Journal of Engineering and Technology

ISSN 2180-3811 eISSN 2289-814X https://jet.utem.edu.my/jet/index

ENHANCING SAFETY AND RELIABILITY IN RAILWAY SIGNALLING SYSTEMS: A COMPREHENSIVE FMEA-BASED APPROACH

D. Sheikhi*[1], B. Ghorbani[1] and Z. Ahmadi[1]

[1] School of Railway Engineering, Iran University of Science and Technology, Tehran Province, Tehran, District 8, Dardasht St, Iran.

corresponding: donyasheikhi75@gmail.com

Article history:
Received Date:
16 October 2023
Revised Date:
14 May 2024
Accepted Date:
14 June 2024

Keywords:
Railway Signaling, Object Controllers, Risk Assessment, FMEA

Abstract— Railway signalling systems, classified as safety-critical systems, must adhere to specific safety principles outlined in CENELEC standards to ensure the desired levels of safety and reliability. The Interlocking system serves as the central intelligence behind railway signalling, authorizing trains to navigate safe routes under predefined conditions, eliminating collision risks. Object controllers (OCs), a crucial component of the interlocking subsystem, are responsible for overseeing and managing field elements such as signals, points, track circuits, and other vital controllable objects. Object controller boards encompass both hardware and software components, necessitating

compliance with relevant railway safety standards such as EN50129 and EN50126. This paper focuses on a developed test platform designed to streamline the design and development life cycle of Object controllers. Within this tool, the importation of system architecture facilitates risk identification and assessment using the Failure Modes and Effects Analysis (FMEA) method. Ultimately, the paper calculates the reliability of both subsystems and the entire system.

I. Introduction

Railway transport networks, while experiencing a lower frequency of collisions compared to roadways, can still result in catastrophic consequences in terms of human injuries, loss of life, and damage to rolling stock and infrastructure. This underscores the paramount importance of safety in railway operations. The railway signalling system is pivotal in ensuring the safe, reliable, and efficient movement of trains Its development must adhere to both domestic and international rail transit signal system standards, drawing from the extensive application experience in this field. Moreover, strict adherence to the entire life cycle of safety product development is imperative, with all signalling subsystems undergoing rigorous third-party safety certifications. The signalling system has the following technical features:

1. The signalling system prioritizes safety, strictly adhering to international standards (EN50126/8/9) and the "fail-safety" principle. It meets SIL4 (Safety Integrity Level 4) safety requirements and holds SIL4 safety certification from an independent third-party authority for all safety-related signal subsystems.

2. The system achieves high reliability and continuous operation using dependable equipment and built-in redundancy technology.
3. The system boasts high maintainability with reduced costs. Key equipment features redundancy, self-diagnosis, and alarm functions. It also utilizes a unified hardware platform, effectively minimizing maintenance time and expenses.
4. The wayside subsystem controller employs a safety redundancy structure (2x2 out of 2) and holds an SIL4 safety certificate from an independent third-party authority. It integrates interlocking and train control functions, reducing software and hardware complexity and enhancing system reliability.
5. The loss of line synchronism indicates a disruption in signal synchronization along the line.

In contrast, the on-board control subsystem prioritizes vehicle compatibility by ensuring that components like the On-Board Computer Unit (OBCU), speedometer, accelerometer, transponder reader, and antenna are compact and easily installable within the vehicle's limited space. Additionally, the vehicle control algorithm and interface of on-board equipment can be adjusted to match specific vehicle characteristics.

To enhance railway network safety and mitigate hazards, various critical on-board and trackside systems have been implemented. A track circuit -a vital safety critical component- serves as an electrical trackside device designed to detect the absence of a train within a specific track section. This equipment transmits essential data used to establish conflict-free routes in overlap and flank protection areas within the signalling system. It operates by passing an electric current from a power supply at one end of the section, through the rails, to a relay positioned at the other end. When a train enters the section, the relay deactivates due to the lower resistance of the train

axles compared to the relay itself. This action signals to the signalling system that a train is present in the track section, ensuring safe and efficient railway operations. In Figure 1, the track circuit and its associated subsystems are depicted.

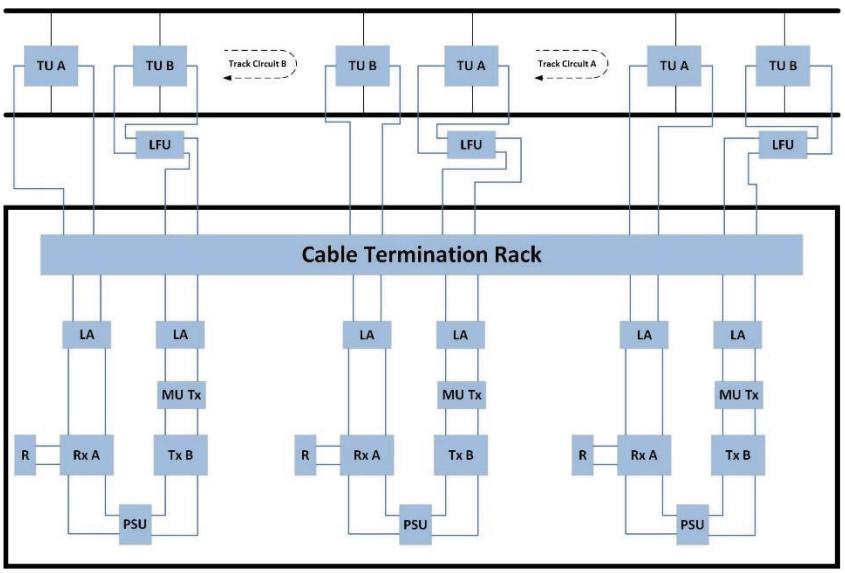


Figure 1: A track circuit with its subsystems [1]

Each track circuit is supervised and regulated by a crucial component known as the OC. In the domain of railway signaling systems, OCs play a pivotal role in overseeing and managing critical trackside equipment. Given their significance in ensuring the safety and reliability of railway operations, there exists a pressing need for a dedicated risk assessment tool tailored specifically for OCs. This tool is essential to systematically identify, evaluate, and mitigate potential risks associated with OCs, thereby preempting operational disruptions and enhancing overall safety standards within railway signaling networks. As for the specific objectives of the risk assessment tool, its primary aim is to comprehensively identify and analyze risks inherent in OC operations,

encompassing both hardware and software components. By leveraging advanced methodologies such as FMEA and Fault Tree Analysis (FTA), the tool seeks to proactively anticipate potential failure scenarios and their corresponding impacts. Additionally, the tool aims to streamline risk mitigation strategies, enabling railway operators to implement targeted interventions to minimize risks and uphold safety standards. Through rigorous adherence to safety standards such as EN50129 and EN50126, the tool ensures compliance with regulatory requirements and certification criteria for OCs, thus bolstering confidence in the reliability and safety of railway signaling systems. Furthermore, the tool incorporates innovative features such as real-time data integration and predictive analytics, offering enhanced capabilities compared to traditional risk assessment approaches. The OC is responsible for overseeing and monitoring its associated wayside elements and transmitting relevant data to the interlocking system to establish appropriate train routes. The failure of any track circuit OC or its associated field elements can result in substantial disruptions to train movement routes and pose critical safety hazards. To mitigate such risks, the implementation of a well-structured design and development methodology is imperative. Given that most of a system's design and development life cycle costs are tied to decisions made during the design phase, it becomes imperative to prioritize the safe and standardized design, development, and reliability analysis of OCs throughout these critical processes.

In this research, we introduce a developed test platform designed for the evaluation of railway signaling Object Controller boards. Specifically, we focus on testing a typical track circuit OC board. This platform offers capabilities such as system architecture extraction, risk assessment using the FMEA method, and equipment reliability calculations. In

accordance with the EN50126 standard, critical components within safety- critical systems are designed in duplicate forms for increased efficiency and calculation accuracy, as outlined in Table 1.

Table 1: Acceptable structure of the tested board's blocks

Subsystems	Redundancy Types
Power Supply	1001 & 1002 & 1003
Connector	1001 & 1002
Diode	1001 & 1002 & 2002
Filter	1001 & 1002
Fuse	1001 & 1002 & 1003
Current Sensor	1001 & 1002 & 1003 & 2003
Relay	1001 & 1002 & 1003 & 2002 & 2003 & 3003
MOSFET	1001 & 1002 & 1003
Logic Gate	1001 & 1002 & 1003
Resistance Block	1001 & 1002 & 1003
Op-amp	1001 & 1002 & 1003
Resistance Block	1001 & 1002 & 1003
Microcontroller	1001 & 1002 & 1003 & 2002 & 2003 & 3003
CAN IC Converter	1001 & 1002 & 1003

The assessment process begins by evaluating these redundant blocks and abstracting the system's structure. Subsequently, based on the nature of the subsystems' structure, whether they are in series, parallel, or a combination of both, the platform calculates the overall system reliability level. To assess its performance accuracy, the process is conducted on a standard track circuit OC board. This OC board comprises critical sub-sections that demand adherence to safety standards, given their safety-critical significance. These subsections encompass key components such as the processing unit, linear/switching power supplies, data transfer module, connectors, self- test, and object monitoring unit, among others.

II. Reliability Analysis

Reliability, denoted as 'R,' is a critical product attribute defined as the probability that a product or system can perform its required task under specified conditions for a defined duration without failure [2]. Enhancing the reliability of railway signaling systems is of paramount importance to

preventpotential breakdowns and mitigate the risk of collisions or accidents leading to passenger injuries during system operation [3]. Risk assessment in the design of control command and signaling devices (CCS) is one of the elements required by law [4]. A systematic and comprehensive risk assessment is essential for the success of railway construction projects. Even though numerous studies have been conducted on railway construction project risk assessment, few attempts have been made to evaluate the overall dynamics, inter relationships, uncertainty, and impact of risks on project objectives [5]. Risk management stands as an integral component of project success, serving as a process for early problem identification and the implementation of necessary measures to preempt the transformation of potential issues into critical project challenges. The evaluation of risks necessitates an assessment based on both their likelihood of occurrence and analysis, and fault tree evaluation.

In this research endeavor, we have developed a software tool designed to assess and calculate the reliability level during the design phase of high-level systems. This tool streamlines the sensitive process integral to the development and testing life cycle of safety-critical systems. FMEA stands as the most effective and widely employed technique for identifying, assessing, and preventing potential hazards across diverse fields. Numerous risk analysis models, rooted in FMEA, have been utilized to identify, evaluate, and prioritize risks, thereby enhancing the reliability of complex systems [6]. This analysis represents a systematic approach aimed at identifying and preempting issues within both the product and its associated processes.

The primary focus of this method is to proactively prevent defects, enhance safety, and elevate customer satisfaction. Additionally, it aids organizations in anticipating problems in both product and

process, addressing their underlying causes proactively before they manifest. Hence, employing the FMEA method for risk assessment offers the capability to pinpoint diverse factors with the potential to trigger adverse conditions and operational accidents. FMEA was initially developed by the US military in the 1940s and gained widespread adoption in the mid-1960s when it was embraced by the National Aeronautics and Space Administration (NASA) for use in manned space missions [7].

In today's context, complex equipment and systems are required not only to operate flawlessly at time t = 0 (start-up moment) but also to maintain their intended function without failure for a specified duration, even when critical faults occur [8]. Enhancing system reliability requires early identification of potential risks and hazards during the design phase. In [9], multiple modeling techniques are employed to compute the reliability of trackside equipment within the signaling system, encompassing components like point machines, track circuits, and signals, while also considering the overall system failure rate. Paper [10] introduces a modified FMEA methodology to comply with EU regulations for risk assessment in railway transport, specifically focusing on safety at railway crossings due to issues in Slovakia. By investigating accident causes and proposing a new methodology framework, the paper aims to assist railway infrastructure managers in identifying and mitigating risks, ultimately improving safety and service quality in rail transport.

In this research, an application plan is formulated. It entails the identification and analysis of errors, encompassing causes, effects, mechanisms, and states, utilizing the FMEA method. Additionally, the research offers an automated solution designed to decrease life cycle costs while simultaneously enhancing safety and reliability. The tool is coded in C# and defines 14 primary hardware blocks for the high-level electronic board design. By identifying the necessary blocks for board design, establishing

their reliability levels, and determining the extent of redundancy, the FMEA table is generated, considering subsystem features like redundancy values. This allows the designer to achieve the desired design by making revisions if necessary. The data presented in Table 2 conforms to the EN50129 standard, which mandates a comprehensive investigation of designated risks; proportion of our results is displayed within Table 2.

Safety standards, including MIL-HDBK-217F, have been formulated on established principles to guide designers. The method presented in this paper offers the capability for automated reliability assessment at both subsystem and system-wide levels. To compute the failure rate and reliability of the system and its subsystems, the Reliability Block Diagram (RBD) method has been employed. In accordance with the stipulations of EN50128 and EN50129 standards, for the formal implementation of the system verification process, the high-level design furnished by the designer is translated into an integrated modeling language (PLANT UML) using the tool developed. Consequently, by creating a block diagram mapping of subsystems and depicting their connections and dependencies using an integrated modeling language, the reliability of both the system and its subsystems has been computed. This calculation considers the architecture and series/parallel structure of the blocks, as well as the Mean Time Between Failures (MTBF) values, all contributing to the enhancement of system safety.

Figure 2 illustrates the characteristics of each block and their interrelationships in the form of a class diagram. The test platform leveraged this information to evaluate risks and compute the reliability of individual subsystems as well as the entire system. Any complex system can undergo evaluation by abstracting its hardware architecture design and calculating the reliability of each block, along with its connections to other blocks. The configuration of these blocks

and their reliability calculation method align with one of the models depicted in Figure 3.

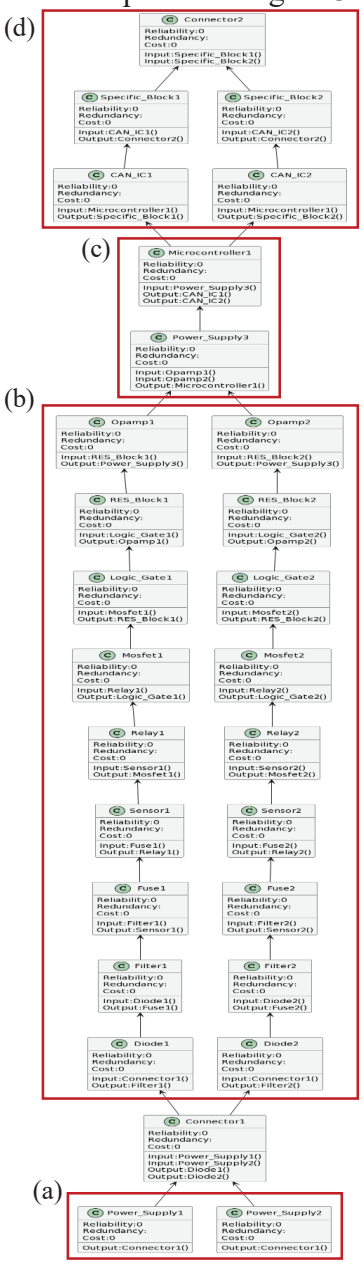


Figure 2: Class diagram of the Track Circuit Board (TC board)

III. Risk Assessment Analysis

Safety covers preventing injuries and reducing hazards during system operation. It includes two aspects which are safety during normal operation and safety during failures. The first focuses on accident prevention under regulations. The second deals with safety during error and involves a five steps process.

i. risk identification
ii. cause identification
iii. effects determination
iv. classification
v. risk prevention/mitigation

Early train safety used mechanical interlocking systems, now replaced by electronic ones. These require both safety and reliability. Safety assures components remain safe during failures (fail-safe). Reliability aims to minimize failures. Research emphasizes risk assessment across design, development, and maintenance. Techniques like FTA and Event Tree Analysis (ETA) identify hazards and potential loss of life.

A methodological approach enhances railway system

reliability, assessing human errors and control system failures using Failure Modes, Effects, and Criticality Analysis (FMECA) and Human Reliability Analysis (HRA). A FMEA model prioritizes risks in railway systems, considering severity, occurrence, and detectability. Integrated tools for risk assessment, modeling, reliability calculation, and system design are lacking in railway standards compliance. This research introduces a tool for risk assessment and compliance. It identifies vulnerabilities by generating an FMEA table based on EN50129 standards. The tool calculates subsystem and system reliability using parameter values and equations. Complex structures are simplified for reliability calculations.

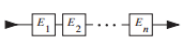
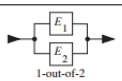
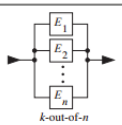
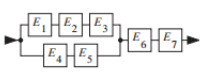
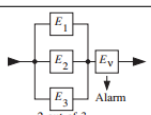
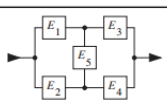
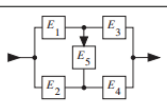
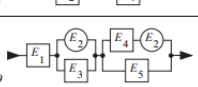
Reliability Block Diagram	Reliability Function ($R_S = R_{S0}(t)$; $R_i = R_i(t)$, $R_i(0) = 1$)	Remarks
1 	$R_S = R_i$	One-item structure, $\lambda(t) = \lambda \Rightarrow R_i(t) = e^{-\lambda_i t}$
2 	$R_S = \prod_{i=1}^{n} R_i$	Series structure, $\lambda_S(t) = \lambda_1(t) + \ldots + \lambda_n(t)$
3  1-out-of-2	$R_S = R_1 + R_2 - R_1 R_2$	1-out-of-2-redundancy, $R_1(t) = R_2(t) = e^{-\lambda t}$ $\Rightarrow R_S(t) = 2e^{-\lambda t} - e^{-2\lambda t}$
4  k-out-of-n	$E_1 = \ldots = E_n = E$ $\rightarrow R_1 = \ldots = R_n = R$ $R_S = \sum_{i=k}^{n} \binom{n}{i} R^i (1-R)^{n-i}$	k-out-of-n redundancy for $k = 1$ $\Rightarrow R_S = 1 - (1-R)^n$ see p. 44 for $E_1 \neq \ldots \neq E_n$
5 	$R_S = (R_1 R_2 R_3 + R_4 R_5 - R_1 R_2 R_3 R_4 R_5) R_6 R_7$	Series-parallel structure
6  2-out-of-3 Alarm	$E_1 = E_2 = E_3 = E$ $\rightarrow R_1 = R_2 = R_3 = R$ $R_S = (3R^2 - 2R^3) R_V$	Majority redundancy, general case $(n+1)$-out-of-$(2n+1)$, $n = 1, 2, \ldots$
7 	$R_S = R_5 (R_1 + R_2 - R_1 R_2) \cdot (R_3 + R_4 - R_3 R_4) + (1 - R_5) \cdot (R_1 R_3 + R_2 R_4 - R_1 R_2 R_3 R_4)$	Bridge structure (bi-directional on E_5)
8 	$R_S = R_4 [R_2 + R_1 (R_3 + R_5 - R_3 R_5) - R_1 R_2 (R_3 + R_5 - R_3 R_5)] + (1 - R_4) R_1 R_3$	Bridge structure (unidirectional on E_5)
9 	$R_S = R_2 R_1 (R_4 + R_5 - R_4 R_5) + (1 - R_2) R_1 R_3 R_5$	The element E_2 appears twice in the reliability block diagram (not in the hardware)

Figure 3: Reliability evaluation of simple systems

ISSN: 2180-3811 Vol. 15 No. 1 January - June 2024

Table 2: FMEA evaluation of the power supply block

FMEA Report	system: SIG-OC (Signal Object Controller) Module	subsystem: power unit		date of writing:		
Code	failure mode	causal factors	imm. eff	sys. eff	Recom. Action	Comment
FMEA-SIG-P-1	open circuit in Series elements (Fuse, Transformer)	Bad Soldering, Burning out	Power disconnection	The board power off and become inaccessible	Use a checklist after soldering and making an indicator for power, use redundant power lines, and test points be provided	
FMEA-SIG-P-2	short circuit in Series elements (Fuse, Transformer)	Burning out, Rush current, Over Current	Power disconnection in some cases	The board power off, Ignorance of protection	Use a checklist after soldering and making an indicator for power	
FMEA-SIG-P-3	open circuit in Parallel elements (capacitors, MOVs, …)	Overvoltage at the input power line, Using improper capacitors, Poor soldering	Bad filtration of the power signal, Weak protection against unusual input signals	The board burnt, Change in logic levels, and errors in calculations	Use proper Soldering oil and tin, prepare a checklist for testing elements after soldering, and test points be provided	test point to be provided for all units of the board
FMEA-SIG-P-4	short circuit in parallel elements (capacitors, MOVs, …)	Overvoltage at the input power line, Using improper capacitors	The power line became short circuit and fuses will burn	The board power is off and gets damaged, making damage to the power unit	Use capacitors that became open circuit in case of failure, Use redundant power lines	class Y caps (EN50129)

					The track should become occupied in the system, use at least an Industrial Type DC/DC converter, and use proper tolerance for input power, use redundant power lines, appropriate alarms should be sent to the CP and/or maintenance operator, provide an LED indicator for indoor faults	A specific company or model can be named
FMEA-SIG-P-5	24 to 5 converters short circuit	Burning out because of high input power	Power off the board	The board became inaccessible and lack of knowledge about the track occupancy		
FMEA-SIG-P-6	24 to 5 output oscillation	Oscillation at input power, Working at out of temperature range	Change in logic levels and get wrong information about the field	IM take the wrong decision, and a mishap would occur	Use a DC/DC Converter with higher stability and lower ripple, Use Industrial type	Values can be mentioned
FMEA-SIG-P-7	5 to 3.3 converter short circuit	Burning out because of high input power	Power off microcontroller	The board became inaccessible and lack of knowledge about the track occupancy	The track should become occupied in the system, using at least an Industrial Type DC/DC converter, and using proper tolerance for the input power, using redundant power lines, providing an LED indicator for indoor faults	

FMEA-SIG-P-8	5 to 3.3 converter short circuit	Burning out because of high temperature	Power off microcontroller	The board became inaccessible and lack of knowledge about the track occupancy	The Track should become occupied in the system, using at least ab Industrial Type DC/DC converter with higher efficiency, using a heat sink according to the element's heat	safe mode should be defined for different fail Modes and the board should switch to the safe mode in case of a failure
FMEA-SIG-P-9	5 to 3.3 output oscillation	Oscillation at input power, working out of temperature range, Choosing improper values for related elements	Burning out microcontroller, Troubles happen in data communication	lack of knowledge about the track occupancy, IM take wrong decisions and mishaps would occur	Using a DC/DC Converter with higher stability and lower ripple, Using Industrial type	
FMEA-SIG-P-10	Signal 30v power failure	Input power off,	TC out of service	impossible to set routes which that TC belongs to them	power supply monitoring, redundant power supply to be provided, providing an LED indicator for indoor faults	For this purpose, the power line should be across the board for being monitor able

For example, row 5 in Figure 3 demonstrates methods (i) to (iii) and this simplifies the reliability calculation as shown in Figure 4.

i. Series blocks B1-B3 are replaced by B8.
ii. B4-B5 are replaced by B9.
iii. B6-B7 are replaced by B10.

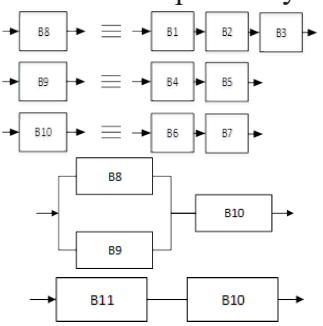


Figure 4: Example of simplified reliability block diagram

$$\mathbf{R_{10}(t) = R_6(t)R_7(t)} \quad (1)$$

$$\mathbf{R_{11}(t) = [R_8(t) + R_9(t)] - [R_8(t)R_9(t)]} \quad (2)$$

where, $R_8(t) = R_1(t)R_2(t)R_3(t)$ and $R_9(t) = R_4(t)R_5(t)$

From Equation (1) and (2), the system reliability is shown as Equation (3) and (4).

$$\mathbf{R_s = R_{s0}(t), R_i = R_i(t), R_i(0) = 1, i = 1, \dots 7} \quad (3)$$

$$\mathbf{R_s = R_{11}R_{10} = [(R_1R_2R_3) + (R_4R_5)] - [(R_1R_2R_3R_4R_5)][R_6R_7]} \quad (4)$$

The mean time to failure can be calculated from Equation (5) and (6). All elements should have a constant failure rate (λ1 to λ7), therefore,

$$R_{S0}(t) = e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_6+\lambda_7)t} + e^{-(\lambda_4+\lambda_5+\lambda_6+\lambda_7)t} + e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4+\lambda_5+\lambda_6+\lambda_7)t} \quad (5)$$

$$\boldsymbol{MTBF_{S0}} = \frac{1}{\lambda_1+\lambda_2+\lambda_3+\lambda_6+\lambda_7} + \frac{1}{\lambda_4+\lambda_5+\lambda_6+\lambda_7} - \frac{1}{\lambda_1+\lambda_2+\lambda_3+\lambda_4+\lambda_5+\lambda_6+\lambda_7} \quad (6)$$

To forecast the reliability of each electrical / electronic element, the standard 'MIL-HDBK-217F' offers a standardized foundation, relying on the analysis of the most up-to-date data available at the time of publication. According to this standard, the failure rates of resistors and capacitors are calculated as Equation (7).

$$\lambda_p = \lambda_b \pi_{cv} \pi_Q \pi_E Failure/10^6 Hour \quad (7)$$

where, λ_b is based failure rate, π_E is environment factor, π_Q is quality factor.

In calculating the board failure rate, the failure rate of passive elements (ceramic resistors and capacitors) due to their small values can be neglected.

The equation of Relays failure rate is shown in Equation (8).

$\Lambda_p = \lambda_b \pi_L \pi_c \pi_{cyc} \pi_F \pi_Q \pi_E Failure/10^6 Hour$ (8)

where, π_L, π_{cyc}, π_c, π_F are load stress, cycling, contact, and application and construction factors respectively. Referring to a typical relay's datasheet, its failure rate is shown in Equation (9).

$\lambda_p = 0.1 * 10^{-6}/\text{OPERATION}$ (9)

Hence, its reliability value is,

$R = e^{-\lambda t} = e^{-(0.1 \times 8760) \times 10^{-6}} = 0.9991$ (10)

The failure rate of active components like Bipolar operational amplifiers equation is shown in Equation (11).

$\Lambda_p = [\sum N_c \lambda_c][10.2\pi_E]\pi_F \pi_Q \pi_L \, Failure/10^6 Hour$ (11)

where, λ_c is failure rate of each component, N_c is number of each component, π_F is circuit function factor, π_L is learning factor.

In this research, LM321 is used as the Op-Amp elements which its failure rate is given by Equation (12).

$\lambda_p = C_1 \pi_T \pi_Q \pi_L Failure/10^6 Hour$ (12)

Hence, the value of reliability per one-year is

$R = e^{-\lambda t} = e^{-(0.31 \times 8760) \times 10^{-6}} = 0.9973$ (13)

For the other elements, the failure rate and reliability quantities are summarized in Table 3. After calculating the reliability of each block, the tool calculates the series-parallel blocks reliability according to Figure 3.

Table 3: Failure rate and reliability for other elements

Element	Failure rate	Reliability
Gates	$\lambda_p = (C_1 \pi_T + C_2 \pi_E)\pi_Q \pi_L$ Failure /10^6 Hours $= 0.0477$ Failure /10^6 Hours	$R = e^{-\lambda t} = e^{-(0.0477 \times 8760) \times 10^{-6}} = 0.99958$
MOSFET	$\lambda_p = 0.00533$ Failure /10^6 Hours	$R = e^{-\lambda t} = e^{-(0.00533 \times 8760) \times 10^{-6}} = 0.999953$

Filters	$\lambda_p = \lambda_b \pi_Q \pi_E$Failure /$10^6$ Hours $= 0.696$Failure /10^6 Hours	$R = e^{-\lambda t}$ $= e^{-(0.696 \times 8760) \times 10^{-6}}$ $= 0.9939$
ICs	$\lambda_p = (C_1 \pi_T \pi_A + C_2 \pi_E) \pi_Q \pi_L$Failure /$10^6$ Hours $= 0.9052$Failure /10^6 Hours	$R = e^{-\lambda t}$ $= e^{-(0.9052 \times 8760) \times 10^{-6}}$ $= 0.9921$
Fuses	$\lambda_p = \lambda_b \pi_E$Failure /$10^6$ Hours $=0.02$Failure /10^6 Hours	$R = e^{-\lambda t}$ $= e^{-(0.02 \times 8760) \times 10^{-6}}$ $= 0.99982$
Diodes	$\lambda_p = \lambda_b \pi_T \pi_S \pi_C \pi_Q \pi_E$Failure /$10^6$ Hours $=0.0069$Failure /10^6 Hours	$R = e^{-\lambda t}$ $= e^{-(0.0069 \times 8760) \times 10^{-6}}$ $= 0.99994$
Connectors	$\lambda_p = 0.0313$Failure /10^6 Hours	$R = e^{-\lambda t}$ $= e^{-(0.0313 \times 8760) \times 10^{-6}}$ $= 0.99972$
Sensors	$\lambda_p = 0.09$Failure /10^6 Hours	$R = e^{-\lambda t}$ $= e^{-(0.09 \times 8760) \times 10^{-6}}$ $= 0.99921$
Power supplies	$\lambda_p = 0.075$Failure /10^6 Hours	$R = e^{-\lambda t}$ $= e^{-(0.075 \times 8760) \times 10^{-6}}$ $= 0.99934$

Q represents the probability of failure in reliability analysis. The relationship between Q and R can be expressed as $Q = 1 - R$. For parallel blocks, Q can be expressed as Equation (14).

$$Q_p = \prod_{i=1}^{n} Q_i \quad (14)$$

For simplifying the calculation of reliability in parallel blocks, Q can be employed as a convenient metric. Next, the reliability for each block as depicted as (a), (b), (c) and (d) in Figure 2 are calculated.

For (a);

$$R_p = 1 - \prod_{i=1}^{n} Q_i \quad ,$$

$$R_{s2} = 1 - (Q_{11} \times Q_{12}) = 1 - (0.00066 \times 0.00066) = 0.9999996 \quad (15)$$

For (b);

$$R_{ps} = (R_{p2} \times R_{p3} \times R_{p4} \times R_{p5} \times R_{p6} \times R_{p7} \times R_{p8} \times R_{p9} \times R_{p10} \times R_{p11} \times R_{p12} = 0.98856$$

$$Q = 1 - 0.98856 = 0.01144$$

$R_{s2} = 1 - (Q_{11} \times Q_{12}) = 1 - (0.01144 \times 0.01144) = 0.99987$ (16)

For (c);

$R_{ps} = (R_{p13} \times R_{p14}) = 0.9993$ (17)

For (d);

$R_{ps} = (R_{p15} \times R_{p16} \times R_{p17}) = 0.986$

$Q = 1 - 0.986 = 0.014$

$R_{p2} = 1 - (Q_{21} \times Q_{22}) = 1 - (0.014 \times 0.014) = 0.9998$ (18)

By calculating subsystem's reliability, the value of total systems reliability is shown in Equation (19).

$R_{t1} = R_{s1} \times R_{s2} \times R_{s3} \times R_{s4} = 0.9999996 \times 0.99987 \times 0.9993 \times 0.9998 = 0.99897$ (19)

IV. Conclusion

Object controllers entrusted with the critical tasks of controlling and monitoring trackside equipment, hold a pivotal role in ensuring safety and reliability within railway systems. As such, their design and development processes demand strict adherence to safety standards. This paper has embarked on the mission to streamline these processes by delving into the architecture of OC boards and the analytical methods governing reliability.

The result of this endeavor is a sophisticated software platform tool, meticulously crafted to align with safety and functional standards. During the design phase of this test platform, precise parameters related to reliability and redundancy, for each hardware block, along with their interconnections, are defined. Furthermore, the tool seamlessly generates an integrated modeling language representation of the control board plan, employing PLANT UML, while concurrently applying the FMEA method for risk assessment.

This comprehensive approach culminates in the calculation of the system's reliability, ultimately yielding results that align with safety and reliability standards. This work underscores the instrumental role of FMEA analysis in not only identifying potential hazards within both the product and its associated processes but also in proactively mitigating risks and bolstering safety measures. Consequently, it

paves the way for achieving the desired levels of reliability at the device level, marking a significant stride towards enhanced safety and reliability in railway signaling systems.

V. References

[1] J. Scalise, "How Track Circuits detect and protect trains," *Railwaysignalling*. 1-7, 2014.

[2] Zhang, Rong et al., "Reliability analysis on railway transport chain," *International Journal of Transportation Science and Technology*, 2019.

[3] P.E. Rahmayana, H.H. Purba, "Risk Management in Railway During Operation and Maintenance Period A Literature Review," *International Journal of Engineering Applied Sciences and Technology,* 2019.

[4] P. Ilczuk, M. Kycko, "Risk Assessment in the Design of Railroad Control Command and Signaling Devices Using Fuzzy Sets," *Applied Sciences*, vol. 13, no. 22: 12460, 2023.

[5] T. Gashaw and K. Jilcha, "Design risk modeling and analysis for railway construction projects," *International Journal of Construction Management*, 23(14), pp. 2488–2498, 2023.

[6] W. Wang, Y. Wang, and X. Han, "A dynamic failure mode and effects analysis for train systems failures risk assessment using FCM and prospect theory," *Management System Engineering*, 2022.

[7] A. Mascia, A.M. Cirafici, A. Bongiovanni, et al. "A failure mode and effect analysis (FMEA)-based approach for risk assessment of scientific processes in non-regulated research laboratories," *Accred Qual Assur*, 25, pp. 311–321, 2020.

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

[9] L. Tang, "Reliability assessments of railway signaling systems: A comparison and evaluation of approaches," *Master Thesis, Norwegian University of Science and Technology, Department of Industrial Economics and Technology Management*, June 2015.

[10] E. Nedeliaková, M. Hranický and M. Valla, "Risk identification methodology regarding the safety and quality of railway services," *Production Engineering Archives*, Vol. 28 (Issue 1), pp. 21-29, 2022.

[11] A. Birolini, "Basic concepts, quality and reliability (RAMS) assurance of complex equipment and systems," *Reliability Engineering: Theory and*

Practice, pp.1-24.

[12] F. D. Felice, A. Petrillo, "Methodological Approach for Performing Human Reliability and Error Analysis in Railway Transportation System," *International Journal of Engineering and Technology* Vol. 3 (5), 341-353, 2011.

[13] Fu, Yong et al, "An Extended FMEA Model Based on Cumulative Prospect Theory and Type-2 Intuitionistic Fuzzy VIKOR for the Railway Train Risk Prioritization," *Entropy (Basel, Switzerland)*, Vol. 22, 12, 1418, 2020.

[14] P. Liu, M. Shen, "Failure Mode and Effects Analysis (FMEA) for Traffic Risk Assessment Based on Unbalanced Double Hierarchy Linguistic Term Set,". *Int. J. Fuzzy Syst. 25*, 423–450, 2023.