Safety Analysis of Automatic Door Operation for Metro Train: A Case Study

Ajeet Kumar Pandey*, Srinivas Panchangam, and Jessy George Smith

Cognizant Technology Solution, Hyderabad, India
{ajeet.kumar3,srinivas.panchangam,jessy.smith}@cognizant.com

Abstract. Transportation industries are growing not only in volume but in technology as well. To keep pace with changing business paradigms, automotive manufactures needs to use latest information technology and tools to make the transportation system economically viable, safe and reliable. Safety is the most important concern for today's railway system. Various subsystems of modern rail are safety critical and could result in loss of life, significant property damage or damage to the environment, if failure occurs. This paper presents the systematic approach to counter the risk in such system by analyzing the failure mode and its effect. The automatic door operation subsystem which forms one of the major safety critical systems in metro train is discussed along with a case study by analyzing various failure modes and its effect. Analysis processes as well as the significance of different metrics are also elaborated.

Keywords: reliability, safety, failure mode and effect analysis (FMEA), risk, risk priority number (RPN), automatic door operation (ADO).

1 Introduction

The transportation industry today has to be on the move, constantly, in more ways than any other industry. It has to deal with the increasing demands of customers and suppliers, while simultaneously trying to optimize the entire business operation at minimum cost. To keep pace with changing business paradigms, transporters need to use information technology, not merely as an enabler of operations but as a strategic driver and critical business tool. Railway transportation is more energy efficient and economical than the road transportation. The railways have always been ecologically safe with much less atmospheric pollution, compared to aircrafts and motor vehicles. The Railways have performed the twin tasks of providing adequate transport for industrial sustenance and growth and ensuring cheap, reliable and safe transportation for the population. Modern rails are now using many safety instrumented system (SIS) for handling safety critical functionalities. SIS implements the required safety functions necessary to achieve or maintain a safe state for some equipment.

Safety critical systems are those systems whose failure could result in loss of life, significant property damage or damage to the environment. There are well known

* Corresponding author.

K. Singh, A.K. Awasthi, and R. Mishra (Eds.): QSHINE 2013, LNICST 115, pp. 962–974, 2013.

examples in application areas as such as railways, aircraft flight control, weapons and nuclear systems. Many modern information systems are becoming safety-critical in a general sense because financial loss and even loss of life can result from their failure. There are plenty of definitions of the term safety-critical systems but the intuitive notion actually works quite well. The concern both intuitively and formally is with the consequences of failure. If the failure of a system could lead to consequences that are determined to be unacceptable, then the system is safety critical. In essence, a system is safety-critical when we depend on it for our well being. Safety is the most important challenge for railway companies worldwide. A great deal of attention and effort has been paid to making railway operations safe. Despite these best efforts, accidents still occur, shaking people's faith in safety. And each time an accident occurs, further safety measures are taken. Today's railway safety is based on the many bitter experiences of the past. Railways are deeply rooted in society and people's consciousness worldwide and they are also strongly influenced by the each nation's social, cultural and geographical climate.

Several systems of locomotive/railways have gained importance in terms of safety measures. For example, through the last decade's door systems have developed tremendously. Safety and reliability are the key points in this development. Accurate controlling and checking of this safety related component are vital for reliable operation, making the door control unit the 'brain' of the door system. Door control units control door opening / closing so that passengers can safely get in and out of trains. Doors come in all sizes and shapes, different power systems, controls and door types. This paper presents a case study of Automatic Door Operations (ADO).

Rest of the paper is organized as follows: Section 2 presents the backgrounds behind the work. Sections 3 and 4 discuss literature surveys on safety and FMEA. Section 5 gives the brief idea about the automatic door operation (ADO), and contains a case study on ADO FMEA, whereas conclusions are presented in Section 6.

2 Backgrounds

2.1 Safety Critical System: Quality, Reliability and Safety

Safety-critical systems are those systems whose failure could result in loss of life, significant property damage, or damage to the environment. It is the system where human safety is dependent upon the correct operation of the system. Safety must be considered as whole system, including hardware , software, and other E/E/PE systems. Quality, reliability and safety issues must be considered with high importance in safety critical system.

Although the terms quality and reliability are often used interchangeably, there is a difference between these two disciplines. Reliability is the probability of the system meeting adequate performance for specified period of time under specified use condition. Reliability is concerned with the performance of a product over its entire lifetime; quality control is concerned with the performance of a product at one point in time, usually during the manufacturing process. Moreover, a close relationship also exists among the terms quality, reliability and safety especially in the context of

software controlled product. Quality is the degree to which the systems meet its laid down specification. Reliability is a dynamic measure and varies with time. Qualitative measure is not sufficient for making engineering decision and therefore a quantitative, reliability measure is required.

Safety and reliability are often equated in the software context, but the conflicts between these two are growing to separate them [1]. Safety is the probability that the conditions that can lead to a mishap do not occur, whether or not the intended function is performed [6]. According to MIL-STD 882B, safety is defined as "freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property. A system can be defined in two ways: what it is supposed to do and what it is not supposed to do. Reliability focuses on what the system is supposed to do while safety focuses on what system is not supposed to do. In general, reliability requirements are concerned with making a system failure free, whereas safety requirements are concerned with making it mishap free. Reliability focuses on every failure; whereas in safety only the dangerous failures are considered. Safety may decrease reliability and availability e.g. diagnostics and shutdown mechanisms.

2.2 Safety Critical System in Rail Transportation

The complexity of transport system is growing incredibly fast, thus Safety Critical Systems in the transport domain are becoming increasingly complex, not only in scale, but also the underlying technology. The railway industry is a leader in the development of safety critical systems. Modern rail transport systems contain a diverse combination of computers controlling non-critical functions such as entertainment systems and cabin lights, as well as safety critical systems such as track/train transmission, speed controller, and level crossing controller.

Now a day's transportation systems are using electronics for controlling various subsystems that was earlier controlled mechanically or manually. While these new electronic control and monitoring systems offers many benefits; in order to assure safe operations, regulations mandate that such systems comply with industry standards for hardware and software development and are thoroughly tested and documented. In rail transportation, as more electronic systems come into play, it becomes necessary to do whatever is possible to assure correct operation of these advanced systems.

3 Literature Survey

System safety is a sub discipline of system engineering that applies scientific, management, and engineering principle to ensure adequate safety, throughout the system life cycle, within the constraints of operational effectiveness, time and cost [1]. The objective of system safety is to identify, eliminate or control, and document system hazards in order to prevent any unsafe situations. Safety analysis is regarded as an initial investment by many researchers and industry professionals to save the

future losses that would result from the potential mishaps. As a result of this, various hazard analysis techniques [2] for system safety have been developed such as Preliminary Hazard Analysis (PHA), Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Failure Mode and Effect Analysis (FMEA), Markov Analysis, Common Cause Failure Analysis, and HAZOP Analysis.

Each of these techniques has some advantage and disadvantage in certain circumstances. Identification of hazards may utilize more than one technique as one particular hazard analysis may not be able to identify all the hazards within a system. Many researchers have tried to combine the advantages of FMEA and FTA for the safety analysis of the systems. FMEA can be developed as a preparatory activity to fault tree construction [3]. Combining bottom-up FMEA with the top-down FTA, is much effective in understanding underlying combination of circumstances that enable a failure mode to occur, as well as the likelihood of the identified failure mode [4].

On reviewing literature, it is found that FMEA and FTA is the most widely used safety analysis techchiqus. FMEA is a design analysis method that explores the effects of possible software failure modes on the system. There are two types of FMEA for embedded control systems: system software FMEA and detailed software FMEA [5]. System software FMEA can be used to evaluate the effectiveness of the software architecture without all the work required for detailed software FMEA. The detailed software FMEA validates that the software has been constructed to achieve the specified safety requirements. Detailed software FMEA is similar to component level hardware FMEA. However, the analysis is lengthy and labor intensive and also the results are not available until late in the development process. In fact the detailed software FMEA is often cost effective only for systems with limited hardware integrity.

4 Failure Mode and Effect Analysis

Failure Modes and Effects Analysis may have the various activities such as describe product or process, define functions, identify potential failure modes, describe effects of failures, determine causes, direction methods or current controls, calculate risks, take action and assess results. The FMEA process evaluates the overall impact of each and every component failure mode. The primary FMEA goal is to determine the effect on system reliability from component failure; however the technique can be extended to determine the effect on safety. Input data for the analysis include detailed hardware / function design information. Design data may be in the form of design concept, the operational concept, and major components planned for use in the system and major system functions. Table 1 lists the inputs, processes and outputs for conducting the FMEA.

Sources for this information include design specifications, sketches, drawings, schematics, functional block diagram (FBD) or reliability block diagram (RBD). Input data also includes known failure modes for components and failure rates for the failure modes. FMEA output information includes identification of failure modes in

the system under analysis, evaluation of the failure effects, identification of hazards, and identification of system critical item in the form of a critical item list.

Table 1. FMEA Input, Process & Output

Input	FMEA Process	Output
Design Knowledge	Evaluate design	Failure modes
Failure Knowledge	Identify potential failure modes	Consequences
Failure Mode Type	Evaluate effects of failure modes	RPN
Failure Rate	Document Process	Reliability Prediction
Design Knowledge	Evaluate design	Critical Item List (CIL)

The FMEA process begins by identifying "failure modes", i.e. the ways a product, service or process could fail. A project team examines every element of a service, starting from the inputs and working through to the output delivered to the customer. At each step, the team asks "what could go wrong here?" Additionally they find out the probability of such failure (occurrence), the damage it will inflict (severity), should it actually fail and the likelihood of finding out (detectability) such failures before final delivery. These three parameters are ranked on 1-10 scale and product of these three is termed as Risk Priority Number (RPN). RPN can be used as safety indicator to prioritize the control actions.

4.1 FMEA Process

FMEA can provide an analytical basis, when dealing with potential failure modes and their associated causes. When considering possible failures in a design – like safety, cost, performance, quality and reliability – an engineer can get a lot of information about how to alter the development/manufacturing process, in order to avoid these failures. A typical FMEA process is shown in Figure 1. In general, FMEA process involves the following steps:

i. Define the system to be analyzed.

ii. Identify specific design requirements that are to be verified by the FMEA.

iii. Define ground rules and assumptions on which the analysis is based.

iv. Obtain or construct functional and reliability block diagrams.

v. Identify failure modes, effects, severity, and other pertinent information on the worksheet.

vi. Evaluate the severity of failures effect in accordance with the prescribed severity categories.

4.2 FMEA Worksheet

It is recommended to perform the FMEA using a form or worksheet to provide analysis structure, consistency, and documentation. The specific format of the

analysis worksheet is not critical. Typically matrix, columnar or text-type forms are utilized to help maintain focus and structure in the analysis.

An FMEA that supports system safety and hazard analysis should contain the information, as a minimum are: Failure Mode, System Effect of failure mode, System-level hazards resulting from failure, Mishap effect of hazards, Failure mode and / or hazard causal factors, How the failure mode can be detected, Recommendations (such as safety requirements / guidelines that can be applied), and the risk presented by the identified hazard. The format of the FMEA worksheet may be determined by the customer, the system safety group, the safety manager, or the reliability / safety analyst performing the analysis. In the present study, a generalized FMEA worksheet has been used as shown in Table 2.

Table 2. FMEA Worksheet

Sl. No	Component	Failure Modes	Effects	Mitigation
1.	Motor	Open Circuit / Short Circuit	Door Stuck	Hardware failure needs to check mechanical parts.
2.	…	…	…	…
3.	…	…	…	…

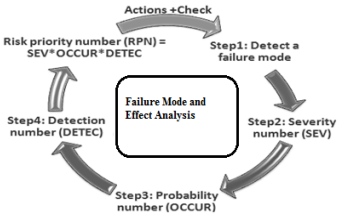

Fig. 1. FMEA Process

4.3 Assessing Risk Priority Number (RPN)

The Risk Priority Number (RPN) is calculated for analyzing the risk associated with potential problems identified during a Failure Mode and Effects Analysis (FMEA). After identifying the potential failure modes; the RPNs are derived using past experience and engineering judgment to rate each potential factor according to three rating scales: *Severity, Occurrence, and Detectability.*

Severity (S) – Severity is a numerical subjective estimate of how severe the customer or end user will perceive the EFFECT of a failure.

Occurrence (O) – Occurrence or sometimes termed likelihood is a numerical subjective estimate of the likelihood that the cause, if it occurs, will produce the failure mode and its particular effect.

$$Criticality = Severity\ (S) * Occurrence\ (O)$$

Detection (D) – Detection is sometimes termed effectiveness. It is a numerical subjective estimate of the effectiveness of the controls to prevent or detect the cause or failure mode before the failure reaches the customer. The assumption is that the cause has occurred.

Assessing Risk – After the ratings have been assigned, the RPN for each issue is calculated by multiplying Severity, Occurrence, and Detection as:

$$RPN = Severity\ (S) * Occurrence\ (O) * Detection\ (D)$$

Rating scales usually range from 1 to 5 or from 1 to 10, with the higher number representing the higher seriousness or risk. The specific rating descriptions and criteria are defined by the organization or the analysis team to fit the products or processes that are being analyzed. Table 3 shows a generic five point scale for severity.

Table 3. Severity Scale

Rating	Description	Criteria
1	Very Low / None	Minor Nuisance
2	Low / Minor	Product operable at reduced performance
3	Moderate / Significant	Gradual performance degradation
4	High	Loss of Function
5	Very High / Catastrophic	Safety related Catastrophic failures

Larger RPN values normally indicate more critical failure modes but not always. For example, consider the three situations of Case-1where the RPNs are identical, but clearly the second situation would warrant the most attention. In general, any failure mode that has an effect resulting in a severity 9 or 10 would have top priority. Severity is given the most weight when assessing risk. Next, the Severity and Occurrence (S x O) combination would be considered; since this is effect represents the Criticality. Consider Case-2, situation #1 is most critical even though it has the lowest RPN value, than #2, and then #3. Here, the failure modes with the lowest RPN values are actually the most critical. One should be very careful when establishing the "threshold values" for RPNs when assessing risk.

Case-1

S	O	D	RPN
2	10	10	200
10	10	2	200
10	2	10	200

Case-2

S	O	D	RPN
10	2	2	40
3	10	2	60
2	5	10	100

5 Case Study- Automatic Door Operations: ADO System

A sliding door is a type of door which opens horizontally by sliding. A sliding door operator is a device that operates a sliding door for pedestrian use. It opens the door automatically, waits, and then closes it. Automatic sliding door is an intelligent application of advanced microcomputer and mechanical design, to meet the requirements for variety of construction, all sectors of the required automatic doors,

with advantages of safe, reliable, and long lifetime. It is being widely used in hotels, restaurants, railway stations, office buildings, supermarkets, major shopping malls and other places.

Sliding door operator will open/reopens the door as per the specifications. However, most operators use sensors to prevent the door from coming into contact with a user in the first place. The simplest sensor is a light beam across the opening. An obstacle in the path of the closing door breaks the beam, indicating its presence. Infrared and radar safety sensors are also used commonly. These are additional security methods used for the cases where an object cannot be detected by safety beam. The BLDC motor signals when an object is sensed and then the processor opens the door leafs.

Once the automatic door system is introduced, safety would automatically become foolproof for passengers, sources say, adding that the railways incur substantial expenditure for manufacturing automatic door coaches with the help of new technology.

5.1 Automatic Door Control Unit

Automatic door control units is a vital unit of sliding door and responsible for opening/closing of door safely for passengers to get in and out of trains. It consists of various modules such as Power Supply, CPU, FPGA, Vital Input Section, Vital Output Section, and general Input / Output unit. Structure of the door control unit is shown in Figure 2.

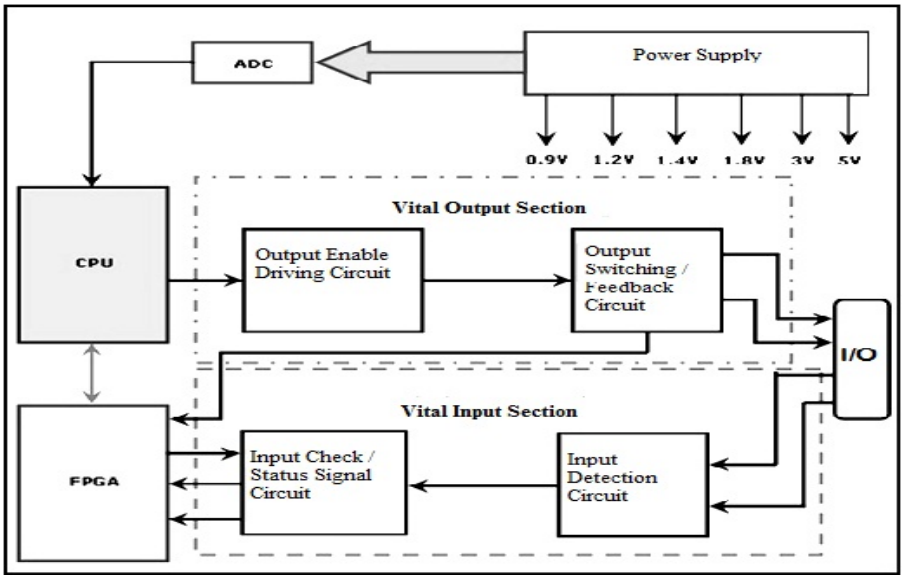

Fig. 2. Architecture of Door Control Unit

Table 4. System Level FMEA

#	Component	Failure Modes	Effects	Mitigation
1	Door Open / Close	Door does not open / close when required	Door permanently will be in open / closed mode. Passengers cannot board or alight from the metro cab.	HW may be damage, need to check the mechanical failures.
		Open / Close when not required	Door open / close when train is in running mode.	HW may be damage, need to check the mechanical failures.
		Door stuck in open / close position	Door always is in open or closed state. Passengers cannot board or alight from the metro cab.	HW may be damage, need to check the mechanical failures.
2	Motor Failure	Motor not working	Door will be in open or closed state. Passengers cannot board or alight from the metro cab.	HW may be damage; Motor conditions needs to be checked.
		Motor halts in between	Door will jam. Passengers cannot board or alight from the metro cab.	HW may be damage; Motor conditions needs to be checked.
		Motor speed is High	Rapid closure of Door. Passenger cannot board or alight.	HW may be damage; Motor interfacing unit needs to be verified.
		Motor speed is low	Slow closure of Door. Door will remain open in train running mode.	HW may be damage; Motor interfacing unit needs to be verified.
3	Power Supply	High Voltage	Door will remain open / close. Passengers cannot board or alight from the metro cab.	HW component may get damaged due to high voltage. Power supply check should take care whenever high voltage present it should cut-off the power supply.
		Low Voltage	Door will not open / close. Passengers cannot board or alight from the metro cab.	Power supply check should take care whenever low voltage present it should cut-off the power supply.
		Variable Voltage	Door will not Open / close. Passengers cannot board or alight from the metro cab.	HW component may get damaged due to unstable voltage. Power supply check should take care whenever unstable voltage present it should cut-off the power supply.
4	Sensor	Fast Detection	Door open / close before the input signal. Door will open immediately before required time.	SW should take care of the delay.
		Slow Detection	Door open / close response will be late. Door will open immediately late after required time.	SW should take care of the delay.
		No Detection	Door will not open / close.	HW may be damage need to check power source.
5	Timing	High Delay	Door will not open / close. Door will not function properly.	HW maybe damage. SW should take care of the delay.
		Low Delay	Door will not open / close. Door will not function properly.	HW maybe damage. SW should take care of the delay.

Input received from I/O section consists of two different logics (True / Compliment Logic), the system designed as redundant enough to capture and utilizes both true and false logic. Vital input section consists of Input Detection Circuit and Input Check Status Signal. Input Detection Circuit consists of an internal logic which helps to identify two different types logic. Input received from I/O circuit whether it is true or compliment is driven to the Signal Status check unit. Input Status check sends a status check signal to the FPGA. FPGA sends an acknowledgment to the status check circuitry about the health of the signal.CPU consists of logic which consists of the entire program which drives the complete unit. The required output from CPU given to the Output Enable Driving circuit, this circuit will drives the motor which helps to open / close the door automatically. Output switching units returns a feedback signals to the FPGA that helps to maintain the health of the unit.

An FMEA for the Door Control Unit is carried for a metro train in typical Indian Rail. For this a brain storming session with the various industry experts was performed. FMEA of Door Control Unit of different level i.e. system level FMEA,

sub-system level FMEA and component level FMEA are listed in the Table 4, Table 5 and Table 6 respectively.

Table 5. Sub-System Level FMEA

#	Component	Failure Modes	Effects	Mitigation
1	CPU	Logic Execution Failure	System comes to unconfigured / safe state	Dual Channel SW commands CPU to Reboot
		Timing Error – Slow / Fast	System reacts variably	Watch Dog Timer takes care
		RAM Corrupted	System comes to unconfigured / safe state	Dual Channel SW commands CPU to Reboot
		Wrongly loaded	System may not work in proper state	User Manual verification
		ALU Error	System comes to unconfigured / safe state	Dual Channel SW commands CPU to Reboot
		Stack overflow	System reacts variably	Watch Dog Timer takes care
		Port Stuck high / low	System comes to unconfigured / safe state	Dual Channel SW commands CPU to Reboot
2	FPGA	Logic Execution Failure	Wrong status to CPU & consecutive checks detects	CPU commands to Reboot
		Timing Error – Slow / Fast	System reacts variably	Watch Dog Timer takes care
		Port Stuck high / low	Wrong status to CPU & consecutive checks detects	CPU commands to Reboot
3	Power Supply	High / Low Voltage	HW may damage	HW may damage and SW may call for Reboot
		Open	No effect	No Power
		Short	System reboots	System reboots
		Spikes	Zener Diode may damage and make the circuit safe	System reboots
4	Interface	Connected Wrongly	No effect	Dual Channel HW will take care
		Loose Connection	Wrong Status	Cannot be detected SW must take the feedback
		Breakage	No Status	Cannot be detected SW must take the feedback

Table 6. Component Level FMEA

Risk Priority Number (RPN) = Severity (S) * Occurrence (O) * Detection (D)

#	Component	Failure Modes	Effects	S	O	D	RPN	Defense / Mitigation	Safe
	Input Inductors	Open	Vital Input will always report as de-energized.	2	2	5	20	No need as de-energized state is safe state.	Yes
		Short	No immediate Safety effect. No error is reported.	1	2	5	10	No Defense necessary.	Yes
	Current Limiting Resistors	Open	Vital Input will always report as de-energized.	2	2	5	20	No need as de-energized state is safe state.	Yes
		Short	Energized: It fails & always shows as de-energized. De-energized: the input will show as de-energized.	8	2	10	160	The Vital Software will read the Vital Input hardware to get the status latch value containing the input states every 2ms. The Vital software will cross check the Vital Input state from Dual channel architecture for every execution cycle, to make sure they both are in agreement.	Yes
	Transorb / Zener Diode	Open	No immediate Safety effect. No error is reported.	1	2	5	10	No Defense necessary.	Yes
		Short	Vital Input Shorted so will always report as de-energized.	2	2	5	20	No need as de-energized state is safe state.	Yes
	Metal Oxide Semiconductor Field Effect Transistors (MOSFET)	Open	Loss of Vital Input status signal.	5	5	5	125	The Vital Software will turn off the input using the Vital Input test control. The results will be checked on every 3 sample sets, and require 2 in a row to fail before the test is deemed to have failed. If the test fails, the software will call shutdown.	Yes

Table 6. (*Continued*)

#	Component	Failure Modes	Effects	S	O	D	RPN	Defense / Mitigation	Safe
		Short Gate & Drain	The input reads de-energized. No failure will be reported. The check Opto-coupler will be shorted during the check and may be destroyed. The check will not work.	5	5	5	125	The Vital Software will read the Vital Input hardware to get the status latch value containing the input states every 2ms. The Vital software will cross check the Vital Input state from Dual channel architecture for every execution cycle, to make sure they both are in agreement. The Vital Software will turn off the input using the Vital Input test control. The results will be checked on every 3 sample sets, and require 2 in a row to fail before the test is deemed to have failed. If the test fails, the software will call shutdown.	Yes
		Short Source & Drain	The status check will not be able to de-energize the input. The check will always fail.						
		Short Gate & Source							
	Input Check Opto Coupler	Open output transistor	MOSFET cannot be turned ON hence loss of the Vital Input check.	8	5	5	200	The Vital Software will read the Vital Input hardware to get the status latch value containing the input states every 2ms. The Vital software will cross check the Vital Input state from Dual channel architecture for every execution cycle, to make sure they both are in agreement. The Vital Software will turn off the input using the Vital Input test control. The results will be checked on every 3 sample sets, and require 2 in a row to fail before the test is deemed to have failed. If the test fails, the software will call shutdown.	Yes
		Shorted output transistor	Irrespective of FPGA command Vital Input status signal is always low.						
		Open Input LED	MOSFET cannot be turned ON hence loss of the Vital Input check.						
		Shorted Input LED	MOSFET cannot be turned ON hence loss of the Vital Input check.						
	Input Status Opto Coupler	Open output transistor	Irrespective of the Vital Input Check Control signal from FPGA the Vital Input status is always high.	8	5	5	200	The Vital Software will read the Vital Input hardware to get the status latch value containing the input states every 2ms. The Vital software will cross check the Vital Input state from Dual channel architecture for every execution cycle, to make sure they both are in agreement. The Vital Software will turn off the input using the Vital Input test control. The results will be checked on every 3 sample sets, and require 2 in a row to fail before the test is deemed to have failed. If the test fails, the software will call shutdown.	Yes
		Shorted output transistor	Irrespective of the Vital Input Check Control signal from FPGA the Vital Input status is always low.						
		Open Input LED	Irrespective of the Vital Input Check Control signal from FPGA the Vital Input status is always high.						
		Shorted Input LED	Irrespective of the Vital Input Check Control signal from FPGA the Vital Input status is always high.						

Table 6. (*Continued*)

#	Component	Failure Modes	Effects	S	O	D	RPN	Defense / Mitigation	Safe
	Output MOSFET	Open	Output cannot be enabled. No failure will be reported.	5	5	5	125	If the Vital Software determines that the output is energized from its reading of the Output feedback when it should be de-energized or vice versa then the Vital Software will put the Output into the failed state. If the Output is in failed state and the Output feedback still detects that the output is energized, the Vital Software shall Shutdown. If the Output is in failed state, and if no energy is detected, the Vital Software shall retry to turn Output ON after some determined time (15s), if the commanded state is energized. To protect against FPGA free-running the Output switch is implemented using a latch controlled from an output pin of the CPU. If the Vital Software determines that the Hardware circuit is generating an output when it's meant to be deenergized, the Vital Software can cut the output to the DC-DC converter by opening the Output Switch.	Yes
		Short Gate & Drain	Output always enabled.	5	5	5	125		
		Short Source & Drain							
		Short Gate & Source							
	Output Feedback Opto Coupler	Open output transistor	Irrespective of the Output the feedback signal to FPGA is always high.	8	5	5	200	If the Vital Software determines that the output is energized from its reading of the Output feedback when it should be de-energized or vice versa then the Vital Software will put the Output into the failed state. If the Output is in failed state and the Output feedback still detects that the output is energized, the Vital Software shall Shutdown. If the Output is in failed state, and if no energy is detected, the Vital Software shall retry to turn Output ON after some determined time (15s), if the commanded state is energized.	Yes
		Shorted output transistor	Irrespective of the Output the feedback signal to FPGA is always high.						
		Open Input LED	Irrespective of the Output the feedback signal to FPGA is always high.						
		Shorted Input LED	Irrespective of the Output the feedback signal to FPGA is always low.						
	Output Inductors	Open	Output cannot be enabled.	2	2	5	20	No need as de-energized state is safe state.	Yes
		Short	No immediate Safety effect. No error is reported.	1	2	5	10	No Defense necessary.	Yes

6 Conclusions

FMEA is one of the most effective safety analyses for achieving high quality system within specified timelines and budget constraints. A brain storming session was performed with the industry experts to conduct the FMEA of Automatic Door Operations. A case study of ADO module of the metro train is presented in this paper. The intension of this study was threefold: to create awareness for failures and their potential causes in order to prevent them, to point out how severe and critical

potential failures may be and to show how they can be eliminated by offering solutions for different causes. As such, FMEA can be a time consuming process, but the results can be very worthwhile. However one has to obtain management support for the project, and the team leader's skills in keeping a team motivated and progressing through the project is essential to ensure the completion of a successful project.

Acknowledgement. Authors wish to thank Dr. Phanibhushan Sistu and Naveen Nair of Cognizant Technology Solution, Hyderabad, for their constant motivation, support and valuable feedback. Thanks are also due to Veerabhadra Prasad Gottimukkala and Vivek Diwanji for their constructive comments and suggestions which are very helpful in improving the paper.

References

1. Leveson, N.G.: Software Safety: Why, What, and How. Computing Surveys 18(2), 125–163 (1986)
2. Ericson, C.A.: Hazard Analysis Techniques for System Safety. Wiley Interscience, New Jersey (2005)
3. Maier, T.: FMEA and FTA to Support Safe Design of Embedded Software in Safety Critical Systems. In: 12th Annual CSR Workshop on Safety and Reliability of Software Based Systems, pp. 351–367 (1997)
4. Lutz, R.R., Woodhouse, R.M.: Bi-directional Analysis for Certification of Safety-Critical Software. In: Proceedings of International Software Assurance Certification Conference, Chantilly, VA, February 28–March 2 (1999)
5. Goddard, P.L.: Software FMEA Techniques. In: Proceedings of Annual Reliability and Maintainability Symposium, Los Angeles, CA, pp. 118–123 (2000)
6. Ericson, C.A.: Software and System Safety. In: Proceedings of the 5th International System Safety Conference 1, part 1, III-B-1–III-B-11 (1981)