Jurnal Rekayasa Industri (JRI), Vol. 8 No. 2 April 2026
p-ISSN: 2714-8882 / e-ISSN: 2714-8874

An FMEA-Based Framework for Operational Technology Security Risk Prioritization in Manufacturing

AA. Nugraha*,
Master of Mechanical Engineering, Swiss German University, German
Tangerang, Indonesia
Email: arya.nugraha@student.sgu.ac.id

* *Corresponding Author*

Article Submit: 9-9-2026 Article Revision: 10-10-2026 Article Accepted: 29-10-2026

ABSTRACT

The increasing convergence of Information Technology (IT) and Operational Technology (OT) in manufacturing has introduced cybersecurity risks that threaten production reliability, operational continuity, and safety. However, conventional cybersecurity assessments often emphasize technical vulnerabilities without adequately considering their operational consequences. This study developed a Failure Mode and Effects Analysis (FMEA)-based framework integrating OT asset identification, cyber threat scenarios, failure modes, and operational impacts. Seven representative OT asset categories were evaluated using Severity (S), Occurrence (O), and Detection (D) criteria to calculate Risk Priority Numbers (RPNs) and establish risk-treatment priorities. The scenario-based assessment identified unauthorized Programmable Logic Controller (PLC) modification as the highest-priority risk (RPN = 420), followed by unauthorized remote access (RPN = 360), engineering workstation compromise (RPN = 324), and industrial network disruption (RPN = 324). A severity-based review mechanism was incorporated to address the limitations of conventional RPN prioritization. The proposed framework demonstrates how cyber-induced failure modes can be systematically translated into manufacturing-oriented risk priorities. By integrating cybersecurity considerations with industrial risk engineering, the framework provides a structured decision-support approach for prioritizing security controls and supporting production reliability, operational resilience, and risk-informed manufacturing management.

Keywords: Cybersecurity; Failure Mode and Effects Analysis; Manufacturing; Operational Technology; Risk Prioritization; Risk Priority Number.

I. INTRODUCTION

The rapid advancement of Industry 4.0 has transformed manufacturing systems from relatively isolated production environments into highly interconnected cyber-physical ecosystems. Technologies such as industrial Internet of Things (IIoT), smart sensors, programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA) systems, human–machine interfaces (HMIs), industrial networks, and cloud-connected manufacturing platforms increasingly enable real-time monitoring, automation, predictive maintenance, and data-driven decision-making. While this transformation improves productivity, flexibility, and operational visibility, the convergence of Information Technology (IT) and Operational Technology (OT) also expands the attack surface of manufacturing environments. Recent research emphasizes that the transition toward interconnected Industry 4.0 architectures has altered the cybersecurity risk landscape of OT systems, which historically relied heavily on physical or logical isolation from external networks (Halawi Ghoson et al., 2025).

Unlike conventional IT environments, OT systems directly interact with physical processes. Consequently, cybersecurity incidents affecting OT assets may extend beyond information loss or service interruption and produce physical and operational consequences, including production downtime, equipment malfunction, process instability, product-quality degradation, safety hazards, and cascading failures across interconnected manufacturing processes. This distinction is particularly important from an industrial engineering perspective because OT cybersecurity risk is inherently associated with the reliability, availability, safety, and continuity of production systems. Contemporary research on industrial control systems further demonstrates the growing convergence between cybersecurity and process safety, emphasizing that cyberattack scenarios must be assessed according to their potential effects on industrial operations rather than solely according to traditional information-security criteria (Da Silva et al., 2025).

DOI: https://doi.org/10.37631/jri.v8i2.2497
Hak Cipta © 2026, Nugraha, Arya Adhi
This is an open-access article under the CC BY-NC License.

Accordingly, cybersecurity risk assessment has become an essential component of manufacturing resilience. Existing approaches to OT cybersecurity commonly employ risk matrices, vulnerability assessment, attack modeling, probabilistic methods, cybersecurity standards, and combinations of qualitative and quantitative techniques. A recent review of OT cybersecurity risk-assessment methods in Industry 4.0 distinguishes between static and dynamic approaches and highlights continuing challenges in representing the evolving and interconnected nature of industrial cyber risk (Halawi Ghoson et al., 2025). Other studies have proposed specialized approaches for assessing particular OT infrastructures, including risk-weighted assessments aligned with established industrial cybersecurity frameworks (Abergos & Medjek, 2024). These developments demonstrate substantial progress in identifying and analyzing cyber threats; however, translating cybersecurity assessment results into actionable priorities for manufacturing decision-makers remains a significant challenge.

This challenge is especially relevant because manufacturing organizations typically operate heterogeneous OT environments comprising legacy equipment, modern connected devices, industrial communication networks, engineering workstations, control systems, and increasingly integrated IT/OT infrastructures. Cybersecurity resources are nevertheless finite. Organizations therefore cannot address every vulnerability, threat scenario, and affected asset simultaneously. Effective OT cybersecurity management requires a structured mechanism for determining which cyber-induced failure scenarios should receive priority based on their potential operational consequences, likelihood of occurrence, and ability to be detected before significant disruption occurs. In this context, risk prioritization, rather than risk identification alone, becomes a critical managerial capability for allocating security resources and maintaining manufacturing continuity.

Failure Mode and Effects Analysis (FMEA) provides a potentially valuable methodological foundation for addressing this problem. FMEA is a systematic risk-analysis technique extensively applied in manufacturing, reliability engineering, quality management, maintenance, and process improvement. The conventional method identifies potential failure modes, evaluates their consequences and causes, and assigns ratings for Severity (S), Occurrence (O), and Detection (D). These factors are commonly combined into a Risk Priority Number (RPN), expressed as \(RPN = S \times O \times D\), which enables failure modes to be ranked according to their relative criticality. The method is particularly attractive for industrial environments because it translates complex failure scenarios into a structured decision-support mechanism that is readily interpretable by engineers and operational managers.

Recent studies demonstrate the continued relevance of FMEA for increasingly complex manufacturing environments. For example, FMEA has been adapted to Industry 4.0 production systems to evaluate the reliability implications of conventional and digitally connected components, demonstrating its applicability to smart manufacturing environments (Salah et al., 2023). More sophisticated approaches have introduced data-driven risk factors and multi-criteria decision-making methods to overcome limitations associated with subjective expert assessments and conventional RPN calculations (Ervural & Ayaz, 2023; Kahouadji & Belkaid, 2025). Similarly, hybrid FMEA approaches have been developed to improve the prioritization of risks in complex manufacturing environments where conventional scoring mechanisms may inadequately represent uncertainty and differences in criterion importance.

The application of FMEA principles to cybersecurity has also begun to emerge. Previous research has modified FMEA for cybersecurity risk assessment in manufacturing by incorporating game-theoretic estimation of cyberattack likelihood, demonstrating that failure-oriented methods can be adapted to represent adversarial risks in cyber-physical manufacturing systems (Zarreh et al., 2019; Rahman et al., 2024; Suorsa & Helo, 2026). Beyond manufacturing, FMEA has been integrated with Bayesian networks for cybersecurity risk assessment in complex operational environments, illustrating its capacity to structure cyber threats as failure scenarios and quantitatively prioritize their associated risks (Park et al., 2023). More recent research into manufacturing equipment has likewise demonstrated the potential of failure-mode-based reasoning for analyzing cyber threats to computer numerical control systems, although increasingly sophisticated probabilistic models are being proposed to address uncertainty in expert assessment (Zhang et al., 2026).

Despite these developments, an important research gap remains. Existing OT cybersecurity studies predominantly emphasize threat identification, vulnerability analysis, attack modeling, or cybersecurity controls, while manufacturing-oriented FMEA studies primarily address equipment failures, process disruptions, quality problems, and conventional operational risks. The intersection between these streams remains comparatively underdeveloped: cyber threats to OT assets are not yet consistently conceptualized as potential failure modes whose effects can be evaluated in terms of manufacturing consequences and subsequently translated into operational risk priorities. Moreover, increasingly sophisticated cybersecurity risk models may require substantial data, probabilistic assumptions, or specialized expertise, potentially limiting

DOI: https://doi.org/10.37631/jri.v8i2.2497
Hak Cipta © 2026, Nugraha, Arya Adhi
This is an open-access article under the CC BY-NC License.

their practical adoption by manufacturing organizations seeking an interpretable initial risk-prioritization mechanism. Recent literature continues to identify risk-informed decision-making and cyber-risk quantification as important areas for advancing resilient manufacturing systems.

This study addresses this gap by proposing an FMEA-based framework for Operational Technology security risk prioritization in manufacturing. Rather than treating cybersecurity risk exclusively as an information-security problem, the proposed approach conceptualizes cyber threat scenarios as potential failure modes within manufacturing OT systems. The framework connects OT assets, cyber threat scenarios, vulnerabilities or failure causes, operational effects, existing detection mechanisms, and risk-treatment priorities through the conventional FMEA dimensions of severity, occurrence, and detection. In this manner, cybersecurity risks can be translated into a risk language that is familiar to manufacturing, reliability, maintenance, and industrial engineering practitioners.

The novelty of this study therefore lies not merely in applying FMEA to cybersecurity, but in reframing OT cybersecurity risk prioritization as a manufacturing risk-engineering problem. The proposed framework establishes an explicit analytical linkage between cyber events and their consequences for production operations, enabling cybersecurity decisions to be prioritized according to operational criticality. This perspective is intended to bridge the disciplinary gap between cybersecurity risk management and traditional manufacturing risk analysis while preserving the simplicity and managerial interpretability of conventional FMEA. At the same time, the study recognizes established limitations of conventional RPN-based prioritization—including subjectivity in scoring and the possibility that different combinations of severity, occurrence, and detection generate identical RPN values (Ervural & Ayaz, 2023). Accordingly, the framework is positioned as a transparent and practical baseline for OT security prioritization rather than as a replacement for advanced probabilistic or dynamic cyber-risk models.

Based on this research gap, the study addresses three research questions: (RQ1) How can OT cybersecurity threats in manufacturing systems be systematically represented as failure modes using an FMEA-based approach? (RQ2) How can severity, occurrence, and detection criteria be operationalized to prioritize cyber-induced risks according to their potential effects on manufacturing operations? (RQ3) How can the resulting risk priorities be translated into a structured decision-support framework for OT cybersecurity risk treatment? Accordingly, the objective of this study is to develop an FMEA-based OT security risk prioritization framework that systematically identifies cyber-related failure scenarios, evaluates their potential operational consequences, calculates their relative risk priorities, and supports manufacturing organizations in determining appropriate risk-treatment priorities.

The study contributes theoretically by extending failure-oriented risk analysis into the domain of OT cybersecurity and positioning cyber risk within the broader context of manufacturing reliability and operational resilience. From a practical perspective, the proposed framework is expected to provide manufacturing organizations with a structured and interpretable mechanism for integrating cybersecurity considerations into existing risk-management, maintenance, reliability, and operational decision-making processes. In doing so, the framework seeks to support a transition from vulnerability-centered cybersecurity assessment toward risk-informed OT security management based on the potential consequences of cyber threats to manufacturing operations.

II. METHOD

2.1 Research Design

This study employed a design-oriented risk assessment approach to develop an FMEA-based framework for prioritizing Operational Technology (OT) security risks in manufacturing environments. The research was designed to bridge conventional manufacturing risk analysis and OT cybersecurity by translating cyber threat scenarios into failure modes that can be evaluated according to their potential operational consequences. Rather than developing a probabilistic cyber-risk model, the study focused on constructing a transparent and practically applicable decision-support framework that can be integrated into existing manufacturing risk-management practices.

The methodological process consisted of five sequential stages: (1) OT system characterization and asset identification; (2) cyber threat and failure-mode identification; (3) FMEA criteria development; (4) risk evaluation and prioritization using the Risk Priority Number (RPN); and (5) development of risk-treatment priorities and the proposed OT security risk prioritization framework. Figure 1 presents the overall research procedure.

DOI: https://doi.org/10.37631/jri.v8i2.2497
Hak Cipta © 2026, Nugraha, Arya Adhi
This is an open-access article under the CC BY-NC License.

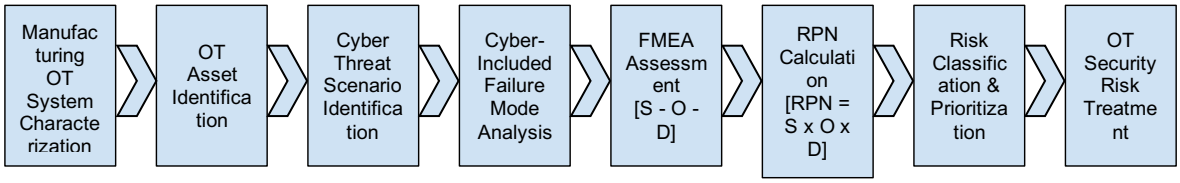


Figure 1. Research Methodological Framework

This sequence was designed to maintain traceability from an OT asset and its associated cyber threat to the resulting operational consequence and recommended treatment priority.

2.2 OT System and Asset Characterization

The unit of analysis was the OT environment of a representative manufacturing production system. The study focused on OT assets that directly support or influence production processes, including programmable logic controllers (PLCs), human–machine interfaces (HMIs), supervisory control and data acquisition (SCADA) components, engineering workstations, industrial communication networks, historians, and other supporting OT infrastructure.

Asset identification was conducted according to the functional role of each component within the production system rather than solely according to its technological characteristics. Each asset was characterized based on four attributes: asset function, operational dependency, connectivity, and potential consequence of compromise. This characterization was necessary because the criticality of an OT asset cannot be adequately determined from its cybersecurity properties alone; it must also reflect its contribution to production continuity, process control, equipment operation, product quality, and safety. The asset characterization stage produced an OT asset inventory that served as the analytical foundation for subsequent threat and failure-mode identification.

2.3 Cyber Threat Scenario and Failure-Mode Identification

Following asset identification, potential cyber threat scenarios were mapped to the identified OT assets. Threat scenarios considered common attack mechanisms relevant to industrial environments, including unauthorized access, malware infection, credential compromise, denial-of-service conditions, unauthorized configuration or logic modification, manipulation of process information, network communication disruption, and compromise of engineering or operator interfaces.

For the purpose of FMEA, a distinction was established between a cyber threat scenario and a failure mode. A cyber threat scenario represents the mechanism or event through which an OT asset may be compromised, whereas a failure mode represents the resulting undesirable condition of the asset or production process. For example, unauthorized modification of PLC logic represents a cyber threat scenario, while incorrect execution of process-control logic constitutes the corresponding failure mode. The effect may subsequently include production interruption, equipment damage, quality deviation, or unsafe process conditions. Accordingly, each risk scenario was structured using the following analytical chain:

$$OT\ Asset \rightarrow Cyber\ Threat \rightarrow Failure\ Mode \rightarrow Operational\ Effect \quad (1)$$

This structure extends conventional FMEA reasoning by explicitly incorporating cybersecurity threats as potential causes of manufacturing system failures.

2.4 FMEA-Based Risk Assessment

Each identified cyber-induced failure mode was evaluated using the three conventional FMEA dimensions: Severity (S), Occurrence (O), and Detection (D). A ten-point ordinal scale was adopted for each dimension, where higher values represent greater risk. Severity (S) measures the magnitude of the potential operational consequences if a cyber-induced failure occurs. The assessment emphasizes manufacturing consequences rather than only information-security impact. The criteria include effects on production continuity, equipment, product quality, safety, and recovery requirements. Occurrence (O) represents the relative likelihood that the identified cyber-induced failure scenario may occur. The assessment considers factors such as asset exposure, connectivity, known vulnerabilities, threat applicability, access pathways, and the presence or absence of preventive security controls.Detection (D) represents the likelihood that the cyber-induced failure or its initiating condition will remain undetected before producing a significant operational consequence. Consistent with conventional FMEA logic, a higher detection score indicates lower detectability and therefore greater risk. Detection considerations include security monitoring, network visibility, logging, anomaly detection, alerting capability, and operational monitoring mechanisms. To improve reproducibility and reduce ambiguity in assigning scores, the study established operational definitions for the three dimensions, as summarized in Table 1.

DOI: https://doi.org/10.37631/jri.v8i2.2497
Hak Cipta © 2026, Nugraha, Arya Adhi
This is an open-access article under the CC BY-NC License.

Table 1. FMEA Rating Criteria for OT Security Risk Assessment

Score	Severity (S)	Occurrence (O)	Detection (D)
1–2	Negligible operational effect; no meaningful production disruption	Rare; highly restricted exposure and effective preventive controls	Very high probability of early detection
3–4	Minor disruption with localized operational impact	Unlikely; limited exposure with generally effective controls	High probability of detection through existing controls
5–6	Moderate production degradation or temporary process interruption	Possible; credible attack pathway or moderate control weakness	Moderate detection capability
7–8	Major production interruption, significant quality or equipment impact	Likely; exposed attack pathway and substantial control weakness	Low probability of timely detection
9–10	Critical production shutdown, major equipment damage, or serious safety consequences	Highly likely under relevant threat conditions or critically exposed environment	Very low probability of detection before significant operational impact

The detailed assessment retained individual scores from 1 to 10, while the ranges shown in Table 1 provide interpretive anchors to improve consistency in risk evaluation. The application of FMEA in manufacturing risk assessment has been demonstrated in studies addressing equipment reliability, operational failures, and maintenance prioritization. For instance, Yuda and Al-Faritsy (2026) integrated FMEA with reliability-centered maintenance to identify critical equipment failures and establish maintenance interventions aimed at reducing production downtime. Similarly, Asdi et al. (2025) applied FMEA to prioritize operational risks and formulate mitigation strategies. These studies provide methodological support for adapting failure-oriented risk assessment to OT cybersecurity scenarios in manufacturing environments.

2.5 Risk Priority Number and Risk Classification

The relative priority of each failure mode was determined using the conventional Risk Priority Number (RPN). The RPN was calculated as the product of severity, occurrence, and detection:

$$RPN = S \times O \times D \tag{2}$$

Where S represents severity, O represents occurrence, and D represents detection. Because each dimension ranges from 1 to 10, the resulting RPN ranges from 1 to 1,000. The calculated RPN values were used primarily as a relative prioritization mechanism rather than an absolute measure of cybersecurity risk. Failure modes with higher RPN values were considered to require greater management attention and more immediate consideration for risk treatment. For practical interpretation, the resulting RPN values were grouped into four priority categories, as presented in Table 2.

Table 2. Proposed RPN-Based OT Security Risk Priority Classification

RPN	Priority Level	Management Response
1–100	Low	Maintain existing controls and periodically monitor

DOI: https://doi.org/10.37631/jri.v8i2.2497
Hak Cipta © 2026, Nugraha, Arya Adhi
This is an open-access article under the CC BY-NC License.

101–250	Moderate	Evaluate additional controls and monitor risk development
251–500	High	Develop and implement prioritized risk-treatment measures
501–1,000	Critical	Immediate management attention and risk treatment required

The thresholds were used as decision-support bands developed for the proposed framework, rather than universal FMEA thresholds. Organizations adopting the framework may adjust these boundaries according to their risk appetite, production criticality, regulatory requirements, and operational context. In addition, the interpretation of RPN was not performed mechanically. Failure modes receiving very high severity scores were separately flagged for management review even when their overall RPN did not fall within the highest category. This safeguard was introduced to reduce the possibility that a potentially catastrophic but relatively low-occurrence scenario would receive insufficient attention because of the multiplicative structure of conventional RPN.

2.6 OT Security Risk Register and Prioritization Framework

The results of the FMEA assessment were consolidated into an OT Security FMEA Register. The register was designed to maintain traceability between manufacturing assets, cybersecurity threats, operational failures, risk scores, and treatment decisions. Each record contained the following attributes:

$$OT\ Asset \rightarrow Asset\ Function \rightarrow Cyber\ Threat\ Scenario \rightarrow Failure\ Mode \rightarrow Operational\ Effect \rightarrow S \rightarrow O \rightarrow D \rightarrow RPN \rightarrow Priority\ Level \rightarrow Recommended\ Treatment \quad (3)$$

Risk-treatment recommendations were subsequently formulated according to the characteristics of each prioritized failure mode. Treatment measures were classified into preventive, detective, and recovery controls, allowing the proposed framework to connect FMEA results directly with cybersecurity and operational resilience decisions. The resulting framework therefore operates at three analytical levels: asset level, which determines what manufacturing resources require protection; failure-mode level, which determines how cyber threats may disrupt production; and decision level, which determines which risks should receive treatment priority.

2.7 Analytical Procedure

The complete analytical procedure was conducted through the following stages:

1. Identify OT assets and their functions within the manufacturing production system.
2. Determine relevant cyber threat scenarios for each OT asset.
3. Translate cyber threat scenarios into potential cyber-induced failure modes.
4. Determine the operational effects associated with each failure mode.
5. Assign Severity, Occurrence, and Detection scores using the predefined assessment criteria.
6. Calculate the RPN for each identified failure mode.
7. Rank the failure modes according to their RPN values while separately reviewing high-severity scenarios.
8. Classify risks into low, moderate, high, and critical priority levels.
9. Determine appropriate preventive, detective, and recovery treatments.
10. Consolidate the analytical relationships into the proposed FMEA-based OT security risk prioritization framework.

This procedure enables the assessment to be replicated for different manufacturing systems by modifying the asset inventory, threat scenarios, operational context, and organizational risk criteria while retaining the underlying analytical structure.

2.8 Methodological Validity and Limitations

Several measures were incorporated to strengthen methodological consistency. First, explicit operational definitions were established for severity, occurrence, and detection to reduce inconsistent interpretation of FMEA scores. Second, each assessment maintained traceability between the OT asset, threat scenario, failure mode, and operational effect. Third, RPN values were interpreted as relative decision-support indicators, acknowledging that conventional FMEA scoring does not constitute a probabilistic estimate of cyber risk.

DOI: https://doi.org/10.37631/jri.v8i2.2497
Hak Cipta © 2026, Nugraha, Arya Adhi
This is an open-access article under the CC BY-NC License.

The study also recognizes inherent limitations of conventional FMEA. The multiplication of three ordinal ratings may produce identical RPN values for failure modes with substantially different risk characteristics, while the equal mathematical weighting of severity, occurrence, and detection may not accurately represent organizational priorities. Furthermore, expert-based scoring can introduce subjectivity into the assessment process. These limitations were partially addressed by retaining the individual S, O, and D scores alongside the RPN and requiring separate review of high-severity scenarios. Future extensions of the framework may incorporate multi-criteria decision-making, fuzzy logic, Bayesian methods, or empirical incident data to improve weighting and uncertainty representation.

As the study focused on the development and analytical application of a risk-prioritization framework and did not involve intervention on human participants, collection of personally identifiable information, or experimentation affecting individuals, formal human-subject ethical approval was not applicable. Nevertheless, where organizational OT information is used, asset configurations, vulnerabilities, and security-control details should be anonymized to prevent disclosure of security-sensitive information.

III. RESULT AND DISCUSSION

3.1 OT Cyber-Induced Failure Modes

The proposed framework was applied to seven representative OT asset categories: Programmable Logic Controller (PLC), Human–Machine Interface (HMI), engineering workstation, SCADA server, industrial network, historian server, and remote access infrastructure. Cyber threat scenarios were translated into operational failure modes using the relationship:

$$\text{OT Asset} \rightarrow \text{Cyber Threat} \rightarrow \text{Failure Mode} \rightarrow \text{Operational Effect} \quad (4)$$

This structure shifts the assessment from purely technical cybersecurity events toward their consequences for manufacturing operations.

Table 3. Identification of OT Cyber-Induced Failure Modes

No.	OT Asset	Cyber Threat Scenario	Potential Failure Mode	Primary Operational Effect
1	PLC	Unauthorized logic modification	Incorrect execution of control logic	Process deviation or production shutdown
2	HMI	Malware infection	Loss or manipulation of operator interface	Reduced process visibility and incorrect operator action
3	Engineering workstation	Credential compromise	Unauthorized modification of OT configuration	Process instability and unauthorized system changes
4	SCADA server	Denial-of-service attack	Loss of supervisory control and monitoring	Production interruption and reduced operational visibility
5	Industrial network	Network intrusion or communication disruption	Loss or manipulation of industrial communication	Control-system communication failure
6	Historian server	Process-data manipulation	Loss of integrity of historical process data	Incorrect operational and maintenance decisions
7	Remote access infrastructure	Unauthorized remote access	Unauthorized control or configuration of OT assets	Potential manipulation of production processes

The results indicate that OT cybersecurity risks should be interpreted according to the operational role of the affected asset. A cyber event affecting a PLC, for example, can propagate directly into physical process behavior, whereas historian compromise primarily affects the integrity of operational and maintenance

DOI: https://doi.org/10.37631/jri.v8i2.2497
Hak Cipta © 2026, Nugraha, Arya Adhi
This is an open-access article under the CC BY-NC License.

decisions. This supports the argument that vulnerability severity alone is insufficient for manufacturing-oriented cybersecurity prioritization.

3.2 FMEA-Based Risk Prioritization

Each failure mode was evaluated using Severity (S), Occurrence (O), and Detection (D), with the Risk Priority Number calculated as:

$$RPN = S \times O \times D \quad (5)$$

The resulting prioritization is presented in Table 4.

Table 4. Proposed RPN-Based OT Security Risk Priority Classification

Rank	OT Asset	Cyber-Induced Failure Mode	S	O	D	RPN	Priority
1	PLC	Unauthorized modification of control logic	10	6	7	420	High
2	Remote access infrastructure	Unauthorized remote control of OT assets	10	6	6	360	High
3	Engineering workstation	Unauthorized OT configuration changes	9	6	6	324	High
4	Industrial network	Disruption/manipulation of industrial communication	9	6	6	324	High
5	SCADA server	Loss of supervisory control and monitoring	9	5	6	270	High
6	HMI	Loss/manipulation of operator interface	8	5	6	240	Moderate
7	Historian server	Manipulation of historical process data	7	4	6	168	Moderate

Unauthorized PLC logic modification generated the highest RPN (420), followed by unauthorized remote access (360). Engineering workstation compromise and industrial network disruption produced identical RPN values (324). These results emphasize the criticality of assets that directly control physical processes, configure control systems, or provide connectivity between OT components.

However, RPN should be interpreted as a relative prioritization indicator rather than an absolute measurement of cybersecurity risk. Different combinations of S, O, and D can generate identical RPN values despite representing different risk characteristics. This limitation is particularly relevant in OT environments, where low-frequency events may still produce catastrophic physical or operational consequences. Therefore, the framework applies a severity override, requiring scenarios with Severity scores of 9–10 to receive explicit management review regardless of their overall RPN classification.

3.3 Risk Treatment and Proposed Framework

The proposed FMEA-based framework extends conventional cybersecurity risk assessment by systematically linking cyber-induced failure modes to risk-treatment decisions and manufacturing performance

DOI: https://doi.org/10.37631/jri.v8i2.2497
Hak Cipta © 2026, Nugraha, Arya Adhi
This is an open-access article under the CC BY-NC License.

objectives. The framework integrates three interconnected dimensions: risk identification, risk prioritization, and operational improvement. This integration enables manufacturing organizations to prioritize cybersecurity interventions according to their potential contribution to production reliability, equipment availability, and operational continuity.

Based on the FMEA assessment, risk-treatment strategies were developed by considering the individual Severity (S), Occurrence (O), and Detection (D) scores alongside the Risk Priority Number (RPN). Preventive measures were directed toward reducing the likelihood of cyber-induced failures, detective measures toward improving early threat identification, and recovery measures toward limiting disruption duration and restoring production capabilities. Table 5 presents the corresponding treatment strategies and their expected operational contributions.

Table 5. OT Security Risk Treatment Priorities

OT Asset	RPN	Preventive Priority	Detective Priority	Recovery/Resilience Priority
PLC	420	Access restriction, logic-change authorization, network segmentation	PLC configuration and logic-change monitoring	Validated configuration backup and controlled restoration
Remote access	360	Strong authentication, controlled remote access, least privilege	Remote-session monitoring and access logging	Rapid access revocation and recovery procedures
Engineering workstation	324	Privileged-access restriction, application control, system hardening	Configuration-change and endpoint monitoring	Secure engineering backup and workstation restoration
Industrial network	324	Segmentation, communication restrictions, secure architecture	Industrial network anomaly monitoring	Network redundancy and communication recovery
SCADA server	270	System hardening and access control	Service, event, and security monitoring	Backup, redundancy, and tested restoration
HMI	240	Endpoint hardening and access restrictions	HMI integrity and abnormal-behavior monitoring	Configuration restoration and alternative operating procedures
Historian server	168	Access control and data-integrity protection	Integrity and anomalous-data monitoring	Backup and validated data restoration

Risk-treatment priorities were determined using the FMEA assessment matrix, which integrates Severity (S), Occurrence (O), and Detection (D) into the Risk Priority Number (RPN = S × O × D). Based on the predefined risk classification criteria, scenarios with RPN values of 251–500 were categorized as high priority, requiring prioritized risk-treatment actions, while those with values of 101–250 were classified as moderate priority and subjected to planned control improvements and periodic monitoring. Accordingly, unauthorized PLC logic modification (RPN = 420) received the highest treatment priority, followed by unauthorized remote access (RPN = 360), engineering workstation compromise (RPN = 324), industrial network disruption (RPN = 324), and SCADA server disruption (RPN = 270). HMI compromise (RPN = 240) and historian data manipulation (RPN = 168) were assigned moderate priority. In addition to RPN-based ranking, failure modes with Severity scores of 9–10 were designated for explicit management review to prevent potentially catastrophic operational consequences from being underestimated. Preventive controls were prioritized to reduce Occurrence, while detective controls were intended to improve threat detectability and consequently reduce Detection scores. Recovery measures were directed toward limiting production disruption and

DOI: https://doi.org/10.37631/jri.v8i2.2497
Hak Cipta © 2026, Nugraha, Arya Adhi
This is an open-access article under the CC BY-NC License.

strengthening operational resilience. Following control implementation, the individual FMEA scores and residual RPN should be reassessed to evaluate changes in risk exposure and determine whether further treatment is necessary. Based on these relationships, the proposed framework consists of five integrated stages, as illustrated in Figure 2.

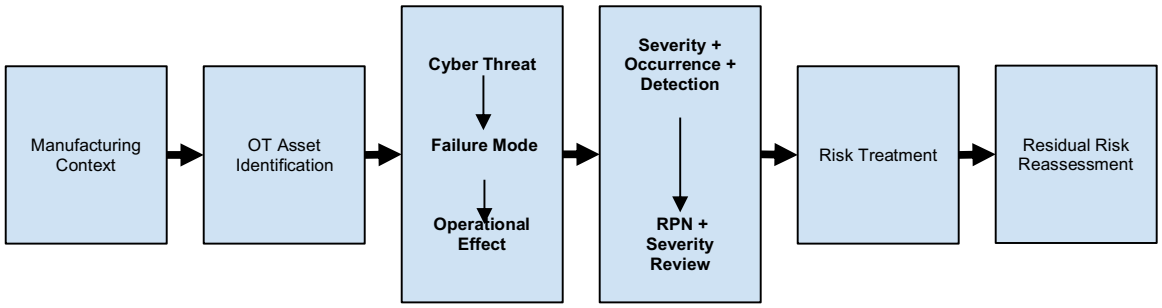


Figure 2. FMEA-Based OT Security Risk Prioritization Framework

The framework changes the primary decision question from "Which vulnerability should be fixed first?" to "Which cyber-induced failure presents the greatest risk to manufacturing operations?" This distinction enables cybersecurity priorities to reflect production criticality rather than technical vulnerability characteristics alone.

3.4 Operational Risk Assessment Using the FMEA Framework

The operational risk assessment was conducted by integrating the proposed FMEA framework with the manufacturing consequences of cyber-induced failure scenarios. Each identified OT risk was evaluated using three criteria: Severity (S), representing the magnitude of potential operational consequences; Occurrence (O), indicating the relative likelihood of a cyber-induced failure; and Detection (D), reflecting the difficulty of identifying the failure before significant operational disruption. The resulting Risk Priority Number (RPN = S × O × D) provided a systematic basis for ranking risk-treatment priorities.

The assessment identified five high-priority scenarios, with RPN values ranging from 270 to 420, and two moderate-priority scenarios, with RPN values of 168 and 240. Unauthorized PLC logic modification received the highest priority (RPN = 420) because of its potential to disrupt critical process-control functions. Unauthorized remote access ranked second (RPN = 360), reflecting the operational consequences of compromised external connectivity. Engineering workstation compromise and industrial network disruption shared an RPN of 324, followed by SCADA server disruption (RPN = 270). These findings indicate that risks affecting process control, system configuration, and industrial communication require particular attention in manufacturing risk management.

To support operational decision-making, the framework combines RPN-based ranking with a severity-based review mechanism. Scenarios with Severity scores of 9–10 require explicit management evaluation regardless of their overall RPN classification. This approach helps prevent potentially catastrophic operational failures from receiving insufficient attention because of relatively low Occurrence or Detection scores. Risk-treatment decisions are subsequently aligned with the dominant risk factors: preventive controls address Occurrence, detective controls improve Detection, and recovery measures support production restoration and operational resilience.

The framework also establishes a basis for evaluating risk-treatment effectiveness through residual FMEA assessment and manufacturing performance indicators, including unplanned production downtime, equipment availability, and mean time to recovery (MTTR). Although the present scenario-based assessment does not provide empirical evidence of operational performance improvement, the proposed evaluation mechanism enables future manufacturing applications to examine whether prioritized cybersecurity controls contribute to measurable reductions in operational disruption. Thus, the FMEA framework connects cybersecurity risk assessment with manufacturing-oriented decision-making while maintaining traceability between failure scenarios, risk scores, treatment priorities, and expected operational outcomes.

The proposed risk prioritization approach is consistent with previous industrial engineering research emphasizing systematic assessment of operational failure consequences. (Asdi et al., 2025) demonstrated the application of FMEA-based prioritization to operational risk mitigation, while (Ayu Febriana et al., 2025)

DOI: https://doi.org/10.37631/jri.v8i2.2497
Hak Cipta © 2026, Nugraha, Arya Adhi
This is an open-access article under the CC BY-NC License.

highlighted the importance of identifying interrelated risk factors in manufacturing operations. Building upon these perspectives, the present study extends operational risk assessment by explicitly incorporating cyber-induced failure modes into manufacturing-oriented FMEA prioritization.

3.5 Discussion

The findings suggest that FMEA provides a structured connection between OT cybersecurity and industrial risk engineering by treating cyber-induced operational failure scenarios as the primary unit of analysis. Unlike vulnerability-centered approaches, the proposed framework evaluates cybersecurity threats according to their potential consequences for production reliability, equipment availability, operational safety, and manufacturing continuity. This perspective extends conventional manufacturing risk analysis by explicitly incorporating cybersecurity threats into failure-mode identification and operational risk prioritization.

An important methodological contribution is the adaptation of the Detection criterion to OT cybersecurity. Within the proposed framework, Detection represents the capability to identify malicious activities, unauthorized configuration changes, abnormal industrial communications, or compromised OT components before they cause significant operational consequences. This interpretation enables cybersecurity monitoring capabilities to be evaluated within an established industrial risk-assessment structure, facilitating communication among cybersecurity specialists, production engineers, maintenance personnel, and management.

Nevertheless, conventional RPN-based prioritization has several limitations, including subjective scoring, equal mathematical treatment of Severity, Occurrence, and Detection, and the possibility of identical RPN values for different risk profiles. Furthermore, cyber threats involve adaptive adversaries whose behavior cannot always be represented through conventional failure-frequency assumptions. Although the proposed severity-based review mechanism provides an additional safeguard, the framework requires further validation using industrial operational data and structured expert assessment.

The principal contribution of this study is therefore the development of an interpretable framework that integrates cybersecurity risk assessment with manufacturing-oriented decision-making. By linking cyber threats, operational failure modes, risk priorities, and corresponding treatments, the framework provides a foundation for allocating cybersecurity resources according to their potential significance for manufacturing resilience. Future research should investigate the integration of Analytic Hierarchy Process (AHP), fuzzy FMEA, or probabilistic approaches to improve risk-factor weighting, uncertainty representation, and empirical validation.

IV. SIMPULAN

This study developed an FMEA-based framework for prioritizing Operational Technology (OT) security risks in manufacturing environments by integrating cybersecurity threat analysis with failure-oriented industrial risk assessment. The framework addresses the need for a practical mechanism that translates cyber threats into operationally meaningful risk priorities. Instead of assessing OT cybersecurity primarily from the perspective of vulnerabilities and technical consequences, the proposed approach establishes a traceable relationship between OT assets, cyber threat scenarios, failure modes, operational effects, FMEA criteria, risk priorities, and corresponding treatment measures.

The findings demonstrate that FMEA can provide a structured mechanism for differentiating OT cybersecurity risks according to their potential effects on manufacturing operations. Among the representative scenarios analyzed, unauthorized modification of PLC control logic generated the highest RPN (420), followed by unauthorized remote access (360), engineering workstation compromise (324), industrial network disruption (324), and SCADA service disruption (270). These results indicate that assets with direct influence over process control, system configuration, and industrial communications require particular attention because their compromise may propagate from the cyber domain into physical production processes. The analysis also demonstrates that RPN should not be interpreted as an absolute measure of cybersecurity risk. High-severity scenarios require explicit management review even when their occurrence or detection scores result in a comparatively moderate RPN.

The study contributes theoretically by extending conventional FMEA reasoning into OT cybersecurity and positioning cyber-induced events as potential causes of manufacturing system failures. This establishes a conceptual bridge between cybersecurity risk management, reliability engineering, and operational resilience. The proposed approach therefore shifts the analytical focus from determining which technical vulnerabilities

DOI: https://doi.org/10.37631/jri.v8i2.2497
Hak Cipta © 2026, Nugraha, Arya Adhi
This is an open-access article under the CC BY-NC License.

are most severe to determining which cyber-induced failure scenarios present the greatest consequences for manufacturing operations. This distinction represents the principal contribution of the framework to industrial risk engineering.

From a practical perspective, the framework can support manufacturing organizations in allocating limited cybersecurity resources according to operational priorities. The resulting risk ranking can inform the implementation of preventive, detective, and recovery measures, including network segmentation, privileged-access management, OT monitoring, configuration control, backup, redundancy, and recovery planning. Furthermore, the use of FMEA terminology may facilitate collaboration among cybersecurity professionals, production engineers, maintenance personnel, reliability specialists, and management by providing a common risk language that is already familiar within manufacturing environments.

Several limitations should be considered when interpreting the findings. The numerical assessment presented in this study represents a framework-based application to representative OT scenarios and should therefore not be generalized as universal risk values for all manufacturing environments. Severity, occurrence, and detection scores remain dependent on organizational context, system architecture, threat exposure, existing controls, and expert judgment. In addition, conventional RPN calculations may produce identical values for substantially different combinations of risk factors and do not explicitly account for the adaptive behavior of cyber adversaries. Consequently, organizations applying the framework should calibrate the assessment criteria and priority thresholds according to their specific operational context and risk appetite.

Future research should empirically validate the proposed framework through industrial case studies and structured expert evaluation involving cybersecurity, production, maintenance, and reliability practitioners. Further development may integrate FMEA with multi-criteria decision-making methods such as the Analytic Hierarchy Process (AHP), fuzzy logic, or probabilistic approaches to address uncertainty and differential weighting among risk factors. Longitudinal studies could also examine whether changes in RPN and individual FMEA dimensions following security-control implementation correspond with measurable improvements in OT resilience.

In conclusion, effective OT cybersecurity in manufacturing requires more than identifying technical vulnerabilities; it requires understanding how cyber threats can cause operational failures and which of those failures demand priority attention. The proposed FMEA-based framework provides a systematic and interpretable foundation for this purpose, enabling OT cybersecurity decisions to be aligned with the broader objectives of production reliability, operational continuity, and manufacturing resilience.

APPRECIATION

The author expresses appreciation to all parties who provided support and relevant sources of information for the conduct of this research.

DECLARATION

ARTIFICIAL INTELLIGENCE USE STATEMENT (AI STATEMENT)

The author declares that there was no use of artificial intelligence (AI) in the process of compiling, writing, or analyzing the data in this article.

AUTHOR CONTRIBUTION STATEMENT

Conceptualization, methodology, data collection, data analysis, visualization, and writing of the first draft, review, and final editing of the manuscript. The author has read and approved the final published version of the manuscript.

FUNDING STATEMENT

This research was conducted independently and did not receive funding from any institution, organization, or party.

CONFLICT OF INTEREST STATEMENT

The author declares that there is no conflict of interest, either financial or non-financial, related to the conduct of the research or publication of this article.

STATEMENT OF RESEARCH AND PUBLICATION ETHICS (ETHICAL CONSIDERATION / PUBLICATION ETHIC)

This research evaluates Operational Technology security risks through analytical framework development and simulation/scenario-based modeling; it does not involve human subjects, animal testing, or confidential personal data collection. Participation consent and human research ethics clearance were not required. All data used were anonymized and strictly processed in compliance with research and publication ethics standards.

DOI: https://doi.org/10.37631/jri.v8i2.2497
Hak Cipta © 2026, Nugraha, Arya Adhi
This is an open-access article under the CC BY-NC License.

REFERENCE

Automotive Industry Action Group, & Verband der Automobilindustrie. (2019). AIAG & VDA FMEA handbook (1st ed.). Automotive Industry Action Group.

Abergos, V. J., & Medjek, F. (2024). A Risk Assessment Analysis to Enhance the Security of OT WAN with SD-WAN. *Journal of Cybersecurity and Privacy*, *4*(4), 910–937. https://doi.org/10.3390/jcp4040042

Asdi, R. Z., Utomo, D. S., Daulika, P., & Sumarna, D. (2025). Manajemen Risiko pada Distributor Tandan Buah Segar (TBS) Kelapa Sawit: Analisis dan Strategi Mitigasi. *Jurnal Rekayasa Industri (JRI)*, *7*(1), 61–68. https://doi.org/10.37631/jri.v7i1.1850

Ayu Febriana, D., Lucy Ardiani, F., Yuliadi Wijaya, E., & Yuliawati, E. (2025). Analisis Terstruktur Faktor Risiko Operasional Industri Manufaktur Kertas Menggunakan Pendekatan ISM-MICMAC. *Jurnal Rekayasa Industri (JRI)*, *7*(2), 109–119. https://doi.org/10.37631/jri.v7i2.2008

Da Silva, M., Mocanu, S., Puys, M., & Thevenon, P.-H. (2025). Safety-security convergence: Automation of IEC 62443-3-2. *Computers & Security*, *156*, 104477. https://doi.org/10.1016/j.cose.2025.104477

Ervural, B., & Ayaz, H. I. (2023). A fully data-driven FMEA framework for risk assessment on manufacturing processes using a hybrid approach. *Engineering Failure Analysis*, *152*, 107525. https://doi.org/10.1016/j.engfailanal.2023.107525

Halawi Ghoson, N., Meyrueis, V., Benfriha, K., Guiltat, T., & Loubère, S. (2025). A review on the static and dynamic risk assessment methods for OT cybersecurity in industry 4.0. *Computers & Security*, *150*, 104295. https://doi.org/10.1016/j.cose.2024.104295

Kahouadji, H. A., & Belkaid, F. (2025). A New Hybrid FMECA Model for Prioritizing Failure Modes Using Multi-Criteria Decision Making. *Management and Production Engineering Review*, *16*(1). https://doi.org/10.24425/mper.2025.153926

Park, C., Kontovas, C., Yang, Z., & Chang, C.-H. (2023). A BN driven FMEA approach to assess maritime cybersecurity risks. *Ocean & Coastal Management*, *235*, 106480. https://doi.org/10.1016/j.ocecoaman.2023.106480

Rahman, H., Hamedani, E. Y., Son, Y. J., & Shafae, M. (2024). Taxonomy-Driven Graph-Theoretic Framework for Manufacturing Cybersecurity Risk Modeling and Assessment. *Journal of Computing and Information Science in Engineering*, *24*(7). https://doi.org/10.1115/1.4063729

Salah, B., Alnahhal, M., & Ali, M. (2023). Risk prioritization using a modified FMEA analysis in industry 4.0. *Journal of Engineering Research*, *11*(4), 460–468. https://doi.org/10.1016/j.jer.2023.07.001

Suorsa, M., & Helo, P. (2026). Cybersecurity Risks and Defense for a European Energy Retail Business: A Case Study Using FMEA and Bowtie Incident Analysis. *Information Security Journal*, *35*(2). https://doi.org/10.1080/19393555.2025.2489421

Zarreh, A., Wan, H., Lee, Y., Saygin, C., & Janahi, R. A. (2019). Risk Assessment for Cyber Security of Manufacturing Systems: A Game Theory Approach. *Procedia Manufacturing*, *38*, 605–612. https://doi.org/10.1016/j.promfg.2020.01.077

Zhang, J., Chu, H., Xu, J., Cheng, Q., Cao, J., & Wang, Y. (2026). Quantifying potential cyber-attack risks in CNC systems under zero-subjectivity closed-loop Dempster–Shafer theory FMECA and rule-based Bayesian network modelling. *Reliability Engineering & System Safety*, *274*, 112427. https://doi.org/10.1016/j.ress.2026.112427

International Organization for Standardization, & International Electrotechnical Commission. (2022). Information security, cybersecurity and privacy protection—Guidance on managing information security risks (ISO/IEC Standard No. 27005:2022). https://www.iso.org/standard/80585.html

DOI: https://doi.org/10.37631/jri.v8i2.2497
Hak Cipta © 2026, Nugraha, Arya Adhi
This is an open-access article under the CC BY-NC License.