
**RELIABILITY IMPROVEMENT OF IOT-BASED SECURITY MONITORING DEVICES
THROUGH INTEGRATED FAULT TREE ANALYSIS AND FAILURE MODE AND
EFFECT ANALYSIS**

<satu spasi>

Muhammad Ardiansa¹, Franka Hendra^{2*}, Surasa³¹ Department of Industrial Engineering, Universitas Pamulang, South Tangerang, IndonesiaCorresponding author: dosen01508@unpam.ac.id**Abstract**

The increasing implementation of Internet of Things (IoT)-based security monitoring systems requires high communication reliability to ensure continuous and accurate data transmission. However, connectivity failures caused by electronic component degradation, communication instability, and device design limitations remain significant challenges that can reduce system performance. This study aims to analyze the root causes of connectivity failures and develop reliability improvement strategies for IoT-based security monitoring devices using an integrated Fault Tree Analysis (FTA) and Failure Mode and Effect Analysis (FMEA) approach. The research was conducted on the Alarm Node-PR22 device at PT Eyro Digital Teknologi using failure data collected from October 2024 to March 2025. A total of 66 failures were identified from 500 installed devices, consisting of 3.3V Power IC failure, internal antenna failure, total device failure, and SIM800 module overheating. The FTA method was applied to identify failure pathways and determine basic causes, while FMEA was used to evaluate risk priorities based on severity, occurrence, and detection parameters. The results showed that 3.3V Power IC failure was the dominant failure mode with a total Risk Priority Number (RPN) of 1390, followed by total device failure (1328), SIM800 overheating (1198), and internal antenna failure (902). The highest individual risk factors were permanent IC silicon layer damage and PCB short circuit caused by solder bridging, both with an RPN value of 648. Based on these findings, improvement strategies were proposed, including component replacement, maintenance improvement, ESD protection implementation, casing redesign, and PCB layout optimization. The integration of FTA and FMEA provides an effective reliability analysis framework for identifying failure mechanisms and improving the operational reliability of IoT-based security monitoring devices.

Keyword: Internet of Things; Reliability Analysis; Fault Tree Analysis; Failure Mode and Effect Analysis; Connectivity Failure; Security Monitoring System

INTRODUCTION

The rapid development of Internet of Things (IoT) technology has accelerated the transformation of conventional monitoring systems into intelligent systems capable of collecting, transmitting, and processing data through interconnected communication networks. IoT implementation has been widely adopted in various sectors, including industrial monitoring, healthcare, transportation, and security systems, due to its capability to provide real-time information and support automated decision-making processes. However, the effectiveness of IoT-based monitoring systems strongly depends on communication reliability, data transmission stability, and continuous network availability. Recent studies have highlighted that connectivity performance, communication protocols, and network reliability are critical factors influencing the operational performance of IoT applications, particularly in systems requiring continuous data transmission (Al-Turjman & Al-Fagih, 2020; Ferrag et al., 2020; Sethi & Sarangi, 2021; Hendra et al 2024).

In IoT-based security monitoring systems, connectivity disruption can become a critical problem because communication failure may prevent alarm information from being transmitted to the monitoring center. Network instability, signal attenuation, limited communication capacity, and hardware degradation can cause delays, data loss, or complete failure of information delivery. Several studies have emphasized that reliability challenges in IoT systems are associated with communication quality, energy limitations, environmental conditions, and device-level failures (Ammar et al., 2021; Sicari et al., 2021). Although GSM-based communication remains widely applied in remote IoT devices due to its extensive coverage and relatively low implementation cost, limitations related to signal quality, bandwidth capacity, and infrastructure availability may affect

system reliability, especially in long-term operational environments (Ali et al., 2020; Mekki et al., 2019; Hendra et al 2021).

To improve system reliability, failure identification and risk analysis approaches are required to determine the root causes of disruptions and establish appropriate improvement strategies. Fault Tree Analysis (FTA) and Failure Mode and Effect Analysis (FMEA) are widely used reliability analysis methods because they provide systematic approaches for identifying failure mechanisms and prioritizing corrective actions. FTA applies a deductive approach by tracing failure events from the top event to basic causes, while FMEA evaluates potential failure modes based on severity, occurrence, and detection parameters to determine risk priority numbers (RPN). Recent studies have demonstrated the effectiveness of FTA and FMEA integration in identifying reliability problems in industrial systems, production processes, and equipment maintenance (Anwar et al., 2023; Nabila et al., 2025; Nur & Aulia, 2024; Ruspendi et al., 2025).

Previous applications of FTA and FMEA have mainly focused on manufacturing processes, product quality improvement, and production equipment reliability. These methods have been applied to analyze quality problems in manufacturing systems (Hanif et al., 2021), identify production process failures (Alhamda et al., 2023), evaluate machine reliability (Muhdor et al., 2023; Nabila et al., 2025), and determine risk mitigation strategies (Aulawi et al., 2022; Nur & Aulia, 2024). However, studies applying FTA and FMEA for analyzing connectivity failures in IoT-based security devices remain limited, particularly for devices that depend on GSM communication modules for real-time alarm transmission. Therefore, further investigation is required to understand the failure mechanisms of IoT communication devices and develop appropriate reliability improvement strategies.

PT Eyro Digital Teknologi develops and maintains Alarm Node-PR22 devices implemented in banking security systems. The device utilizes a SIM800-based 2G modem to transmit alarm signals from ATM security systems to the monitoring center. Since the device relies on continuous communication connectivity, the stability of power supply, antenna performance, communication modules, and electronic components becomes an essential factor affecting system reliability. Any failure in these components may interrupt alarm transmission and reduce the effectiveness of security monitoring operations.

Based on operational failure records from October 2024 to March 2025, 66 devices experienced failures from 500 installed Alarm Node-PR22 units. The identified problems consisted of 3.3V Power IC damage, internal antenna failure, total device failure, and SIM800 module problems. These conditions indicate that connectivity reliability issues still occur and require systematic analysis to determine the dominant causes and appropriate corrective actions.

Table 1. Total 2G Modem Damage Period October 2024 – March 2025

No	Month	Amount Device Installed on ATM Machine	Amount Damage (Device)	%
1	October	100	11	11 %
2	November	50	10	20 %
3	December	30	7	23 %
4	January	140	15	11 %
5	February	120	12	10 %
6	March	60	11	18 %
Total		500	66	13 %

(Source: Eyro Digital Teknologi, October 2024-March 2025)

The failure data indicate that connectivity problems are not only caused by individual component damage but may also result from interactions between electrical components, communication modules, environmental conditions, and device design factors. Therefore, a structured reliability analysis approach is needed to identify failure pathways, evaluate risk levels, and determine improvement priorities. The integration of FTA and FMEA provides a comprehensive framework by combining root cause identification and risk prioritization analysis.

This study aims to identify connectivity disruption modes occurring in the Alarm Node-PR22 device, determine the root causes and risk priority levels using FTA and FMEA methods, and develop improvement recommendations to reduce connectivity failures and enhance the reliability of IoT-based security monitoring systems.

METHOD

This study employed a qualitative approach supported by quantitative analysis to identify and evaluate the causes of connectivity failures in the Alarm Node-PR22 device at PT Eyro Digital Teknologi. The qualitative approach was applied to explore the failure mechanisms, identify the root causes, and analyze the relationship between failure factors based on field observations and technical investigations. Meanwhile, quantitative analysis was used to support the evaluation process through failure frequency analysis and risk assessment using the severity, occurrence, and detection parameters in the Failure Mode and Effect Analysis (FMEA) method.

The research was conducted on the maintenance activities of the Alarm Node-PR22 device at PT Eyro Digital Teknologi using failure data recorded during the period of October 2024 to March 2025. The research process consisted of several stages, including field observation, literature review, problem identification, data collection, failure cause analysis using Fault Tree Analysis (FTA), and risk evaluation using Failure Mode and Effect Analysis (FMEA).

The initial stage of the research involved field observation and literature review. Field observations were carried out through direct inspection of Alarm Node-PR22 devices experiencing connectivity problems, interviews with maintenance technicians, technical supervisors, and related personnel, as well as reviewing technical records related to troubleshooting and repair activities. Literature reviews were conducted by examining books, scientific journals, previous research, and other references related to Internet of Things (IoT) reliability, connectivity disruption, FTA, and FMEA.

The next stage was problem identification and problem formulation, which aimed to determine the main issues related to connectivity failures in the Alarm Node-PR22 device. After identifying the research problems, data collection was performed using primary and secondary data sources.

Primary data were obtained from direct observations, interviews, and technical inspection results of devices experiencing failures. These data included failure symptoms, affected components, operational conditions, and maintenance records. Secondary data were obtained from historical failure reports, maintenance documentation, technical inspection reports, and previous studies related to system reliability analysis.

The collected data were then analyzed using Fault Tree Analysis (FTA) and Failure Mode and Effect Analysis (FMEA) to identify the root causes and determine the priority level of each failure mode. The research flow is presented in Figure 1.

Fault Tree Analysis (FTA) Method

Fault Tree Analysis (FTA) is a deductive analytical method used to identify the root causes of system failures by describing the logical relationship between an undesired event (*top event*) and its contributing factors. This method analyzes failures by tracing the cause-and-effect relationship from the main failure event to the basic events that contribute to the occurrence of the failure.

In this study, FTA was applied to analyze the causes of connectivity disruptions in the Alarm Node-PR22 device. The analysis was performed by identifying the main failure events, including IC Power 3.3V failure, internal antenna failure, total device failure, and SIM800 module overheating. Through the FTA approach, each failure event was decomposed into several possible causes until the root causes were identified.

The results of the FTA analysis were subsequently used as input for identifying potential failure modes in the FMEA analysis.

Failure Mode and Effect Analysis (FMEA) Method

Failure Mode and Effect Analysis (FMEA) is a systematic risk analysis method used to identify potential failure modes, determine their causes and effects, and prioritize improvement actions. FMEA applies a *bottom-up approach* by evaluating each failure mode based on its impact on system performance.

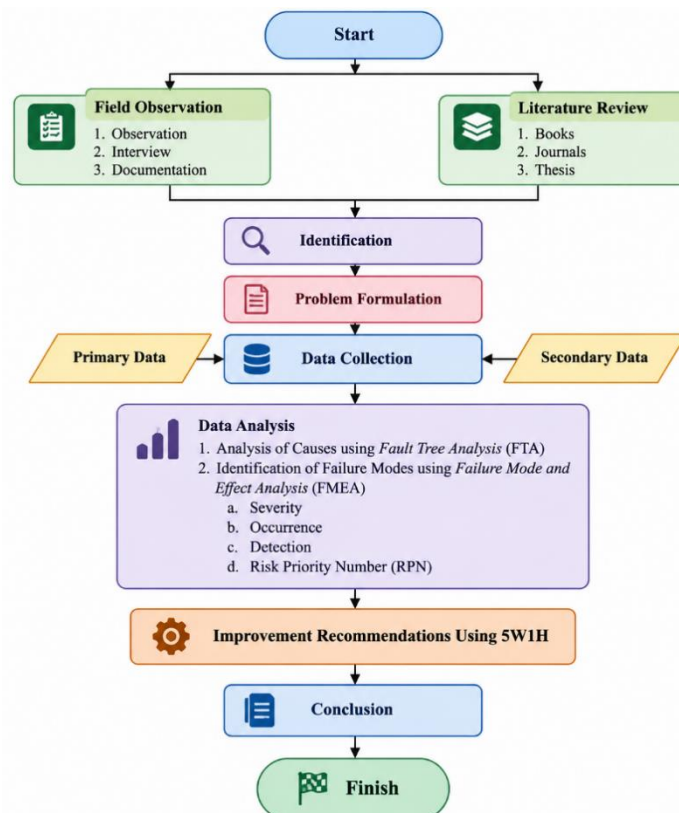
In this research, FMEA was used to assess the risk level of each failure mode identified from the FTA results. Each failure mode was evaluated based on three parameters:

1. Severity (S), representing the impact level of failure on device performance.
2. Occurrence (O), representing the frequency or probability of failure occurrence.
3. Detection (D), representing the ability to detect failure before affecting system operation.

The three parameters were calculated to obtain the **Risk Priority Number (RPN)** using the following equation:

$$RPN = S \times O \times D \dots \dots \dots (1)$$

The RPN value was then used to determine the priority ranking of failure modes. Failure modes with higher RPN values were considered to have higher risks and required priority improvement actions.



Flow chart Study

Figure 1. Research Flowchart

RESULTS AND DISCUSSION

Analysis of Disturbance Types Alarm Device Node-PR22

Data on Node-PR22 alarm problems from October 2024 to March 2025 served as the basis for the research analysis. Table 2 presents the types and number of problems that occurred during that period.

Table 2. Number of Types of 2G Modem Problems for the Period October 2024 – March 2025

Month	Amount Installed on ATM Machine	Types of Disturbance Constraints Connectivity Node-PR22 Device				Number of Constraints (Devices)	Constraint %
		3.3 V Power IC	Internal Antenna	Device Dead	SIM800		
October	100	5	3	2	1	11	11%
November	50	3	1	3	3	10	20%
December	30	3	1	1	2	7	23%
January	140	8	5	1	1	15	11%
February	120	6	2	3	1	12	10%
March	60	4	3	3	1	11	18%
Total	500	29	15	13	9	66	13%

Based on Table 2, there are 66 *devices* experiencing problems out of a total of 500 installed *devices*, with a percentage of problems of 13%. The most common type of problem is the 3.3 V *Power IC* with 29 *devices*, followed by 15 internal antennas, 13 dead *devices*, and 9 SIM800 *devices*. These data indicate that problems with the 3.3 V *Power IC* are the most dominant type of damage, so they need to be prioritized in analysis and repair actions.

1.1. Analysis Identifying the Main Causal Factors

The analysis was conducted to identify the main causal factors and risk levels of each disruption that occurred on the Node-PR22 device. The analysis was conducted using a combination of *Fault Tree Analysis* (FTA) and *Failure Analysis* (FTA) methods. *Mode and Effects Analysis* (FMEA) through the following stages.

To trace the causal relationship of connectivity disruptions on the Node-PR22 device, an analysis was performed using the *Fault Tree Analysis* (FTA) method. This method is used to identify the causative factors of failure down to the root cause. The FTA diagram of the 3.3V *Power IC* failure is shown in Figure 2.

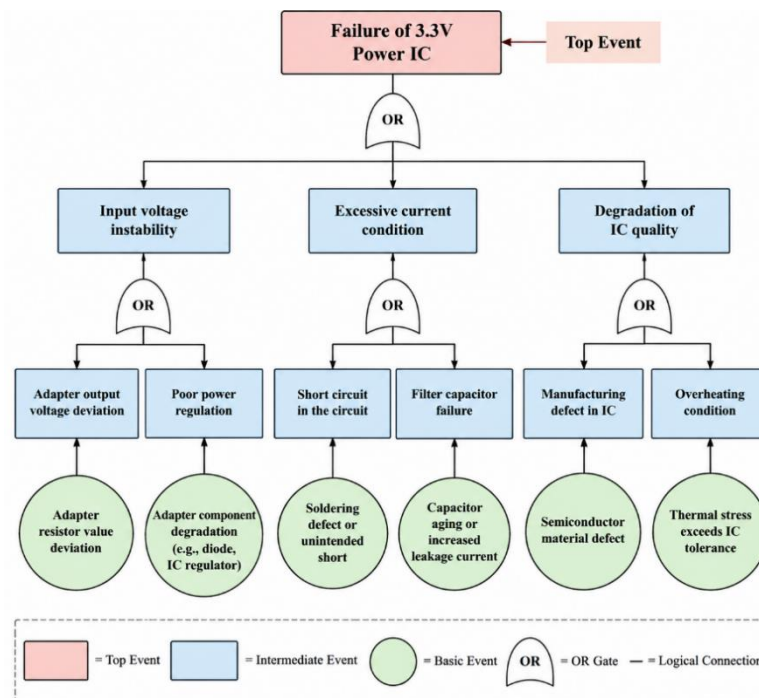


Figure 2. Fault Tree Analysis of 3.3V Power IC damage

The Fault Tree Analysis (FTA) results in Figure 2 show that the failure of the 3.3V Power IC is influenced by three main intermediate events, namely input voltage instability, excessive current conditions, and degradation of IC quality. These intermediate events are connected through an OR gate, indicating that the occurrence of one of these conditions can trigger failure of the 3.3V Power IC. The analysis further identifies several basic events that contribute to the failure mechanism, including adapter resistor value deviation, poor power regulation, short circuit conditions, filter capacitor degradation, semiconductor material defects, and thermal stress exceeding IC tolerance. Among these causes, semiconductor degradation and thermal-related stress represent critical factors because they can directly affect the internal structure and electrical performance of the IC. Therefore, the failure of the 3.3V Power IC is not only caused by a single component defect but results from the interaction between electrical instability, component degradation, and environmental operating conditions. The identified basic events from this FTA analysis are subsequently evaluated using FMEA to determine their risk priority based on severity, occurrence, and detection capability..

Furthermore, connectivity failure analysis was conducted on the internal antenna system, as presented in Figure 3. The FTA model identifies that the inability of the internal antenna to receive GSM signals is caused by three intermediate events: weak GSM signal conditions, antenna damage, and incorrect antenna positioning. These factors are connected using an OR gate, meaning that each condition has the potential to independently cause communication disruption. The basic events identified include radio wave obstruction caused by concrete walls, disconnected antenna cables, and antenna coverage by the device casing. These findings indicate that antenna performance is influenced not only by the physical condition of antenna components but also by installation conditions and the surrounding environment. Signal attenuation caused by obstacles and improper antenna placement can reduce communication quality, while physical damage to the antenna path can completely interrupt signal transmission. Therefore, improvement actions should consider both hardware inspection and optimization of device installation conditions..Next, the FTA diagram of the internal antenna is not able to reach the signal is shown in Figure 3.

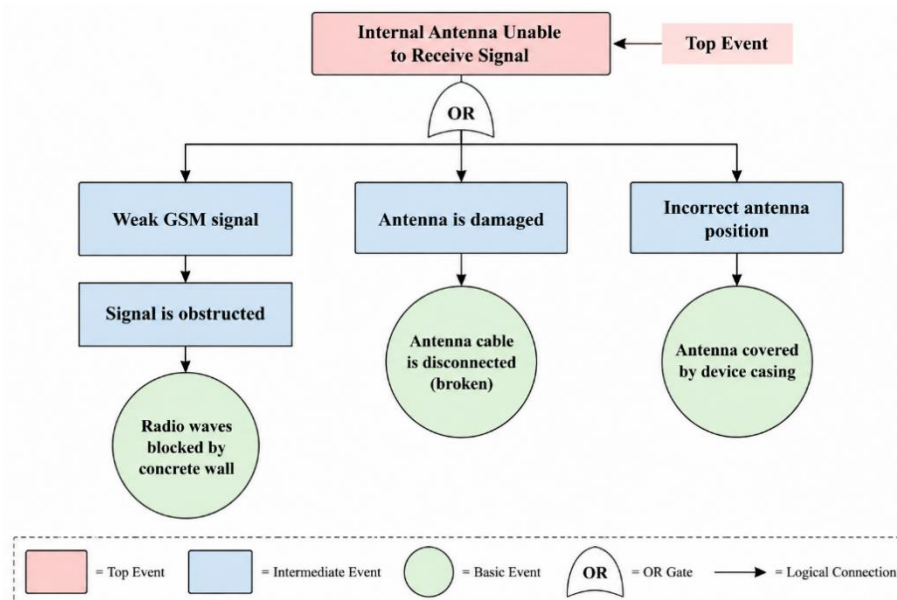


Figure 3. FTA Internal Antenna Not Capable of Reaching Signal

The next FTA analysis focuses on total device failure, where the Alarm Node-PR22 device becomes completely unable to operate, as shown in Figure 4. The analysis reveals three possible failure pathways: loss of incoming power, PCB short circuit, and damage to the main electronic components. These pathways are connected through an OR gate, indicating that each failure mechanism can independently result in total device shutdown. The basic events identified include physical damage to internal cable conductors, solder bridging between PCB tracks, and electrostatic discharge (ESD) exposure affecting sensitive components. The results demonstrate that total device failure is strongly associated with hardware reliability issues during assembly, maintenance

activities, and operational conditions. In particular, PCB short circuits caused by improper soldering processes represent a significant risk because they may directly interrupt electrical continuity and damage other connected components..Next , the FTA *device diagram* total death is shown in Figure 4.

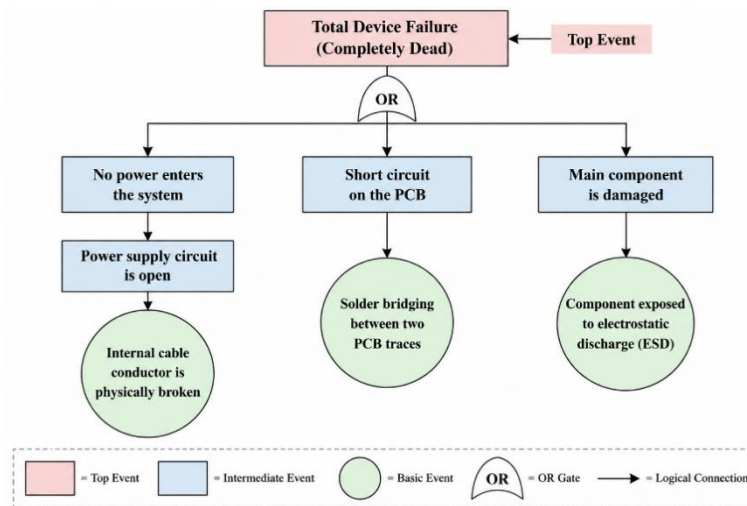


Figure 4. Fault Tree Analysis Device Totally Dead

The final FTA analysis evaluates overheating problems in the SIM800 communication module, as illustrated in Figure 5. The analysis identifies three intermediate events contributing to excessive temperature increase, namely excessive module workload, poor heat dissipation, and restricted cooling conditions. These events are connected through an OR gate, indicating that overheating may occur due to one or a combination of these conditions. The basic events include repeated signal retransmission caused by insufficient GSM signal strength, insufficient ventilation inside the device casing, and limited spacing between PCB components that restricts air circulation. The findings indicate that SIM800 overheating is related to both communication performance and thermal management design. Continuous retransmission increases module workload, while inadequate heat dissipation accelerates temperature accumulation inside the device. Therefore, reliability improvement requires not only communication optimization but also improvements in casing design and PCB thermal layout. Next , the Fault Tree Analysis Diagram of SIM800 Panas is shown in Figure 5.

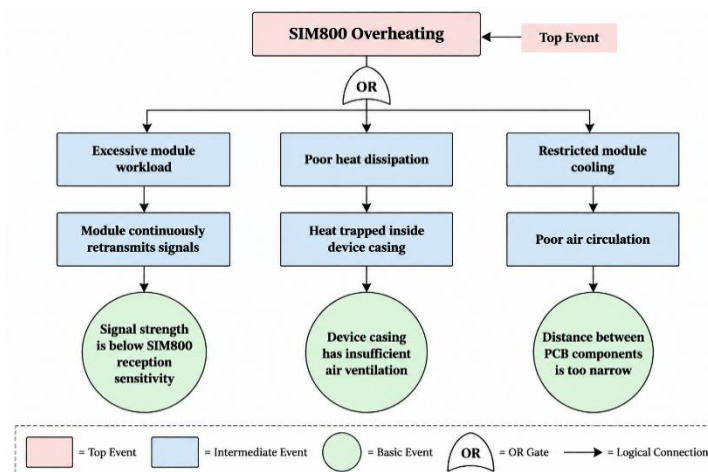


Figure 5. Fault Tree Analysis SIM800 Panas

Based on the overall FTA results, connectivity disruptions in the Alarm Node-PR22 device are caused by several interconnected failure mechanisms involving electrical components,

communication systems, hardware assembly, and thermal management aspects. The FTA approach successfully identifies the relationship between top events, intermediate events, and basic events, allowing the root causes of each failure mode to be systematically traced. The identified basic events from the FTA analysis are then used as input parameters in the FMEA method to evaluate the risk level and determine priority improvement actions. Through the integration of FTA and FMEA, the failure causes can be identified comprehensively, while the most critical risks can be prioritized based on their impact, occurrence frequency, and detection capability.

Risk Level Identification

Based on the results of the Fault Tree Analysis (FTA), the causal factors for each failure mode were identified. These factors were then used as the basis for the Failure Tree Analysis. Mode and Effects Analysis (FMEA) to determine the risk level and priority of improvement. FMEA assessment is carried out based on the levels of severity, occurrence, and detection to obtain a Risk Score. Priority Number (RPN). The RPN value is then used to prioritize each identified failure mode. The assessment results serve as the basis for determining which issues need to be prioritized for improvement. The results of the FMEA analysis are presented in Table 3.

Table 3 Analysis Failure Mode and Effects Analysis (FMEA)

No	Failure Mode Potential	Failure Effect	Failure Cause (Basic Event from FTA)	S	O	D	RPN
1	3.3V Power IC Failure	Power supply instability causing device malfunction and interruption of alarm transmission	Adapter resistor value deviation causing unstable voltage output	7	7	6	294
			Filter capacitor aging or increased leakage current causing loss of filtering capability	8	8	7	448
			Semiconductor material defect causing permanent IC silicon layer damage	9	9	8	648
			Total RPN of 3.3V Power IC Failure				1390
2	Internal Antenna Unable to Receive GSM Signal	Communication failure between Alarm Node-PR22 device and monitoring center	Radio waves blocked by concrete wall causing weak GSM signal	6	6	5	180
			Antenna cable disconnected/broken causing antenna signal path failure	8	8	8	512
			Antenna covered by device casing causing incorrect antenna positioning	5	7	6	210
			Total RPN of Internal Antenna Failure				902
3	Total Device Failure (Completely Dead)	Device cannot operate and alarm signal cannot be transmitted	Internal cable conductor physically broken causing open circuit	8	7	7	392
			Solder bridging between two PCB traces causing short circuit	9	9	8	648
			Component exposed to electrostatic discharge (ESD) causing component damage	8	6	6	288
			Total RPN of Total Device Failure				1328

No	Failure Mode Potential	Failure Effect	Failure Cause (Basic Event from FTA)	S	O	D	RPN
4	SIM800 Module Overheating	SIM800 malfunction, communication instability, and possible module failure	Continuous signal retransmission due to weak signal strength below SIM800 sensitivity	7	8	7	392
			Device casing has insufficient ventilation causing heat accumulation inside module	8	8	8	512
			Narrow distance between PCB components restricting air circulation	7	7	6	294
			Total RPN of SIM800 Overheating				1198

Power IC failure mode with a total RPN of 1,390, followed by a total dead device of 1,328, a hot SIM800 of 1,198, and an internal antenna unable to reach a signal of 902. These results indicate that the 3.3V Power IC failure is the main priority in repair actions because it has the highest risk level. In addition, the causes with the highest RPN values are the IC silicon layer experiencing permanent defects with a value of 648 and solder tin fused on two PCB tracks with a value of 648, so these two factors need to be given primary attention in efforts to improve the reliability of the Node-PR22 device.

Recommendation Repair

Based on results FMEA analysis, RPN value is used as base determination priority repair with consider factor causes that have been identified. The RPN value helps determine type necessary disturbance get attention more formerly based on level the resulting risks. Furthermore, the proposal repair arranged use 5W+1H analysis so that planned actions can done in a way more directed and systematic. Analysis the used For determine appropriate action based on type problems and factors causes that have been found through FTA and FMEA analysis. Recommendations improvements made covers action maintenance and changes design device in accordance with level risks found. Maintenance actions done as effort For guard condition components and prevent occurrence disturbance repeated, whereas change design done in the section device being assessed need improvement. Every action customized with conditions and needs Alarm Node-PR22 device so that expected can reduce potential disturbance connectivity and improve reliability device. Recommendations improvements that have been made arranged based on results analysis the presented in Table 4.

Table 4. Recommendations 5W+1H Repair

N o	What (What is the problem?)	Why (Why does it happen?)	Where (Where does it occur?)	When (When is the improvement implemented?)	Who (Who is responsible?)	How (How is the improvement performed?)
1	Adapter resistor value deviation causing 3.3V Power IC voltage instability	Resistor value changes due to component degradation, resulting in unstable voltage output supplied to the power IC	Adapter circuit / power supply section	During maintenance and component inspection	Maintenance Team	Replace the damaged adapter resistor with appropriate specifications and verify output voltage stability
2	Filter capacitor degradation	Capacitor aging or leakage	3.3V Power PCB circuit	During preventive maintenance	Maintenance Team	Replace the filter capacitor

N o	What (What is the problem?)	Why (Why does it happen?)	Where (Where does it occur?)	When (When is the improvement implemented?)	Who (Who is responsible?)	How (How is the improvement performed?)
	causing loss of filtering capability	current increase reduces the ability of the capacitor to stabilize voltage				according to electrical specifications and perform voltage ripple testing
3	Permanent damage of IC silicon layer causing 3.3V Power IC failure	Semiconductor material degradation or internal IC damage prevents the IC from operating normally	3.3V Power IC module on PCB	During device repair and failure replacement	Maintenance Team	Replace the damaged 3.3V Power IC and perform functional testing after replacement
4	GSM signal attenuation due to environmental obstruction	Concrete walls or physical obstacles weaken radio wave transmission and reduce signal quality	Device installation area	During signal disturbance occurrence	Technician	Relocate the device to an area with stronger GSM signal quality or optimize installation position
5	Internal antenna signal path failure	Antenna cable disconnection or damage interrupts signal transmission between antenna and communication module	Internal antenna connection path / PCB antenna track	During maintenance inspection	Maintenance Team	Repair the antenna connection by resoldering or replace damaged antenna cable/track
6	Internal antenna position is not optimal	Antenna placement is obstructed by device casing, reducing signal reception performance	Device internal antenna section	During maintenance and device assembly evaluation	Technician	Reposition the antenna to achieve optimal signal reception and avoid physical obstruction
7	Internal cable conductor physically broken	Mechanical stress or aging causes physical separation of cable conductor	Device internal cable connection	During maintenance inspection	Technician	Replace damaged cable and ensure proper cable installation to prevent repeated failure
8	PCB short circuit caused	Improper soldering	PCB board assembly area	During inspection and	Maintenance Team	Remove excessive

N _o	What (What is the problem?)	Why (Why does it happen?)	Where (Where does it occur?)	When (When is the improvement implemented?)	Who (Who is responsible?)	How (How is the improvement performed?)
9	by solder bridging between PCB tracks Main component failure due to electrostatic discharge (ESD)	process creates unwanted electrical connection between two PCB traces Static electricity exposure damages sensitive electronic components	PCB component area	maintenance process During assembly, inspection, and maintenance activities	Development Division and Maintenance Team	solder, clean PCB surface, and perform soldering according to standard procedure Implement anti-static protection equipment and apply ESD handling procedures
10	SIM800 communication instability due to insufficient signal strength	Weak GSM network causes repeated signal retransmission and increases module workload	SIM800 communication module	During connectivity disturbance	Technician	Improve device location, optimize antenna position, and ensure sufficient GSM signal availability
11	SIM800 overheating due to insufficient device ventilation	Heat generated by the module cannot dissipate properly because the casing has limited ventilation openings	Device casing / SIM800 module area	After design evaluation and improvement review	Development Division	Add ventilation openings or improve casing design to increase heat dissipation capability
12	Excessive PCB thermal accumulation due to limited component spacing	PCB layout with insufficient distance between components restricts airflow and increases heat concentration	PCB layout design	After engineering evaluation	Development Division	Redesign PCB layout by increasing component spacing and improving thermal management design

In addition to recommendations repair through maintenance, there are two points that require change design device, namely points 11 and 12. Changes the covering part physical and layout device, so that required design redesign as visualization proposed improvements. Changes to the section physique intended For increase circulation air and reduce risk improvement temperature on the device. Layout adjustment device done For increase neatness, facilitating the inspection process, and support activity maintenance in a way more effective. With change said device expected own condition more optimal and supportive operations improvement its reliability.

Based on the FMEA results, insufficient ventilation in the device casing was identified as one of the main causes contributing to SIM800 module overheating. The existing casing design has limited airflow, causing heat accumulation inside the device and reducing the reliability of electronic components during continuous operation. To overcome this problem, a casing redesign was proposed by adding ventilation openings to improve air circulation and enhance heat dissipation performance.

The proposed modification maintains the protective function of the casing while providing better thermal management for internal components. Improved airflow is expected to reduce heat accumulation, maintain the operating temperature of the SIM800 module, and minimize the risk of connectivity failure caused by overheating. The comparison between the existing casing design and the proposed redesign is presented in Figure 6 and Figure 7.

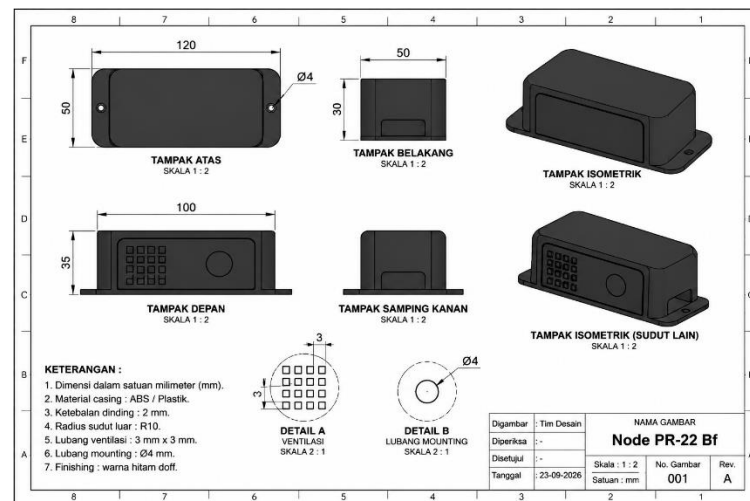


Figure 6. Before Casing

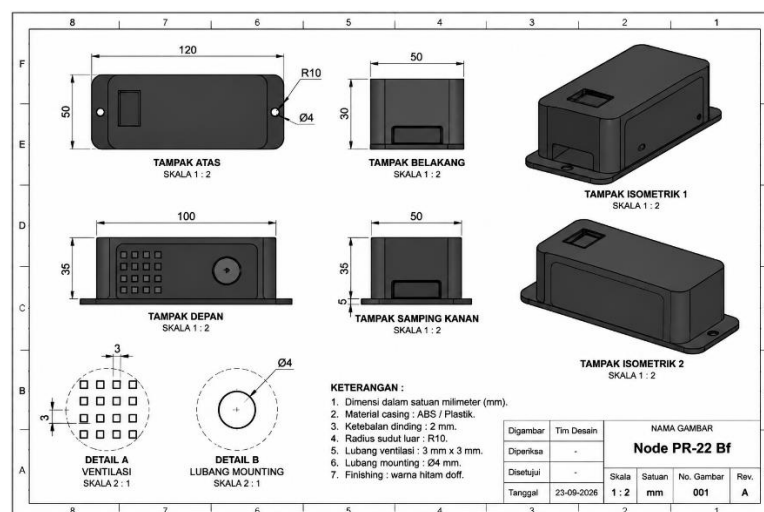


Figure 7. After Casing Design

Based on the FMEA analysis, one of the factors contributing to SIM800 module overheating is the limited distance between PCB components, which restricts airflow circulation and increases heat accumulation in the device. The existing PCB layout has a relatively dense component arrangement, causing heat generated by electronic components to accumulate in certain areas and reducing the effectiveness of thermal dissipation. This condition may affect component performance and decrease the long-term reliability of the Alarm Node-PR22 device.

To overcome this problem, a PCB layout redesign was proposed by adjusting the position and spacing between components to improve thermal distribution and airflow circulation. The redesign

focuses on optimizing component placement while maintaining electrical connections and device functionality. By providing sufficient spacing between components, heat transfer can be improved, making the operating temperature more stable and reducing the risk of thermal-related failures. The comparison between the existing PCB layout and the proposed redesign is presented in Figure 8 and Figure 9.

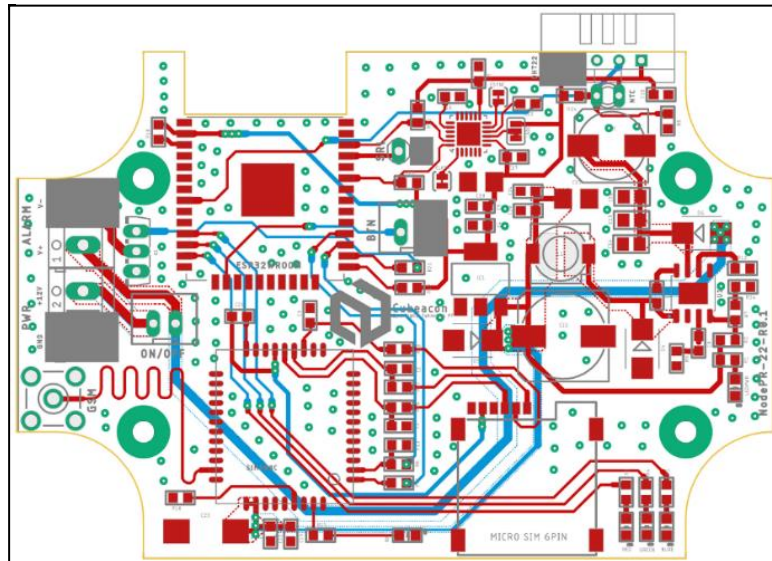


Figure 8. Before designing the PCB layout

Next, the PCB layout *redesign design with the addition of air vents* is shown in Figure 9 .

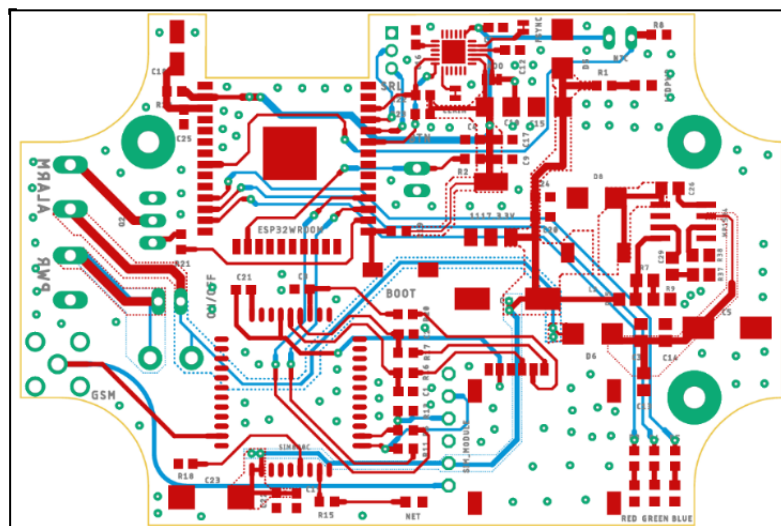


Figure 9. Layout Redesign Plan PCB location

The redesigned PCB layout improves the arrangement and spacing of electronic components, allowing better airflow circulation and reducing heat accumulation in critical areas. This modification is expected to improve thermal performance, simplify maintenance activities, and increase the reliability of the Alarm Node-PR22 device during continuous operation.

CONCLUSION

Based on the analysis of connectivity disruptions in the Alarm Node-PR22 device at PT Eyro Digital Teknologi using Fault Tree Analysis (FTA) and Failure Mode and Effect Analysis (FMEA), 66 devices out of 500 installed units experienced failures during October 2024–March 2025, with a

failure rate of 13%. The dominant failure was the 3.3V Power IC failure, accounting for 29 devices (44%), followed by internal antenna failure, total device failure, and SIM800 module overheating. The FTA results identified that connectivity disruptions were caused by several factors, including voltage instability, component degradation, antenna signal problems, PCB damage, ESD exposure, and insufficient thermal management. The FMEA results showed that the highest risk priority was the 3.3V Power IC failure with a total RPN value of 1390, followed by total device failure (1328), SIM800 overheating (1198), and internal antenna failure (902). The highest individual risk factors were permanent IC silicon layer damage and PCB short circuit caused by solder bridging, both with an RPN value of 648.

Based on the identified risks, improvement recommendations were developed through the 5W+1H approach, including component replacement, antenna and cable repair, implementation of ESD protection, casing redesign with additional ventilation, and PCB layout optimization. The integration of FTA and FMEA provides a systematic approach to identify root causes, prioritize failure risks, and determine effective corrective actions to improve device reliability. The proposed improvements are expected to reduce connectivity disruptions and enhance the operational performance of the Alarm Node-PR22 device as an IoT-based security monitoring system.

ACKNOWLEDGMENT

The authors would like to express their gratitude to the Department of Industrial Engineering, Universitas Pamulang, for providing academic support and research facilities during the implementation of this study. The authors also would like to thank PT Eyro Digital Teknologi for providing access, technical information, and operational data related to the Alarm Node-PR22 device used in this research. Appreciation is also extended to the maintenance team and related personnel who contributed through technical assistance, observations, and valuable insights during the data collection and analysis process..

REFERENCES

- Al-Turjman, F., & Al-Fagih, A. (2020). A survey on Internet of Things communication and networking technologies. *Future Generation Computer Systems*, 106, 1–14.
- Ali, S., Raza, M., & Khan, S. (2020). Energy-efficient communication in GSM-based IoT systems. *International Journal of Wireless Communications and Mobile Computing*, 8(1), 1–10.
- Alhamda, W. S., Noviyarsi, Y. M., Muchtiar, & Setiawati, L. (2023). Analysis of the causes of scattered ink in the notepad production process using Fault Tree Analysis (FTA) and Failure Mode and Effect Analysis (FMEA). *Journal of Industrial Engineering*, 9(1), 41–50.
- Ammar, M., Russello, G., & Crispo, B. (2021). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, 38, 8–27.
- Anwar, S., Ulum, R. B., & Widarman, A. (2023). Quality control analysis using FTA (Fault Tree Analysis) and FMEA (Failure Mode and Effect Analysis) methods in the production process of self-adhesive excise tape. *Multidisciplinary Scientific Journal*, 2(4), 114–128.
- Aulawi, H., Kurniawan, W. A., & Sopian, S. (2022). Failure risk analysis of production process using FTA, FMEA, and AHP methods. *Calibration Journal*, 20(2), 102–112.
- Ferrag, M. A., Shu, L., Yang, X., Derhab, A., & Maglaras, L. (2020). Security and privacy for IoT systems: Challenges and solutions. *IEEE Access*, 8, 70697–70716.
- Hanif, R. Y., Rukmi, H. S., & Susanty, S. (2021). Improving product quality using Failure Mode and Effect Analysis (FMEA) and Fault Tree Analysis (FTA). *Reka Integra*, 3(3), 1–10.
- Hendra, F., Mohammad, R., Amrin, A., Maarop, N., & Zagloel, T. Y. (2024). Systematic literature review of risk assessment techniques, standard and guidelines for railway. *International Journal of Technology*, 15(4), 1148-1161.
- Hendra, F., Mohammad, R., & Amrin, A. (2021). The Risk Priority Number (RPN) At A Level Crossings Along The Railway Line In Indonesia. In *The 2nd International Professional Doctorate and Postgraduate Symposium Universiti Teknologi Malaysia*, 25th September 2021 (p. 170).
- Kabir, S. (2021). An overview of Fault Tree Analysis and its application in risk assessment. *International Journal of Reliability, Quality and Safety Engineering*, 28(1), 2150005.

- Liu, H. C., Liu, L., & Liu, N. (2020). Risk evaluation approaches in Failure Mode and Effects Analysis with extended methods: A review. *Journal of Loss Prevention in the Process Industries*, 63, 104030.
- Mekki, K., Bajic, E., Chaxel, F., & Meyer, F. (2019). A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express*, 5(1), 1–7.
- Muhdor, H., Abdillah, H., & Sidik, M. (2023). Analysis of lathe machine maintenance with Fault Tree Analysis (FTA) and Failure Mode and Effect Analysis (FMEA). *Journal of Vocational Education and Automotive Technology*, 5(2), 174–183.
- Nabila, B. N., Dahda, S. S., & Priyana, E. D. (2025). Application of Failure Mode and Effect Analysis (FMEA) and Fault Tree Analysis (FTA) on production machines for reliability improvement. *Journal of Applied Industrial Technology and Management*, 4(4), 1613–1623.
- Nayoga, T. G., & Mukhtar, M. N. A. (2024). Defect analysis of laminated door products using Failure Mode and Effect Analysis (FMEA) and Fault Tree Analysis (FTA) methods. *PROFISIENSI: Journal of Industrial Engineering Study Program*, 12(2), 114–127.
- Nur, M., & Aulia, Y. P. (2024). Integration of FMEA and FTA methods in workplace accident risk mitigation strategy. *Journal of Applied Industrial Technology and Management*, 3(4), 393–404.
- Putra, A. R., & Rahman, F. (2020). Analysis of network connectivity and latency in Internet of Things (IoT) systems. *Journal of Information Technology and Computer Science*, 7(4), 705–714.
- Ridwan, W., Widiastuti, R., & Nurhayati, E. (2023). Analysis of oil palm seed quality control using Fault Tree Analysis (FTA) and Failure Mode Effect Analysis (FMEA). *Journal of Industrial Engineering*, 9(1), 24–30.
- Ruspendi, R., Rusmalah, R., Hendra, F., & Effendi, R. (2025). Mitigating operational risks and enhancing machine performance through total productive maintenance and OEE: a case study on packaging equipment. *Jurnal Polimesin*, 23(5), 684–689.
- Santoso, H., & Wibowo, A. (2020). Implementation of Internet of Things system for MQTT-based environmental monitoring. *Journal of Information and Computer Technology*, 8(2), 95–102.
- Sari, D. P., Fitria, L., & Hadi, A. (2022). Study of 2G network usage in industrial IoT systems in Indonesia. *Journal of Computer Technology and Systems*, 10(3), 181–188.
- Sethi, P., & Sarangi, S. R. (2021). Internet of Things: Architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*, 2021, 1–25.
- Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2021). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 181, 107538.
- Xu, L. D., He, W., & Li, S. (2021). Internet of Things in industries: A survey. *IEEE Transactions on Industrial Informatics*, 17(6), 3834–3843.
- Zio, E. (2021). Reliability engineering: Challenges and opportunities in the digital era. *Reliability Engineering & System Safety*, 211, 107583.