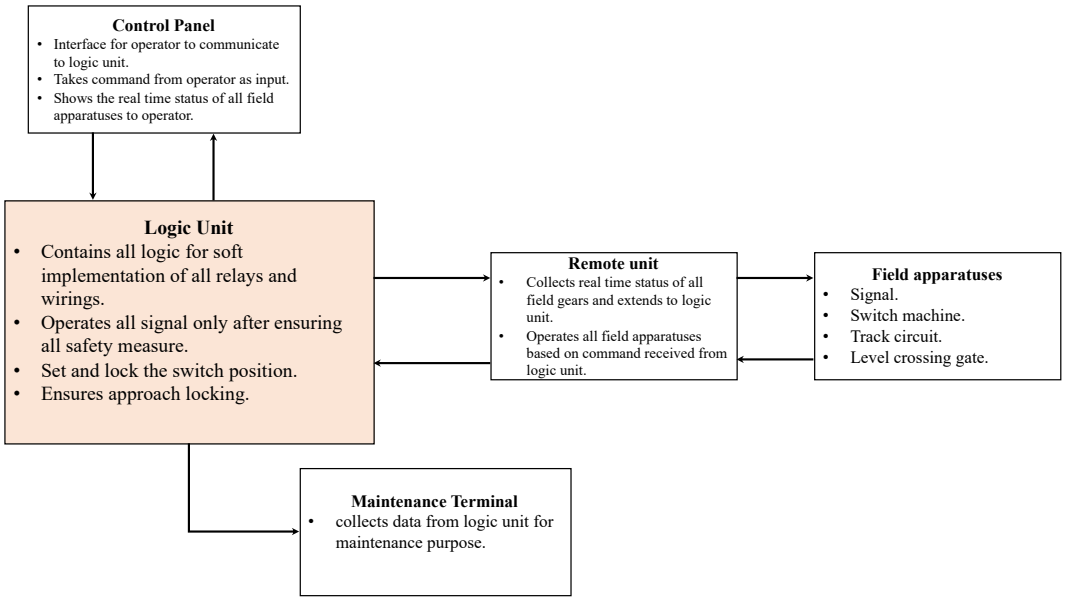


Figure 6-8 Electronic Interlocking block diagram

1. It shall not be possible to take any signal to 'OFF' unless
   a) All the facing points are correctly set. (Point locking)
   b) All the facing points are locked.
   c) All interlocked level crossing gates are closed and locked against road traffic.
   d) The isolation is working.
   e) The route is set and locked (Route locking)
2. Once the signal has been taken OFF, it must not be possible to do any of the following unless the signal has first been put back to the 'ON' position.
   a) Alter the position of the relevant point.
   b) Unlock the relevant facing point.
   c) Unlock and open the level crossing gate.
   d) Disturb the isolation.
3. It must not be possible to take 'OFF' at the same time any two fixed signals, which may lead to any conflicting movement.
4. Where feasible, the points shall be so interlocked as to avoid any conflicting movement.
5. In case of a track circuited yard, it shall not be possible to operate the point in case of point zone track circuit is down or occupied. (Track locking)
6. It shall be possible to cancel and release the route only if
   a) The train has not entered in approach section (in case of entirely track circuited section)
   b) Predefined time has not elapsed (in case of dead approach).

The remote unit can collect all the information from the field apparatus in the form of voltage & current and can transmit this information to the logic unit over the optical fibre. Similarly, it can receive the various command to operate signalling apparatus, from the logic unit over the optical fibre and can extend the voltage and current over copper cables to operate the gears. Use of the remote unit dramatically reduces the need for copper cable laying over long distances and cable maintenance work. It makes the installation and failure diagnosis easier.

Operating panel is provided with the operator to control the train movement. All the intended route commands are given from control panel and interlocking ensure safety in the execution of those commands. The required statuses are also available on the operating panel to give information about the status of all signalling apparatus and location of all the trains in its controlling area.

6.2.3 Conventional FTA analysis of Electronic Interlocking

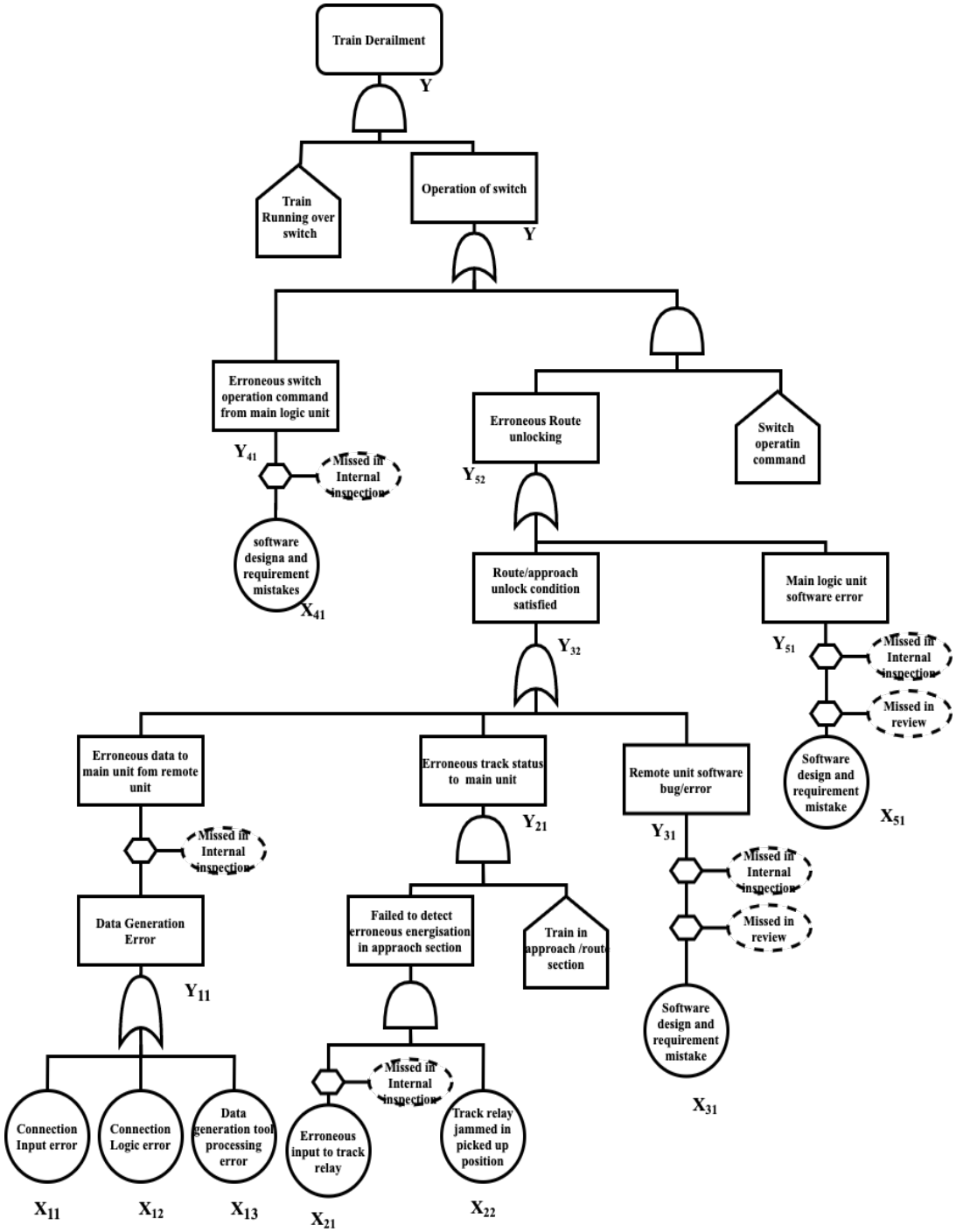


Figure 6-9 Conventional FTA for Electronic Interlocking System.

Electronic interlocking has a wide range of functions that include point locking, route locking, approach locking, real-time status monitoring to ensure safe and smooth train operation. That is why it can have many hazardous top events such as head-on

collision, real-on collision, train derailment, point trail through. In this part, we considered only one top event, and that is train derailment due to erroneous switch operation. The fault tree illustrates how an erroneous switch operation command can erroneously be executed by Interlocking system while a train is running over the switch or approaching towards the switch. Figure 6-9 shows the conventional FTA for Electronic Interlocking. This fault tree is deducing many reasons for the top event in the form of hardware faults, software faults, operational faults.

6.2.3.1 Quantitative analysis

Like the previous case of onboard ATS, quantitative analysis was done to find out the probability of occurrence of the top event. The occurrence probability was assigned to all the primary events, and the probabilities of intermediate and top events were calculated using the Boolean logic. Table 6-5 shows the description of all the primary events along with the code and the assigned occurrence probability. Here also, the third column shows the code for the equivalent event in the fault tree generated by the proposed method.

Table 6-5 probability of occurrence assigned to basic events in conventional FTA

Sr. No.	Event's code in conventional FTA	Equivalent Event's code in New fault tree	Event's description	Probability
1.	X_{11}	A_{11}	Connection input error to the remote unit on the field equipment side	1.1×10^{-9}
2.	X_{12}	A_{12}	Connection logic error on field unit side	2.1×10^{-10}
3.	X_{13}	A_{21}	Data tool processing error. (A_{21} has a broader scope than X_{13} because data processing tool is just one part of communication protocol)	1.7×10^{-10}
4.	X_{21}	A_{13}	Erroneous Input to track relay. (it seems to have a wider scope than A_{13} as it may also include a wrong connection in the field)	0.7×10^{-9}

Sr. No.	Event's code in conventional FTA	Equivalent Event's code in New fault tree	Event's description	Probability
5.	X_{22}	A_{14}	Track relay jammed in pick up position	0.9×10^{-9}
6.	X_{31}	A_{61}	Software design and requirement mistakes in the remote unit	0.4×10^{-9}
7.	X_{41}	A_{71}	Software design and requirement mistake and causing erroneous point operation command	1.3×10^{-10}
8.	X_{51}	A_{41}	Software design and requirement error in the main logic unit causing erroneous route release	0.5×10^{-9}

For the probability of occurrence of intermediate and top events following formulas, derived from events and logic gates were used.

$Y_{11} = X_{11} + X_{12} + X_{13} = 1.1 \times 10^{-9} + 2.1 \times 10^{-10} + 1.7 \times 10^{-10} = 1.5 \times 10^{-9}$

$Y_{21} = X_{21} + X_{22} = 0.7 \times 10^{-9} + 0.9 \times 10^{-9} = 1.6\ 10^{-9}$

$Y_{31} = X_{31} = 0.4 \times 10^{-9}$

$Y_{32} = Y_{11} + Y_{21} + Y_{31} = 1.5\ X\ 10^{-9} + 1.6\ 10^{-9} + 0.4 \times 10^{-9} = 3.5 \times 10^{-9}$

$Y_{41} = X_{41} = 1.3 \times 10^{-10}$

$Y_{51} = X_{51} = 0.5 \times 10^{-9}$

$Y_{52} = Y_{32} + Y_{51} = 3.5 \times 10^{-9} + 0.5 \times 10^{-9} = 4 \times 10^{-9}$

$Y = Y_{41} + Y_{52.} = 1.3 \times 10^{-10} + 4 \times 10^{-9} =$ **4.1×10^{-9}**

6.2.4 New Proposed method analysis of Electronic Interlocking

Same procedure, as done in case of onboard ATS, was applied on the Electronic Interlocking also for application newly proposed method.

6.2.4.1 Identifying Hazards

A hazard is a state of a system that, together with a particular set of worst-case environmental condition leads to a loss. Some hazards for EI includes train derailment while passing over the switch, head-on collision, rear on collision. Here, analyst chose only one hazard, and that is 'train derailment while passing over the switch.'

6.2.4.2 Construction of control structure

Figure 6-10 shows the control structure produced using the STAMP workbench tool.

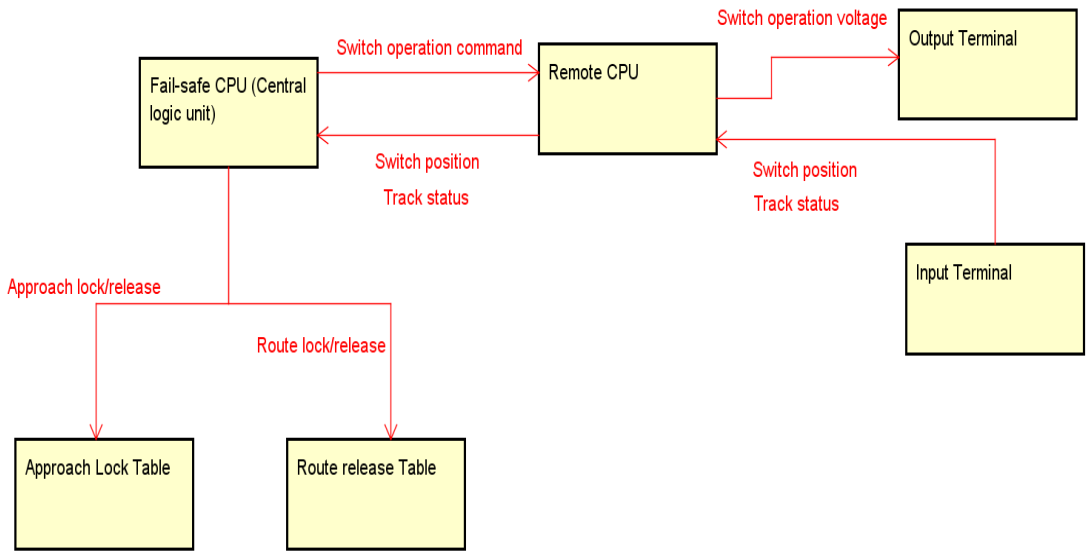


Figure 6-10 Control Structure for Electronic Interlocking.

6.2.4.3 Extraction of UCA

Table 6-6 shows the UCA table for the EI system prepared with the help of the control structure.

Table 6-6 UCA Table Interlockingcgkng Interlocking.

No	CA	From	To	CA Providing Condition	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
1	Switch operation command	Fail-safe CPU (Central logic unit)	The remote CPU	The train is running on route and switch operation command is extended from the central unit.	X	(UCA1-P-1) Erroneous switch command from the main logic unit might cause switch operation under the wheel or when the route is locked, resulting in derailment or collision.	X	X
2	Switch operation voltage	The remote CPU	Output Terminal	The train is running on route and switch operation voltage is extended from the remote unit.	X	(UCA2-P-1) Erroneous switch operation command from the remote unit may cause the switch to operate under the wheel or when the route is locked, resulting in derailment or collision.	X	X
3	Track status	The remote CPU	Fail-safe CPU (Central logic unit)	Various track, signal and point status information is transmitted in multiplexed signal form from the remote unit to the main logic unit.	X	(UCA5-P-1) Erroneous track circuit status from the remote unit to the main logic unit may cause erroneous route release, erroneous approach lock release, erroneous switch operation and erroneous route setting and has the potential to lead to Collison or derailment.	(UCA5-T-1) Delayed track status can cause erroneous route unlocking.	X
4	Track status	Input Terminal	The remote CPU	Track circuit status is sent from track circuit status relay to the remote unit.	X	(UCA6-P-1) Erroneous track circuit status from track status relay to the remote unit may cause erroneous route release, erroneous approach lock release, erroneous switch operation and erroneous route setting and has the potential to lead to Collison or derailment.	(UCA6-T-1) Delayed Track circuit status may cause erroneous route unlocking	X
5	Approach lock/release	Fail-safe CPU (Central logic unit)	Approach Lock Table	To lock the route when the train is in the approach section	X	(UCA7-P-1) Erroneously route release when the train is in the approach section.	X	X

No	CA	From	To	CA Providing Condition	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
6	Route lock/release	Fail-safe CPU (Central logic unit)	Route release Table	To ensure no gear movement in route when the route is set.	X	(UCA8-P-1) Erroneous route release when the train is running on the route.	X	X

6.2.4.4 Extraction of HCF

Table 6-7 shows the HCF table for Electronic Interlocking system.

Table 6-7 HCF Table for Electronic Interlocking

UCA	ID	HCF	Hint Word	Scenario
UCA1-P-1	**HCF1-P-1-1**	Software design or requirement flaws	(2) Flaws in creation, process changes, incorrect modification or adaption	Wrong requirement identified during the initial design phase.
UCA2-P-1	**HCF2-P-1-1**	Communication protocol error	(2) Flaws in creation, process changes, incorrect modification or adaption	Wrong requirement identified during the initial design phase.
	HCF2-P-1-2	Data corruption due to noise or other reason	(10) Unidentified or out-of-range disturbance	Noise interference causing to erroneous signal.
UCA5-P-1	**HCF5-P-1-1**	Communication protocol error	(2) Flaws in creation, process changes, incorrect modification or adaption	Due to wrong Protocol design.
UCA5-T-1	**HCF5-T-1-1**	Communication delays due to protocol error or other issues	(14) Missing or wrong communication with another controller	A wrong protocol may cause communication delay
UCA6-P-1	**HCF6-P-1-1**	Software design error	(2) Flaws in creation, process changes, incorrect modification or adaption	A wrong software requirement of flaws in creation may cause software error
	HCF6-P-1-2	Erroneous input connection at the remote unit terminals	(14) Missing or wrong communication with another controller	A wrong connection may be during commissioning or maintenance.

UCA	ID	HCF	Hint Word	Scenario
	HCF6-P-1-3	False voltage feed to track relay.	(10) Unidentified or out-of-range disturbance	Induced voltage, poor insulation can cause the relay to pick up falsely.
	HCF6-P-1-4	Relay Stuck Up	(4) Component failures, Changes over time	A relay may get stuck up due to some mechanical failure.
UCA6-T-1	**HCF6-T-1-1**	Overaged relay, mechanical issues.	(4) Component failures, Changes over time	
	HCF6-T-1-2	Faulty voltage adjustment at the track	(9) Process input missing or wrong	When track voltage is higher than the nominal value, it may cause false pick up of track.
UCA8-P-1	**HCF8-P-1-1**	Software design or requirement error.	(2) Flaws in creation, process changes, incorrect modification or adaption	Wrong requirement identified during the initial design phase.

6.2.4.5 Transformation of STAMP result into fault tree

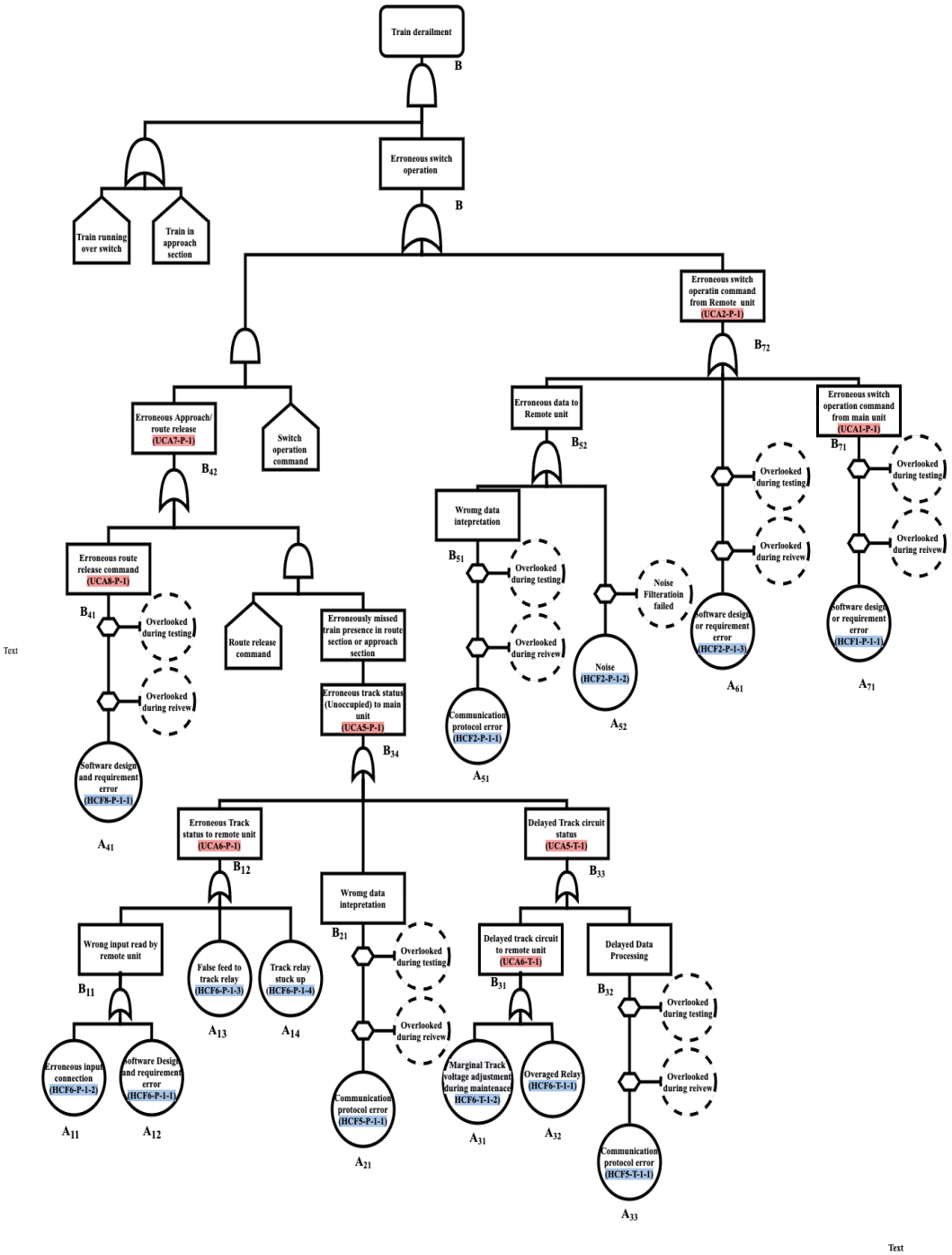


Figure 6-11 Fault Tree for Electronic Interlocking using Newly Proposed Method.

Figure 6-11 shows the fault tree prepared using the new method by taking the Input from the UCA table and HCF table prepared using the STAMP. The blue highlighted events were taken from the HCF table, and red highlighted events were from the UCA table.

6.2.4.6 Quantitative Analysis

For quantitative analysis, each basic event was assigned a probability equal to a similar event in the conventional FTA. For events having no similar event in conventional FTA, the probability was assigned randomly. Table 6-8 shows the description of all basic events of new fault tree along with event code and assigned probabilities. One column also shows the equivalent event's code in conventional FTA.

Table 6-8 Probability of occurrence assigned to basic events in new fault tree

Sr. No.	Event's code in New Fault Tree	Equivalent Event's code in conventional FTA	Event description	Occurrence Probability
1.	A_{11}	X_{11}	Erroneous input connection to the remote unit on the field side	1.1×10^{-9}
2.	A_{12}	X_{12}	Software design requirement error for the remote unit input terminal	2.1×10^{-10}
3.	A_{13}	X_{21}	False feed (Stray voltage/induced voltage) to track relay	0.7×10^{-9}
4.	A_{14}	X_{22}	Track relay stuck up due to contact welding or mechanical failure	0.9×10^{-9}
5.	A_{21}	X_{13}	Erroneous communication protocol causing wrong communication between the main unit and the remote	1.7×10^{-10}
6.	A_{31}		Track voltage set at margins on the higher side. Causing track relay to hang in picked up position for some time causing a **delay in real track**	0.1×10^{-9}

Sr. No.	Event's code in New Fault Tree	Equivalent Event's code in conventional FTA	Event description	Occurrence Probability
7.	A_{32}		Overaged relay taking time to drop due to mechanical issues **causing a delay in track status**	1.7×10^{-10}
8.	A_{33}		Communication protocol error taking longer than the required time to process communication between the main and the remote unit **Causing delay in communication** for real-time status.	0.1×10^{-9}
9.	A_{41}	X_{51}	Software design or requirement error in main logic unit leading to erroneous **route release** command	0.5×10^{-9}
10.	$A_{51} = A_{21}$	X_{13}	Erroneous communication protocol causing wrong communication between the main unit and the remote	1.7×10^{-10}
11.	A_{52}		Random noise creating interference with communication	0.1×10^{-9}
12.	A_{61}	X_{31}	Software design or requirement error for **the remote unit** causing erroneous command of point operation. (or wrong point operation)	0.4×10^{-9}
13.	A_{71}		Software design or requirement error the for **main logic unit** causing erroneous command of point operation. (or wrong point operation)	1.3×10^{-10}

Following formulas were used for the calculation of the probability of occurrence of intermediate and top events.

$B_{11} = A_{11} + A_{12} \quad = 1.1 \times 10^{-9} + 2.1 \times 10^{-10} = 1.3 \text{ X } 10^{-9}$

$B_{12} = B_{11} + A_{13} + A_{14} = 1.3 \times 10^{-9} + 0.7 \times 10^{-9} + 0.9 \times 10^{-9} = 2.9 \times 10^{-9}$

$B_{21} = A_{21} = 1.7 \times 10^{-10}$

$B_{31} = A_{31} + A_{32} = 0.1 \times 10^{-9} + 1.7 \times 10^{-10} = 0.3 \times 10^{-9}$

$B_{32} = A_{33.} = 0.1 \times 10^{-9}$

$B_{33} = B_{31} + B_{32.} = 0.3 \times 10^{-9} + 0.1 \times 10^{-9} = 0.4 \times 10^{-9}$

$B_{34} = B_{12} + B_{21} + B_{33} = 2.9 \times 10^{-9} + 1.7 \times 10^{-10} + 0.4 \times 10^{-9} = 3.5 \times 10^{-9}$

$B_{41} = A_{41} = 0.5 \times 10^{-9}$

$B_{42} = B_{34} + B_{41} = 3.5 \times 10^{-9} + 0.5 \times 10^{-9} = 4 \times 10^{-9}$

$B_{51} = A_{51} = 1.7 \times 10^{-10}$

$B_{52} = B_{51} + A_{52} = 1.7 \times 10^{-10} + 0.1 \times 10^{-9} = 0.3 \times 10^{-9}$

$B_{71} = A_{71} = 1.3 \times 10^{-10}$

$B_{72} = B_{52} + A_{61} + B_{71} = 0.3 \times 10^{-9} + 0.4 \times 10^{-9} + 1.3 \times 10^{-10} = 0.9 \times 10^{-9}$

$B = B_{42} + B_{72} = 4 \times 10^{-9} + 0.9 \times 10^{-9} = \mathbf{4.9 \times 10^{-9}}$

7. Result and Discussion

Detailed result analysis and discussion were made to check the effectiveness of both methods compared to each other. For qualitative comparison, both fault trees were compared based on the total number of events predicted, the number of basic and intermediate events identified. Also, a comparison was made for the number of software events, hardware events, time-delay events, human error events, communication-related events detected in both methods. As it was difficult to directly compare the events identified by both the methods because of the variation in event explanation and scope of coverage of each event, we generated a table keeping similar events from both fault trees together. All the events in the table have a detailed explanation and code number to avoid any kind of confusion during result discussion. For quantitative analysis, the difference in occurrence probability of top events, calculated during the application of both methods, were analyzed and method with better occurrence probability (higher failure rate) was declared as more effective.

Before going through the result, it is crucial to know that Table 7-1 and Table 7-3 are showing similar events and contains all the events from each fault tree. Also, some of the events are a repetition of some other event at a different level. While making the result comparison, repeated events were not counted, and that is why the total number of events used for result discussion might be lower than what is shown in tables of events correspondence.

Further, some events such as data connection error were counted under multiple categories due to nature of the events and that's why the sum of all events under different categories comes higher than the total number of events.

7.1 On-Board ATS

Table 7-1 shows the corresponding events in the fault tree prepared by the proposed method and the conventional FTA. Initial events having a serial number from 1 to 11 are the intermediate events, whereas serial number 12 onwards are the basic events. Table 7-2 shows the number of events covered under various categories by both methods.

Table 7-1 Event correspondence table for On-board ATS

Sr. No.		**The event in the proposed method**	**Corresponding Event in conventional FTA**	**Remarks**
1.	Intermediate Events	The alarm system doesn't initiate due to various reasons B_{11}	No alarm trigger Input to alarm Y_{11}	
2.		Duration of alarm is too short to be noticed due to design faults. $B_{12}=A_{15}$	NA	Identified by new method only
3.		No alarm to the operator when the signal is red due to various reasons. B_{13}	The alarm doesn't alert the operator. Y_{12}	
4.		No manual braking applied by the operator when the signal is red due to ignorance. B_{14}	Manual brake not applied by the operator. Y_{13}	
5.		NO automatic brake command when the signal is Red due to various issues B_{23}	Auto braking actuation failed. Y_{22the}	
6.		No Braking when the signal is red due to failure of both manual and automatic braking B_x	No Braking Y	
7.		Delayed alarm to the operator due to various issues. B_{41}	-	Time delay failures identified by the new method only.
8.		Delayed response by the operator either due	-	

Sr. No.		The event in the proposed method	Corresponding Event in conventional FTA	Remarks
		to delayed information. B_{42}		
9.		Delayed auto brake command due to delayed alarm or other reasons. B_{51}	-	
10.		Late braking due to delayed manual and auto braking. B_y		
11.		Brake mechanism failure due to various mechanical and other issues. B_{31}	Brake mechanism failed to execute brakes due to various reasons Y_{31}	
12.	Basic Events	Wrong Input from ATS due to issue on the trackside. A_{11}	Noise $X_{12} = X_{22}$	A_{11} has a broader scope as there might be various reason other than noise for wrong communication.
13.		Missing Input from ATS Due to communication break on trackside or some other reason. A_{12}	The input signal to the alarm is missing. X_{13}	
14.		Alarm Algorithm Inefficient. A_{13}	Alarm Input component failure. X_{11}	
15.		Alarm Component failure A_{14}		
16.		The alarm system Logic error. A_{15}	The alarm system internal failure or alarm hardware failure. X_{14}	

Sr. No.		**The event in the proposed method**	**Corresponding Event in conventional FTA**	**Remarks**
17.		The operator not alert. A_{16}	Diversion to the operator. X_{15}	
18.	Basic Events	Missing Input from alarm circuit. $A_{21} = B_{11}$	No input from the alarm system. $X_{23} = Y_{11}$	
19.		Timer Algorithm Inefficient. A_{22}	Counter input component failure. X_{21}	
20.		Timer component failure. A_{23}		
21.		Timer trigger circuit fail. A_{24}		
22.		Auto Brake controller failed to issue brake command. A_{25}	ATS controller malfunction. X_{25}	
23.		Brake controller failure to initiate brake mechanism. A_{31}	Brake Controller failure. X_{31}	
24.		Brake mechanism mechanical failure. A_{32}	Brake mechanism internal failure. X_{32}	
25.		Brake mechanism component wear and tear. A_{33}	Brake mechanism component wear and tear. X_{33}	
26.		Delayed initiation of the alarm system. A_{41}		Time- delay sequence failures identified by the new method only.
27.		Longer response time of the alarm. A_{42}		

Sr. No.		**The event in the proposed method**	**Corresponding Event in conventional FTA**	**Remarks**
28.		Operator not alert. A_{43} = A_{16}		
29.		Delayed alarm system initiation. A_{51}		
30.		Delay in trigger circuit. A_{52}		
31.		Delayed brake mechanism response. A_{61}		

Table 7-2 Event number comparison from both methods

Events	New FTA by Proposed Method	Conventional FTA
Total	25	21
Basic	15	13
Intermediate	10	8
Software related	11	9
Hardware-related	13	10
Time delay sequence	6	0
Communication-related	5	2
Human related	2	1

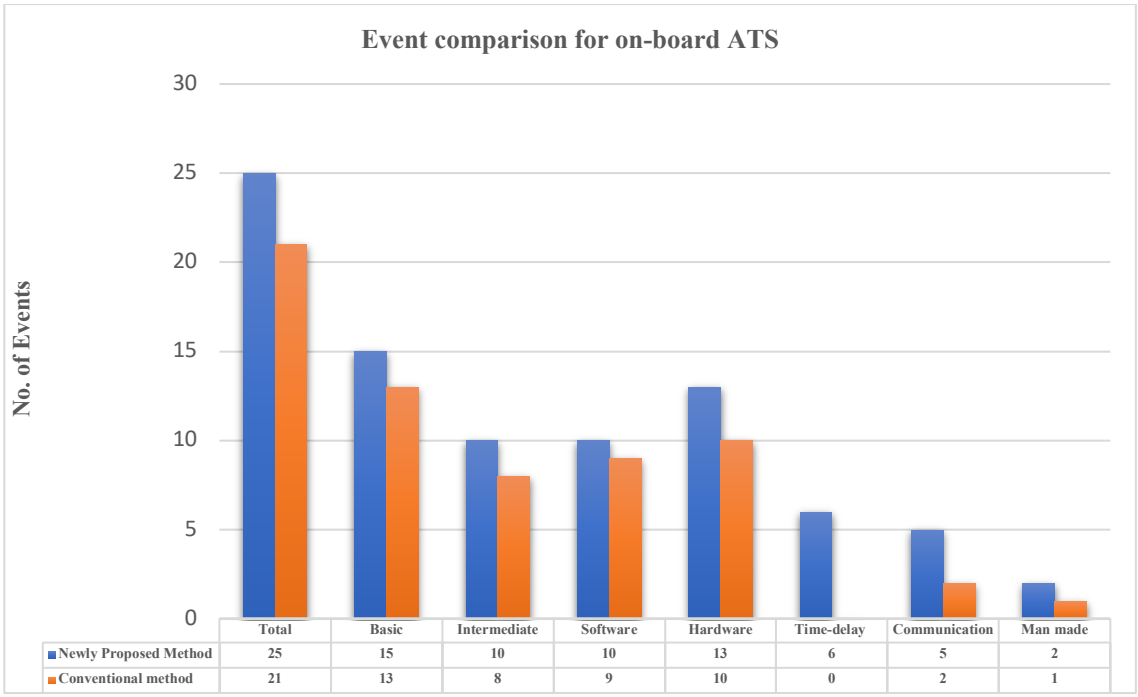


Figure 7-1 Event Comparison for onboard ATS

The result analysis of the comparison of Fault tree generated using the proposed method, and the conventional method is as follows.

1. The proposed method was able to predict all the events identified by the conventional method and skipped no event from conventional FTA.
2. The total number of events identified by the proposed method is significantly higher in number than the conventional methods. It is twenty-five as against the twenty-one identified by the conventional FTA.
3. Basic events are the events that are considered the root cause of any incident. They propagate through the system in association with other events or conditions to turn into an unsafe situation, the total number of basic events identified the new method fifteen against the thirteen from conventional FTA.
4. A total of ten intermediate events were identified by the proposed method against the eight from conventional FTA. Reason of this difference is a thorough explanation done by the proposed method that resulted in more events detailing in the fault tree.
5. For software-related faults, result from both events is almost identical with eleven and nine events identified by each.
6. The new method identified thirteen hardware failure, whereas the conventional FTA could point out only ten hardware related failure.

7. Delayed-time sequence failure is the most critical difference between the two methods. In this failure delayed information at any point leads to delay in all following sequential events. New method can easily predict all possible time delay hazard due to the use of guide words, control applied too late, applied too early, applied too long, or removed too early; in the STAMP application. Whereas, no guidewords and rules are available for conventional FTA, which makes it extremely difficult to predict time sequence hazard. That is why conventional FTA failed to identify any time delay failure and new method predicted the six events of this type. (add information about improved FTA also)
8. Total five communication-related failures, where the hazards occurred during information exchange, were identified by the new method, whereas the conventional method could identify two events.
9. Human related failure, where human negligence caused the events, are mainly the basic event in this analysis, and it is the only type where the conventional method identified more events than the new method. Conventional FTA identified two events as against the one event from the proposed method. All the human-related events identified in both the methods are related either installation negligence or laxity during maintenance. (Add reason for this difference and explain no demerit on new method)

7.2 Electronic Interlocking

Table 7-3 shows the corresponding events in the fault tree prepared by the proposed method and the conventional FTA. Initial events having a serial number from 1 to 9 are the intermediate events, whereas serial number 10 onwards are the basic events. Table 7-4 was generated for the number of events covered under various categories by both methods

.

Table 7-3 Event correspondence table for Electronic Interlocking

Sr. No		The event in the proposed method	Corresponding Even in conventional FTA	Remarks
1.	Intermediate Events	Erroneous Track status to the remote unit from the field. (B_{12}	Erroneous track stats to the remote unit Y_{21}	
2.		Delayed Track circuit status to the remote unit from the field side. B_{31}	-	These time sequence hazards were

Sr. No		The event in the proposed method	Corresponding Even in conventional FTA	Remarks
				identified by the new method only.
3.		Delayed Track circuit to the remote unit due to the remote unit internal processing delay. B_{33}	-	
4.		Erroneous Track circuit (unoccupied) to the main unit due to various reasons. B_{34}	Route/approach unlock condition satisfied (due to erroneous track status caused by various reasons) Y_{32}	
5.		Erroneous route release command from the main unit due software issue. B_{41}	Erroneous route unlocking command from the main unit due to software issue Y_{51}	
6.		Erroneous approach/Route release due to various reasons. B_{42}	Erroneous route and approach unlocking Y_{52}	
7.		Erroneous switch operation command from the main unit due to a software issue. B_{71}	Erroneous switch operation command from the main logic unit. Y_{41}	
8.		Erroneous switch operation command from the remote unit due to various reasons. B_{72}	(Not covered)	This command is not covered separately in conventional FTA; however, it can be considered to

Sr. No		The event in the proposed method	Corresponding Even in conventional FTA	Remarks
				be included in the event $Y_{41.}$
9.		Wrong data interpretation due to a communication protocol error. $B_{21}=A_{21}$	Erroneous data to the main unit from the remote unit due to various reasons including communication error Y_{11}	
10.	Basic Events	Erroneous input connection to the remote unit on the field side. A_{11}	Connection input error to the remote unit on the field equipment side. X_{11}	
11.		Software design requirement error for the remote unit input terminal. A_{12}	Connection logic error on field unit side. X_{12}	
12.		False feed (Stray voltage/induced voltage) to track relay. A_{13}	Erroneous Input to track relay. X_{21}	It seems to have a broader scope than A_{13} as it might include wrong communication in the field.
13.		Track relay stuck up due to contact welding or mechanical failure. A_{14}	Track relay jammed in picked up position. X_{22}	
14.		Erroneous communication protocol causing wrong communication between the main unit and the remote unit. A_{21}	Data Tool Processing error. X_{13}	A_{21} has wider scope thanX_{13} because data processing tool is just one part

Sr. No		The event in the proposed method	Corresponding Even in conventional FTA	Remarks
				of communication protocol.
15.		Track voltage set at margins on the higher side. Causing track relay to hang in picked up position for some time causing a delay in real track status. A_{31}		Time series sequence failures identified by the new method only.
16.		Overaged relay taking time to drop due to mechanical issues, causing a delay in track status. A_{32}		
17.		Communication protocol error taking longer than the required time to process communication between the main and the remote unit Causing delay in communication for real-time status. A_{33}		
18.		Software design or requirement error in main logic unit leading to erroneous route release command. A_{41}	Software design and requirement error in the main logic unit, causing erroneous route release.	

Sr. No		The event in the proposed method	Corresponding Even in conventional FTA	Remarks
19.		Erroneous communication protocol causing wrong communication between the main unit and the remote unit. $A_{51=21}$	Data generation error Y_{11} (one of the -reasons for wrong data is a communication error)	
20.		Random noise creating interference with communication. A_{52}	-	Noise not mentioned separately in conventional FTA, but it may be considered to be included in communication error.
21.		Software design or requirement error for the remote unit causing erroneous command of point operation. (or wrong point operation). A_{61}	Software design and requirement mistakes in the remote unit. X_{31} $=Y_{31}$	
22.		Software design or requirement error for the main logic unit, causing erroneous command of point operation. (or wrong point operation). A_{71}	Software design and requirement mistakes causing erroneous point operation command. X	

Table 7-4 Event comparison from both methods for Electronic Interlocking

Events	New FTA by Proposed Method	Conventional FTA
Total	19	14
Basic	13	8
Intermediate	9	9
Software related basic	7	4
Hardware related basic	2	1
Delayed Time sequence	5	0
Communication-related	3	1
Human related	2	1

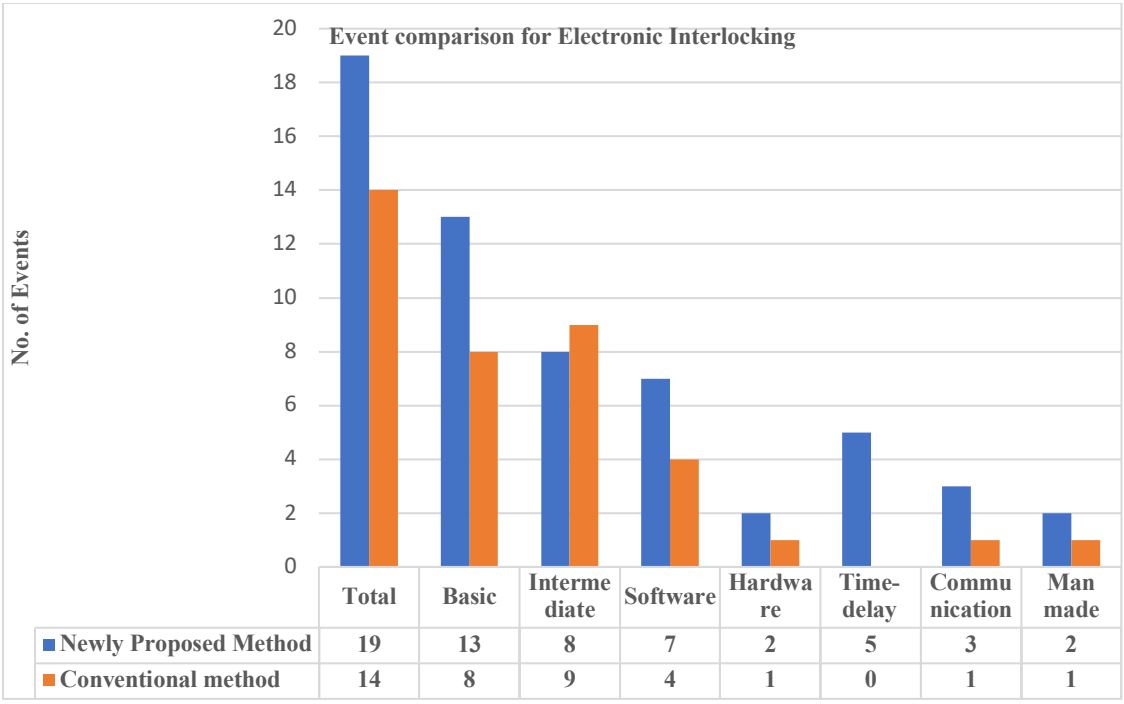


Figure 7-2 Event Comparison for Electronic Interlocking

The result analysis of the comparison of Fault tree generated using the proposed method, and the conventional method is as follows.

1. Total events identified by the conventional FTA is fourteen. In contrast, the proposed method could identify nineteen events in total, and this difference is mainly because of the time-delay sequence events identified by the new method. An important point to note here is that the proposed method was able to cover all the events identified by the conventional FTA
2. The new method could identify thirteen basic events as opposed to nine identified by the conventional method. Again, the reason is the additional time delay events identified by the new method.
3. Both the conventional method and the proposed method identified nine intermediate events.
4. The new method could identify seven software-related hazards as against the four identified by the conventional method.
5. The proposed method identified the two hardware-related events, and conventional method could identify only one event. The new event is related to the delayed response of the track relay due to over-ageing, which is a time-delay hazard.
6. Delayed-time sequence failure is the most crucial difference between the two methods. A time delay at any point leads to delay in all following sequential events. New method can easily predict all possible time delay hazard due to the use of guide words like control applied too late, applied too early, applied too long, or removed too early; in the STAMP application. Whereas, no guidewords and rules are available for conventional FTA, which makes it extremely difficult to predict time-delay hazard. That is why conventional FTA failed to identify any time delay failure and new method predicted the five events of this type.
7. Total three communication-related failures, where the hazards occurred during information exchange, were identified by the new method, whereas the conventional method could identify one event.
8. The new method identified two human-related events, whereas the conventional method could predict only one event. Additional event added by the new method is related to the delayed response by the operator.

The vital point from these results is that for both the target systems, the newly proposed method could identify all the events that were identified by the conventional FTA. Besides, the newly proposed method also identified time-delay events which are very

difficult to be identified by the conventional method. These two features point towards the superiority of the new method. Furthermore, the systematic procedure for failure identification makes the new method much easier compared to conventional FTA. This systematic procedure ensures to cover all hazardous event in tree formation in the new method.

In contrast, chances of missing an event in conventional FTA becomes higher with the increase in size and complexity of the system, in the absence of a systematic procedure. If we talk about the quantitative analysis, in case of the first target system, on-board ATS system, the probability of occurrence of the top event evaluated by the newly proposed method is 4.9×10^{-9}, which is 19.5% higher than 4.1×10^{-9}, predicted by the conventional method. Similarly, for the second system, probability of occurrence of the top event evaluated by the newly proposed method is 8.21×10^{-9}, which is 3.01% higher than 7.97×10^{-9}, predicted by the conventional method. Therefore, the higher probability showed by the newly proposed method for both the target systems proves its quantitative superiority as well. Therefore, it is concluded that both case studies establish the superiority of the new method as qualitatively as well as quantitatively.

8. Conclusion

Various safety evaluation methods are available for railway signalling system that complies with the international standard requirement of qualitative analysis along with quantitative analysis. One of the typical safety methods is FTA.

However, by a thorough review of various research papers, it was observed that FTA has many limitations regarding predicting an exhaustive list of possible failures that might lead to a hazard. Though over time, many improvements have been made in the FTA process, yet it is difficult to predict the time delays hazards that arise due to temporal delay in time. On the other hand, STAMP has been good at predicting the time delay hazards due to its systematic analysis procedure. However, STAMP lacks in quantitative analysis and doesn't comply with international standards alone. The newly proposed method combined the qualitative analysis capability of STAMP and quantitative analysis capability of FTA to overcome the limitation of both FTA and STAMP.

The detailed procedure of conducting analysis using a new method has been explained. The new method has been applied to two systems used in railway signalling for its practicability, and analysis could be done successfully as per the described procedure. The fault tree produced by the new method was compared with the fault tree generated by conventional FTA. The comparison showed that new fault-tree covered time-delay hazards of systems along with all the hazardous events predicted by the conventional FTA and covered the limitations of conventional FTA. This method also did the quantitative analysis of both the target systems successfully. Hence it covered the limitation of STAMP also. It was also observed that quantitative result produced by new methods were better than the quantitative result of the Conventional FTA. Hence the qualitative analysis superiority, as well as quantitative superiority of the new method, has been established.

9. Bibliography

[1] Y. Sugimoto and U. Singh, Examination of safety evaluation method of railway signal system -Combined use of FMEA, FTA and STPA, Wakayama, 2019.

[2] [Online]. Available: https://www.weibull.com/basics/fault-tree/index.htm.

[3] [Online]. Available: https://en.wikipedia.org/wiki/Fault_tree_analysis.

[4] [Online]. Available: https://accendoreliability.com/fault-tree-analysis-8-step-process.

[5] J. Fussel, "A Review of Fault Tree Analysis with Emphasis on Limitation.," *IFAC proceedings volumes,* vol. 8, no. 1, pp. 552-557, 1975.

[6] B. K. Misra, in *Handbook of Performability Engineering*, p. 2008.

[7] R. Karimi, N. Rasmussen and L. Wolf, "Qualitative and Quantitative Reliability Analysis of Safety Systems".

[8] Z. Zhenxu and Q. Zhang, "Condition Fault Tree: An Extension Of Traditional Fault Tree To Handle Uncertainities," 2018.

[9] Cha, S. Stephen, N. G. Leveson and T. J. Shimeall, "Safety Verification of ADA Programs Using Software Fault Trees," July, 1991.

[10] M. Towhidnejad and T. B. Hilbum, "Application of Software Fault Tree Analysis to an Airport Ground Control System.," 2008.

[11] G. Helmer, J. Wong, M. Slagell, V. Honavar, L. Miller and R. Lutz, "A Software Fault Tree Approach to Requirement Analysis of an Intrusion Detection System," 2002.

[12] S. Yu, "A comparison of FMEA, AFMEA, and FTA," 2011.

[13] M. Liu, J. Wang, D. Li and Y. Liu, "SFMEA Assidtant Design Method For Control System Uisng Requirement Modeling," IOP, 2017.

[14] N. G. Leveson and J. P. Thomas, STPA handbook, 2018.

[15] unknown, “https://en.wikipedia.org/wiki/Interlocking,” Wikepedia, [Online]. Available: https://en.wikipedia.org/wiki/Interlocking.

[16] P. Josserand and H. W. Forman, Rights of Trains (5th ed), New York: Simmons-Boardman Publishing Corporation., 1957.

[17] R. J., "Risk Management in Dynamic Society: A Modeling Problem.," 1997.

[18] T. Kobayashi and U. Singh, Consideration of safety analysis application in railway signal system - Safety analysis using FMEA, STAMP and HAZOP, Wakayama, 2019.

[19] T. Takata and H. Nakamura, Applicability of Methods of Safety Analysis of Railway Signaling., Journal of korean society of railways., 2015.

[20] U. Singh, T. Mizuma, H. Nakamura and Y. Sugimoto, “Proposal of New Safety Evaluation Method using STAMP and FTA,” Wakayama, 2019.

[21] T. Takata; H. Mochizuki; Sei Takahashi; H. Nakamura, "Proposal of Methods for Safety Analysis of Railway Signaling," Nagaoka 2019.

10. Publications

1. Main speaker

STAMP&FTA

Proposal of New Safety Evaluation Method using STAMP&FTA

Upvinder SINGH, Takeshi MIZUMA, Hideo Namura and Yukiko Sugimoto

IEICE(The Institute of Electronics, Information and Communication Engineers) Technical Report

Vol.119,no351,DC2019-80,pp11-15, 4th Winter workshop on Safety, 2019.12.20 at Wakayama.

2. Co-author

鉄道信号システムの安全性評価手法の検討

FMEA, FTA, STPA の併用

杉本祐紀子、水間　毅、Upvinder Singh and et.al

IEICE Technical Report

Vol 119,no351,DC2019-81,pp17-20, 4th Winter workshop on Safety, 2019.12.20 at Wakayama.

3. Co-author

鉄道信号における安全性解析適用の考察

FMEA, STAMP, HAZOP を併用した安全性解析

小林　大軌、水間　毅、Upvinder Singh and et.al

IEICE Technical Report

Vol 119,no351,DC2019-79,pp7-10, 4th Winter workshop on Safety, 2019.12.20 at Wakayama.

一般社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report

STAMP & FTA
Proposal of New Safety Evaluation Method using STAMP & FTA

Upvinder SINGH[1], Takeshi MIZUMA[1], Hideo NAKAMURA[2], Yukiko SUGIMOTO[3]

1. The University of Tokyo, 5-1-5 Kashiwanoha, Kashiwa, Chiba 277-0882, Japan.
2. Nihon University, 7-24-1 Narashinodai, Funabashi, Chiba 274-8501, Japan.
3. Kyosan Electric Mfg. co. limited, 2-29-1, Tsurumi ward, Kanagawa, 230-0031, Japan.

Email: 1. singh.upvinder18@ae.k.u-tokyo.ac.jp

Abstract: Modern railway signaling systems are becoming more and more complex with the increased use of software. Conventional safety assessment methods like FMEA and FTA usually work on the basis of component failures and try to trace propagation of those failures through the system. However, using these methods, it is difficult to erase the concern about scenario rationality or how a software failure influences the safety. That is why, STAMP (System Theoretic Accident Model & Process) is drawing attention for safety assessment. STAMP is an accident model that focuses on various module interactions, controls and feedbacks. RAMS standard for railways (IEC62278) requires qualitative as well as quantitative safety assessment of all Railway systems whereas STAMP provides only qualitative assessment. Main target of this paper is to compare FTA and STAMP method by applying on same system and later proposal for a new idea shall be made to incorporate STAMP in safety evaluation of railway signaling systems.

Keywords: STAMP, FTA, Safety, Complex Systems, Safety Engineering Techniques, Risk Analysis

1. Introduction:

Rapid shift in technology in train control and communication-based train operation has increased the complexity in signaling and train control systems. In conventional systems risk were mainly related to component failure and human error, however the kind of risk being faced by modern systems is different from conventional one due to increased use of software and increasing interaction among components. As compared to advancement in railway signaling, not much progress has been made in the field of safety engineering techniques. For safety evaluation of most of modern signaling and train control systems, traditional safety techniques such as Fault Tree Analysis (FTA) and Failure Mode and Effect Analysis (FMEA) are being used. These methods were developed several years ago for relatively simpler systems; and they were effective at past because of their ability to analyze the system by isolating and simplifying the interface between system components [1]. However, higher software dependency and increased component interaction has made modern system more complex and changing nature of hazard has made traditional safety evaluation techniques less effective. That is why, a new approach or method is required for safety evaluation of modern signaling systems that would be capable enough to assess new kind of risks emerging out due to increased complexity.

Recently, STAMP (System Theoretic Accident Model & Processes), a new safety evaluation method developed by MIT professor Nancy Leveson, have been gaining popularity for safety evaluation of complex systems. It treats safety as control problem, and the focus of the system safety is changed from preventing safety failure to implementing safety constraints [4]. After evolution of this technique, it has been applied on many complex systems in different industries and almost every time its superiority has been established over the traditional methods. In field of railway also, it has been tried a few times and results have been in favor of this method. Few papers have also been published on comparison of STAMP with traditional methods by applying on specific systems.

As per IEC 62278 RAMS standards for railways both qualitative as well as quantitative analysis are required for all safety systems of railways whereas STAMP focuses only on qualitative analysis and there is no provision for quantitative analysis. For comprehensive safety analysis of railway signaling systems with the help of STAMP, some efforts in direction of incorporating quantitative analysis in STAMP is required. It can be done by finding some way for qualitative analysis within STAMP or by merging it with other safety analysis techniques. Some papers have been written on merging STAMP with FMEA to do quantitative as well as qualitative analysis.

In this paper an effort has been made to compare the results of FTA and STAMP on a small train control system (on-board ATS) and later an idea of merging STAMP and FTA has been proposed to do safety analysis that include both qualitative as well as quantitative analysis as per IEC 62278 RAMS standards guidelines. The remainder of this paper is organized as follows. In section 2, a brief introduction about Fault tree analysis (FTA) and System theoretic accident model and process (STAMP) has been provided. In section 3, research flow has been presented in form of flow chart. Section 4 covers application of FTA & STAMP on on-board ATS system preceded by system description. Comparison of result of FTA & STAMP is shown in form of table in section 5 which shows clear dominance of STAMP in finding Risk for this system also. In section 6, a new method for safety evaluation as a combination of STAMP and FTA has been proposed to incorporate STAMP in safety evaluation of railways signaling system as per IEC 62278 RAMS standard for railways. Finally, conclusion has been made in section 7.

2. FTA:

Fault Tree Analysis, one of the safety analysis method used in risk control building, is an approach for detailing the cause of the failure event of system placed in the top-down approach, but the level of detail and completeness of the analysis depend largely on the skills of the analyst [3]. It is a top-down approach or deductive analysis technique which visually depicts the failure path in form of a tree. It starts with a potential undesired event (accident) called a TOP event, and then determining all the way it can happen. This method uses logic gate to depict how TOP event can be caused by individual or combined lower level failures or events. [5].

STAMP:

STAMP is a new hazard analysis technique developed by MIT's Aeronautics and Astronautics professor Nancy Leveson in 2011. As traditional methods focus on identifying risks related to component failures and human error, STAMP also focused on identifying other possible failures such as unsafe interaction among non-failing components, which can be caused from design flaws. [6]
STAMP is an iterative process and uses system theory instead of systematic theory. Traditional methods such as FTA and FMEA mainly focuses on component failures and all the efforts are made to predict how these failures can propagate through system and cause hazardous situation. However, in today's complex systems unsafe situation may arise even if all the components work as those are designed to work, and this kind of situation usually occurs due to lack of control actions to avoid such situations. [6] all the components are bound to fail in one or other way, but their effect can be minimized or eliminated by providing sufficient control actions. [6]
Also, STAMP provides guidance to analysts in conducting Hazard Analysis and safety engineers are not required to fill the blank page using personal experience just as in conventional methods. [7]

3. Research flow:

As STAMP has been gaining popularity for safety evaluation in various fields such as aviation, marine etc., this research was started with the aim of finding suitability of STAMP in safety analysis of railway signaling and train control systems. For checking its effectiveness in finding more unsafe situations compared to traditional safety evaluation technique currently being used i.e. FTA, STAMP was applied on on-board ATS system and results were compared with results obtained from FTA. Later on, a new proposal was given to combine STAMP & FTA to incorporate STAMP's comprehensive safety evaluation capability in safety evaluation as per IEC 62278 RAMS standard. A systematic flowchart for research progress is shown in fig.1.

4. Application of STAMP & FTA:

Fig. 2 shows an on-board ATS system used for application of FTA and STAMP, in which on-board system provides an audio and visual alarm to alert operator in case signal ahead is red. Operator needs to acknowledge the alarm within 5 second and take necessary action to stop train before the signal. However, if operator doesn't respond within stipulated time duration then on-board system will automatically actuates the braking mechanism to stop train before the red signal. System only with very basic functionality has been used here for ease of application.

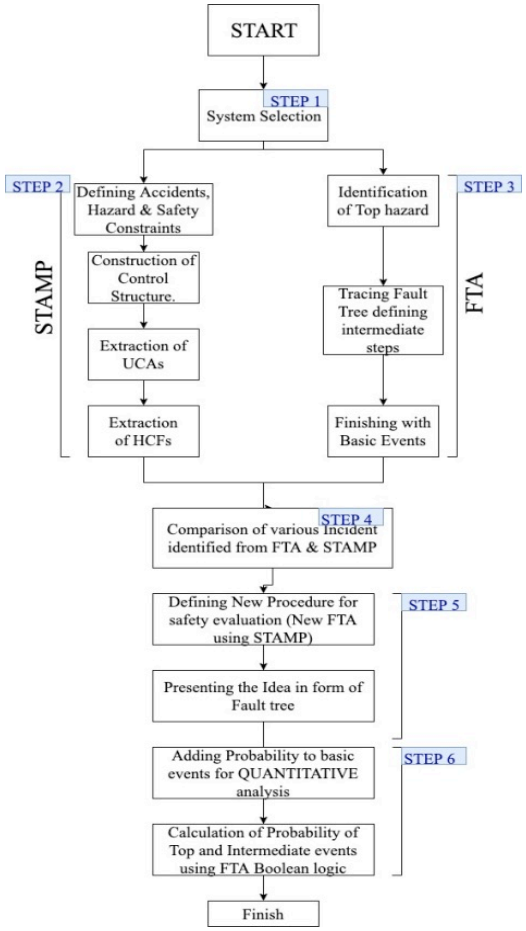


Figure 1. Research Flow Chart.

Main function of the this ATS system is to avoid SPAD (Signal passing at danger), means a train should always stop before a red signal even if operator is not responding to red signal or having some divergence during operation.

STAMP:

STAMP has a systematic procedure to comprehensively cover all hazards and consist of following steps.

1. Identification of accident, hazard and safety constraints.
2. Establishing a control structure.
3. Identification of Unsafe Control Actions (UCAs).
4. Identification of Hazard Casual Factors (HCFs).

Special guide words have been provided to identify scenarios that may possibly lead to casual factors. Fig. 3 shows the control structure from STAMP analysis prepared using IPA Japan STAMP workbench. From the control structure UCA table was prepared by considering each control action in following four categories.

1. Not Provided.
2. Incorrectly Provided.
3. Provided too early, Too late, or out of sequence.
4. Stopped too soon or applied too long.

Following this Hazard casual factor along with scenarios were identified for each UCA with the help of guideword provided with STAMP workbench. A detailed list of UCA is shown in table 1. Similarly, complete table for HCF and related scenarios were also prepared.

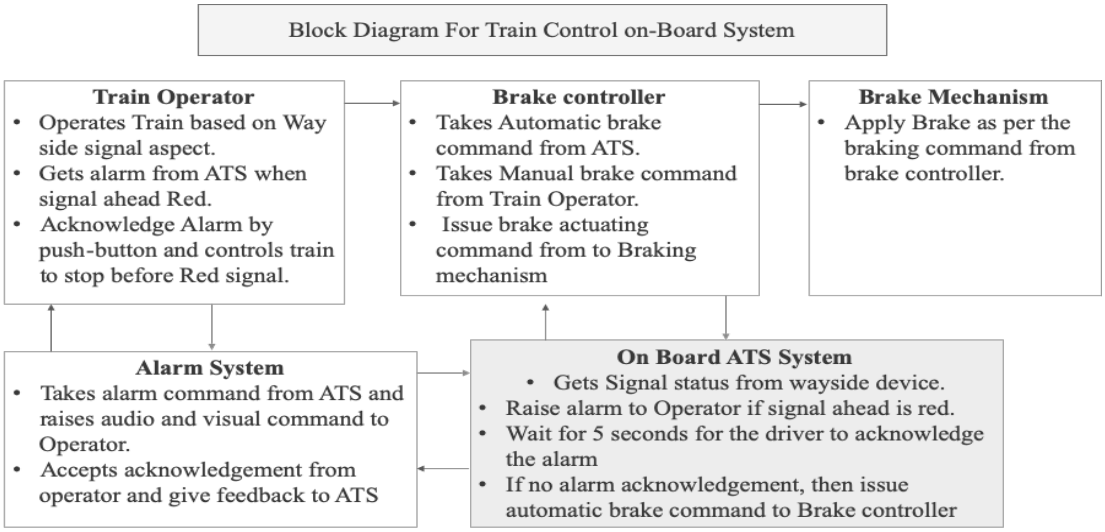


Figure 2. On-Board ATS

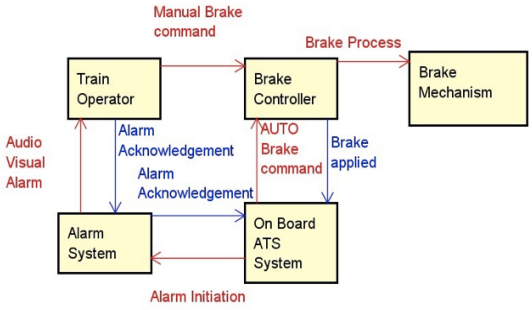


Figure 3. On-Board ATS Control Structure

FTA:

FTA uses a top-down approach that starts with the hazard and trace down the system to basic events, mainly component failures, that propagated through system either alone or in association with other events leading to top hazard. It adopts a logical method that carries out hazard analysis work vividly and its features are intuitive, clear, clear-cut, logical; and can be used for qualitative analysis and quantitatively analysis [4]. Deciding TOP event for FTA is most challenging as no procedure is defined and it totally depends on expertise of safety analyst. On-board system is designed for avoiding SPAD, and unwanted & unsafe situation in this case is Train passes the signal when it is Red. Taking SPAD as top event, a fault tree based on FTA has been prepared and shown in fig.4. This is simple FTA and further restricted gate may also be added after each event as countermeasure.

4. Result analysis and comparison:

Results from both methods were analyzed separately and it was observed that all the undesired events identified by FTA were highlighted by STAMP. However, additional potential unsafe events were identified by STAMP. A

Table 1. UCA extracted for On-Board system

No	CA	From	To	CA Providing Condition	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
1	Alarm Initiation	On Board ATS System	Alarm System	When Siganl is RED operate the warning alarm	(UCA1-N-1) Alarm system doesn't Initiate alarm. [SC1]	(UCA1-P-1) No Alarm actuation when signal is RED [SC2]	(UCA1-T-1) Late Alarm actuation when signal is RED [SC1]	(UCA1-D-1) Alarm command duration not sufficient to actuate alarm [SC2]
2	Audio Visual Alarm	Alarm System	Train Operator	Alert driver when Signal is RED.	(UCA2-N-1) No alarm to operator when signal is RED [SC2]	(UCA2-P-1) Operator gets no warning when alarm activated [SC2]	(UCA2-T-1) Late warning to Operator when signal is RED [SC1]	(UCA2-D-1) Alarm time not sufficient enough to be noticed or acknowledged by operator.
3	Manual Brake command	Train Operator	Brake Controller	Mnaual Braking when signal is RED	(UCA3-N-1) No Braking [SC1]	(UCA3-P-1) Insufficient braking [SC1]	(UCA3-T-1) Braking when signal already inside Tain minimum stopping distance. [SC1]	(UCA3-D-1) Brake time too small to stop the train. [SC1]
4	AUTO Brake command	On Board ATS System	Brake Controller	AUTO brake initiation when driven not reponding to warning	(UCA4-N-1) No Brake command when inaction by Operator. [SC1]	NA	(UCA4-T-1) Delayed Brake command when no action by Operator. [SC1]	(UCA4-D-1) insufficient command time to be read by Brake controller.
5	Brake Process	Brake Controller	Brake Mechanism	Braking when brake initiation cammand is received	(UCA5-N-1) No Braking [SC1]	(UCA5-P-1) Usuccessful Braking [SC1]	(UCA5-T-1) Braking when train alredy inside minimum braking distance. [SC1]	(UCA5-D-1) No Train stopping due to short brake time [SC1]

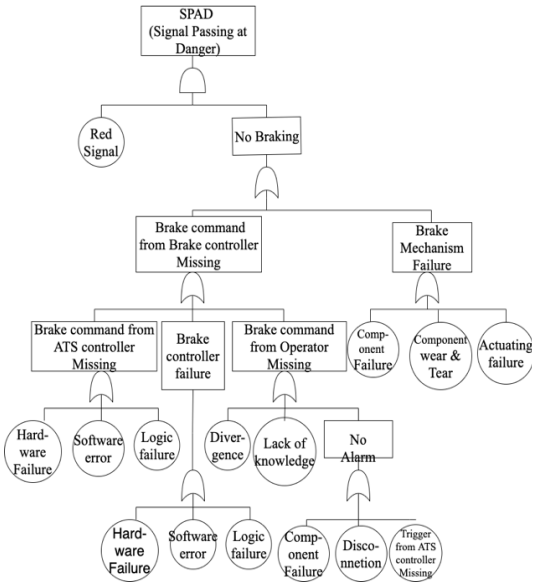


Figure 4. Fault Tree for On-Board ATS System

brief table (table 2) was prepared for component wise associated undesired events with one column showing undesired events identified by both FAT & STAMP and other showing those identified by STAMP only. Result analysis and comparison table clearly indicates dominance of STAMP in identifying unsafe situation due to component failure as well as component interaction. Reason for STAMP having upper hand compared to FTA is its clearly defined procedure to identify Unsafe Control Actions and then guideword for HCF & Scenarios. In case of FTA, no such clear procedure is defined, and results depends entirely on expertise and system understanding of person doing analysis. Also, FTA focuses on component failure whereas STAMP tries to find out unsafe control actions present in the system. Due to the superiority of STAMP in finding the undesired situations more comprehensively, it should also be used in safety evaluation of railway signaling and train control systems.

Table 2. Result comparison from STAMP & FTA

Object	Identified by both FTA & STAMP	Identified by STAMP only
Alarm System	Component Failure, Disconnection	Longer response time, Flaws in alarm actuating system, Wrong alarm intensity & Location (Design Flaws)
On Board ATC	Hardware failure, Software error, Wrong output.	Longer execution time, Delayed response, Complex and erroneous decision making.
Brake Controller	Component failure, Software error.	Conflicting inputs. Complex decision making.
Brake Mechanism	Component failure, Component wear & tear.	Longer actuating time, Inadequate braking power
Train Operator	Lack of knowledge.	Response time of operator, Mental & physical state of operator, Complex operating procedure, Multiple steps for braking.

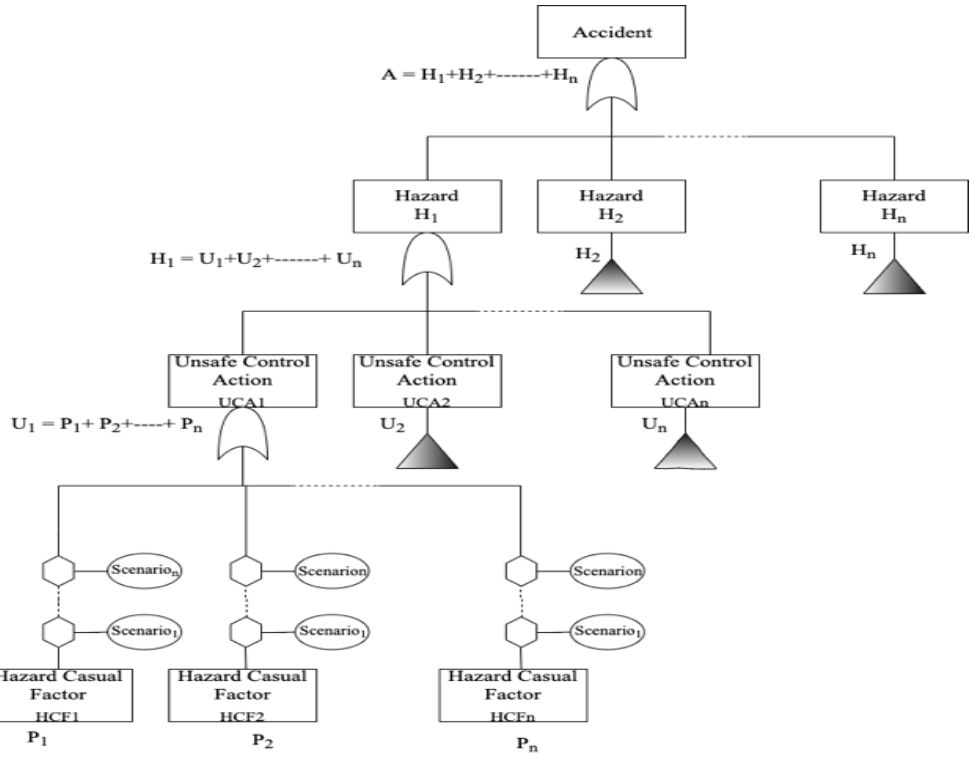


Figure 5. New Fault Tree using STAMP

As per the IEC 62278 RAMS standard for railways each safety equipment should have qualitative as well as quantitative analysis. However, STAMP doesn't have any mean to do quantitative analysis. In case of FTA, both qualitative as well as quantitative analysis can be done but it is really challenging to identify all possible hazardous event due to absence of clear procedure and assessment clearly depends on expertise of analyst. Here, instead of replacing one method with another, it seems much more fruitful to combine 2 methods to complement each other and eliminate their shortcoming [8]. As STAMP is capable of covering almost all hazardous events then it should be used for qualitative analysis and its result can be mapped in the form of a tree that not only make the evaluation results easy to understand but also the probability of top events can be calculated using Boolean logic of FTA for quantitative analysis.

5. New FTA using STAMP:

For combining two methods, I propose application of STAMP followed by creation of fault tree using results of STAMP. Application procedure for both STAMP & FTA has already been explained in this paper. Fig. 5 shows the way how STAMP results can be mapped in tree form along with probability assignment for quantitative analysis. In this proposal, I have shown accident as the top event which is taken from the accident defined in STAMP application and Hazard, UCA and HCF have been mapped in at different levels. For all the HCF, restrictive gates have been provided as counter measure to various scenarios. For each countermeasure restrictive gate is shown as corresponding scenario in proposed fault tree.

Quantitative analysis is started with assigning probabilities to basic events and using the Boolean logic of fault tree, probabilities of all intermediate and top events can be estimated. Using probability of UCA, frequency of occurrence can be estimated. In this way, this new method shall be capable of doing comprehensive qualitative analysis and quantitative analysis. Also, representation in the form of tree makes it more convenient to understand result. A comparison of advantage and limitation of various method is shown in table 3. During application of this method there are 2 main challenges.

1. As all HCFs aren't independent and many times one HCF lead to another HCF and even one UCA may lead to another, so it is not possible for all HCFs or all UCAs to be mapped at same level as shown in proposal. That is why, special system expertise is required to decide correct level of each UCA or HCF level in fault tree.
2. Probability of basic component failure can be estimated using data published by authorized organizations, but it is difficult to estimate the probability of unsafe control action arising when no component fails.

Table 3. Comparison of Various Methods

FEATURES	STAMP	FTA	STAMP+ FTA
Provides Exhaustive list of possible unsafe situations	✓	✗	✓
Provides quantitative analysis	✗	✓	✓
Results easy to understand	✗	✓	✓

7. Summary:

An effort has been made to check if STAMP is needed for railway signaling systems and that was done by comparing the result from STAMP and FTA application on same system. This comparison showed that STAMP is predicting more scenarios that may lead to hazard or accident than what is predicted by FTA. So, the conclusion was made that STAMP need to be incorporated in railway signaling system safety analysis. Following that a proposal to map results of STAMP in tree form has been made that can be used to do qualitative analysis. Further efforts need to be done to apply it on larger and complex systems to find the effectivity of this analysis.

References:

[1] N.G. Leveson, M.V. Stringfellow and B.D. Owens, "Safety-Driven Designs for software-Intensive Aerospace and Automotive Systems", "Institute of Electrical and Electronics Engineers,2010.

[2] Peter Underwood and Patrick Waterson, "Systems thinking, the Swiss Cheese Model and accident analysis: A comparative systemic analysis of the Grayrigg train derailment using the ATSB, AcciMap and STAMP models".

[3] Ka Son, Hideo Nakamura, "Safety Estimation of Railway Signaling System using Color-FTA."

[4] Zitong Zhou, Yanyang Zi Jinglong chen and Tong An, "Hazard analysis for escalator emergency braking system via system safety analysis method based on STAMP."

[5] Marvin Rausand, Arnljot hoyland, "System reliability Theory: Models, Statistical Methods, and Applications".

[6] N. Leveson, An STPA Primer, 2013.

[7] Yao Song, "Applying system-theoretic accident model and processes (STAMP) to hazard analysis."

[8]Tetsuya TAKATA, Hideo NAKAMURA, "Applicability of Methods for Safety Analysis of Railway Signaling."