

Article

Towards Secure Legacy Manufacturing: A Policy-Driven Zero Trust Architecture Aligned with NIST CSF 2.0

Cheon-Ho Min ¹, Deuk-Hun Kim ², Haomiao Yang ³ and Jin Kwak ^{1,*}¹ ISAA Laboratory, Department of Cyber Security, Ajou University,

Suwon 16499, Gyeonggi-do, Republic of Korea; mcheonho@ajou.ac.kr

² ISAA Laboratory, Institute for Computing and Informatics Research, Ajou University,

Suwon 16499, Gyeonggi-do, Republic of Korea; kimdh1206@ajou.ac.kr

³ Center for Cyber Security, University of Electronic Science and Technology of China (UESTC), No. 2006

Xiyuan Avenue, West Hi-Tech Zone, Qingshuihe Campus, Chengdu 611731, China; haomyang@uestc.edu.cn

* Correspondence: security@ajou.ac.kr

Abstract

As smart manufacturing environments continue to evolve, operational technology systems are increasingly integrated with external networks and cloud-based platforms. However, many manufacturing facilities still use legacy systems running on end-of-support/life operating systems with discontinued security updates. It is difficult to mitigate the cyber threats and risks for these systems using perimeter-based security models that isolate them from other networks. To address these constraints, a Zero Trust-based security architecture tailored for legacy manufacturing environments with practical field applicability is proposed. Our architecture builds upon the six core functions outlined in National Institute of Standards and Technology Cybersecurity Framework 2.0—identify, protect, detect, respond, recover, and govern—adapting them specifically to manufacturing environment security challenges. To achieve this, the architecture combines asset identification, policy-driven access control, secure SMB gateway transfers, automated anomaly detection and response, clean image recovery, and organizational governance procedures. This study validates the effectiveness and scalability of the proposed architecture through scenario-based simulations. When combining the EoSL defense hardening and gateway-based perimeter control, the architecture achieves approximately 99% overall threat suppression and a 98% reduction in critical-asset infection rates, demonstrating its strong resilience and scalability in large-scale legacy OT environments.

Keywords: industrial control system security; industrial cybersecurity; legacy system security; NIST CSF 2.0; security governance; zero trust architecture



Academic Editor: Liang Ma

Received: 18 September 2025

Revised: 10 October 2025

Accepted: 16 October 2025

Published: 20 October 2025

Citation: Min, C.-H.; Kim, D.-H.; Yang, H.; Kwak, J. Towards Secure Legacy Manufacturing: A Policy-Driven Zero Trust Architecture Aligned with NIST CSF 2.0. *Electronics* **2025**, *14*, 4109. <https://doi.org/10.3390/electronics14204109>

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The manufacturing environment has evolved into a smart factory through the convergence of various information technologies (ITs), and productivity has greatly improved. As new equipment and technologies are introduced, smart factories are becoming increasingly connected to external networks and cloud computing platforms, but this has simultaneously amplified cybersecurity threats.

Recently, manufacturing companies such as Toyota, TSMC, and Olympus have been hit by cyberattacks, which have caused production disruptions, financial losses, and reputational damage. Many manufacturing companies are still using old operating systems (OSs) (Windows XP, Windows 7, Windows Server 2003) that have reached the

End-of-Service-Life (EoSL) and are vulnerable to security threats. Manufacturers use these OSs because they cannot upgrade them due to production disruptions that may occur during system upgrades, compatibility issues with existing environments, and equipment suppliers' discontinuation of technical support.

In such environments, traditional network-based perimeter security models are insufficient to address the multifaceted threats of smart manufacturing environments, which require a new security approach. Consequently, this study proposes the adoption of a Zero Trust security architecture (ZTA) that continuously verifies and controls all access attempts as a fundamental alternative.

In addition to the ZTA outlined in Special Publication (SP) 800-207, the National Institute of Standards and Technology (NIST) introduced the Cybersecurity Framework (CSF) 2.0 in 2024. This framework emphasizes a comprehensive life cycle-based approach structured around six core functions: identification, protection, detection, response, recovery, and governance. It is increasingly recognized as a practical foundation for systematically strengthening security in high-risk environments, such as manufacturing systems [1,2].

Zero Trust (ZT) is a security architecture and philosophy designed to mitigate risks through continuous access verification and minimum-privilege enforcement. The NIST CSF 2.0 provides a structural foundation for implementing ZT by offering an integrated security operations framework that supports the functional requirements needed for its implementation [1,2].

This study proposes a practical ZTA tailored to the technical and operational constraints of manufacturing environments. To achieve this, the following research objectives are established:

1. Examine the OS landscape and associated security threats in legacy manufacturing systems used in manufacturing process systems.
2. Design a function-specific ZTA aligned with NIST CSF 2.0, focusing on asset identification, secure file sharing, access control, and log management.
3. Examine the distinctions between the proposed architecture and existing security systems and identify the conditions under which the model can be effectively implemented in real-world manufacturing environments.

2. Analysis of Security Vulnerabilities in the Manufacturing Process

2.1. Current Security Threat Landscape in Manufacturing OT Environments

In March 2022, Toyota parts supplier Kojima Industries was affected by a ransomware attack, temporarily halting operations at 14 factories and 28 assembly lines in Japan. This forced Toyota to reduce overall production by 5% [3].

In 2021, a water treatment facility in Oldsmar, Florida, was targeted by a cyberattack, in which a hacker remotely accessed the system and attempted to alter the chemical concentration in the water supply to unsafe levels. Although the attack was detected in real time and mitigated before causing harm, it highlighted the potential for direct physical harm to OT systems [4].

That same year, Olympus, a Japanese medical device manufacturer, experienced a ransomware attack that resulted in network outages and operational disruptions in certain regions. These incidents demonstrate that OT security is not limited to information protection but is directly related to the stability of production processes and critical infrastructure [5].

In 2018, TSMC was infected with ransomware, rendering more than 10,000 production systems inoperative. The incident led to a 48 h production stop and an estimated financial loss of approximately 250 million dollars [6].

A recent report found that 89% of manufacturing companies have experienced a cyberattack, with the average cost of damages estimated at USD 3 million per incident. The results indicate that manufacturing environments require strong cybersecurity measures [7].

2.2. Structural Vulnerabilities in OT Systems

OT systems are inherently designed to prioritize real-time performance and high availability, which complicates the implementation of effective security responses.

First, many OT systems continue to operate using outdated OS and legacy hardware. Due to the long operational life cycles typical of industrial environments, it is common to find systems running on unsupported platforms such as Windows XP, Windows 7, and Windows Server 2003. These outdated systems are exposed to known vulnerabilities without access to critical security patches [8].

Second, because OT systems are tightly coupled with real-time control processes, any system downtime directly disrupts production. As a result, it is challenging to apply security patches or perform timely system updates.

Third, increased integration of OT with IT systems has expanded the network's exposure. As OT environments have become interconnected with external networks and cloud platforms to enable smart factory implementations, the number of potential attack vectors for adversaries has increased significantly [8].

2.3. OS Status of Manufacturing Process Systems

To support this study, an empirical analysis was conducted on the OSs of production and process control personal computers (PCs) currently used in two major manufacturing plants. The analysis revealed that in Plant A, 10,925 of 20,498 systems (approximately 65.7%) were running EoSL versions of Windows OS that no longer received security updates from Microsoft. Similarly, in Plant B, 277 of the 700 systems (approximately 39.6%) were using outdated platforms that were no longer eligible for security patches (data collected in April 2025). The OS distribution for Plant A is summarized in Table 1.

Table 1. Distribution of OS in production and process PCs at manufacturing plant A.

Category	OS	Number of Systems	Percentage
EoSL	Windows XP, 7, Server 2003, etc.	10,925	65.7%
Supported	Windows 10, 11, etc.	7573	34.3%
Total	–	20,498	100%

According to a report by a leading cybersecurity media outlet, a collaborative study conducted by Honeywell, Yokogawa Electric, and Schneider Electric examined the versions of stations and servers across 635 distributed control systems (DCSs). The results showed that only 22.5% of the systems were operating on current versions of Microsoft Windows, whereas the remaining 77.5% were running on discontinued versions [9].

It is evident that the continued use of outdated OS across manufacturing environments poses a significant threat to the security of production systems. Specifically, EoSL OS versions like Windows XP, Windows 7, and Windows Server 2003 contain numerous vulnerabilities as documented in the Common Vulnerabilities and Exposures (CVEs) database, making them easy targets for attackers [10].

A single system vulnerability can be used as an entry point for compromising the entire production environment.

The security of process control systems should extend beyond merely addressing unpatched software vulnerabilities; it involves responding to broader threats where

unmanaged legacy assets can be exploited by attackers as initial vectors for supply chain compromises or ransomware propagation.

2.4. The Inevitability of Maintaining Legacy Systems

Although security updates and vendor support for legacy systems have terminated, they remain widely used in OT environments across the manufacturing industry because their replacement is often delayed due to various practical constraints. The Global Cyber Alliance (GCA) and the International Society of Automation (ISA) have analyzed the underlying factors contributing to this continued reliance, as well as the associated security risks [10]:

1. End-of-vendor support and technical limitations: Many legacy systems are no longer supported by vendors, making hardware replacements or software updates infeasible [10].
2. High replacement costs and operational disruption: Upgrading OT systems involves more than just software changes; it may require a complete redesign and revalidation of the entire system [10].
3. Compatibility issues and integration challenges: Legacy systems may be optimized for specific hardware and software environments, making integration with modern systems difficult [10].

2.5. Limitations of Conventional Security Approaches

In industrial environments, traditional perimeter-based security approaches like firewalls and IP-based access control are increasingly ineffective against the modern threat landscape due to their inherent limitations [11]. The overall system architecture is shown in Figure 1

1. The perimeter-based models are particularly vulnerable to lateral movements, authentication bypasses, and external intrusions [11].
2. Assets in OT environments change dynamically, whereas static policy-based access control (PBAC) mechanisms struggle to detect and respond to real-time threats [11].
3. Mechanisms for identifying users and devices are often lacking, resulting in poor accountability and insufficient granularity of access control [11].
4. The application of security patches is frequently delayed or postponed indefinitely to minimize system downtime [11].

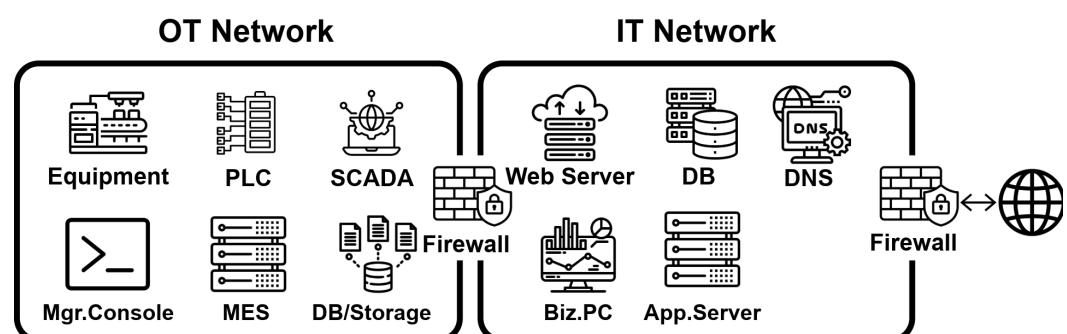


Figure 1. Perimeter-based IT-OT security architecture.

These limitations suggest the need for a new security paradigm. OT systems in manufacturing remain at risk due to (i) increasingly sophisticated cyber threats, (ii) the continued use of legacy systems, and (iii) the technical limitations of existing security mechanisms.

Therefore, rather than relying on conventional perimeter-based and network-centric approaches, it is imperative to adopt a ZTA that continuously verifies and controls access based on identity, device attributes, user behavior, and contextual factors.

3. Theoretical Background of ZTA

3.1. Overview of the ZTA

A ZTA is a security architecture that begins with the premise that trust based on network location, whether internal or external to an organization, can no longer be assumed. As summarized in NIST SP 800-207, ZT is defined as ‘a security model that enforces access decisions based on continuous verification, regardless of the physical or network location of assets, users, or services, and applies the principle of least privilege’ [1].

According to the ZTA described in NIST SP 800-207, the following core principles apply [1]:

1. All assets are treated as resources that require protection.
2. All communications are encrypted and subject to verification.
3. All access decisions are made on a per-session basis and follow the principle of least privilege.
4. The basis of policy is dynamically determined.
5. The security posture of assets is continuously assessed.
6. Authentication and authorization are continuous and performed in real time.
7. Organizations must continuously collect and analyze information about assets and network status.

In essence, ZT is not a standalone solution but rather a comprehensive architecture in which an organization’s security strategy, policies, and technologies work in an integrated and coordinated way.

3.2. Security Challenges in Smart Manufacturing Environments

Paul, B. and Rao, M. defined several key security threats in smart manufacturing environments:

1. Implicit trust between devices allows for unauthenticated internal communications.
2. The growing adoption of cloud services renders perimeter-based defenses ineffective.
3. Most manufacturing systems are not designed with security considerations from the outset.

These structural weaknesses strongly indicate the need to adopt a ZTA.

3.3. Core Components of ZTA

Table 2 summarizes the core logical components of the ZTA, based on NIST SP 800-207 and related studies [1,11].

Paul, B. and Rao, M. further propose two adapted models tailored for smart manufacturing environments: “PRA server-based remote access control” and “endpoint compliance-based access control”. These models emphasize practical implementations that align with the specific characteristics and constraints of manufacturing systems.

Table 2. Mapping of core ZTA components to architecture implementation in manufacturing environments.

ZTA Component	Description	Implementation in Proposed Architecture (Section 4)
Policy engine (PE)	Central decision-making engine that evaluates access requests against defined policies.	Realized through the PBAC mechanism in the server message block (SMB) gateway, which verifies user/device/session context and enforces file access rules (Section 4.2.2).

Table 2. Cont.

ZTA Component	Description	Implementation in Proposed Architecture (Section 4)
Policy administrator (PA)	Applies PE decisions by configuring session paths and connection permissions.	The SMB gateway locates file resources and manages indirect delivery paths based on PE decisions, preventing direct access to file locations (Section 4.2.1).
Policy enforcement point (PEP)	The enforcement entity where access is allowed or denied; typically implemented as a gateway or agent.	All file transfers and copies are strictly permitted only through the SMB gateway, which acts as the Policy Enforcement Point (PEP). The gateway enforces access control by allowing or denying file operations based on predefined policies, user credentials, and device attributes (Sections 4.2.2 and 4.4.1).
Continuous diagnostics and mitigation (CDM)	Continuously monitors asset status, vulnerabilities, and threat behaviors.	Integrated anomaly detection system monitors unauthorized protocol usage, abnormal traffic, and external access attempts in real time (Sections 4.3.1 and 4.3.2).
Identity management	Manages authentication and identity verification for users and devices.	Multi-factor authentication (MFA) and asset registration metadata are enforced through administrator-assigned roles and access control workflows (Sections 4.2.2 and 4.6.1).
Threat intelligence and SIEM	Supports anomaly detection, correlation, and automated response using threat data and logs.	Logging systems correlate detection-response events, enabling continuous policy refinement and integration with security orchestration, automation, and response (SOAR) platforms (Sections 4.4.3 and 4.6.2).

3.4. Limitations of Prior Research and Contributions of This Study

Previous studies have recognized critical issues, including the prevalence of EoSL OS and equipment, the need for maintaining continuous operations without production downtime, and the inability to upgrade legacy applications because of the absence of vendor support [8,10,11], but they have not provided sufficiently concrete and actionable strategies to overcome these limitations.

In response, our study designs a ZTA that can be implemented without replacing existing systems to address the unique constraints of manufacturing environments.

4. Application of ZTA to Manufacturing Processes

In manufacturing environments, two critical security threats are the injection of malware-laden files and the exfiltration of sensitive data. Malware often infiltrates internal systems through external files.

Accordingly, this section provides a detailed description of how a security architecture based on NIST CSF 2.0 can be implemented to address these threats in legacy manufacturing environments. The overall CSF 2.0-based security architecture is illustrated in Figure 2.

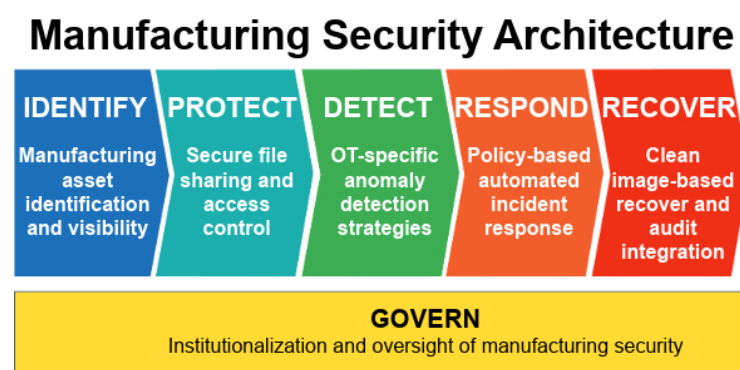


Figure 2. Structured security framework for manufacturing environments integrating ZT principles with the six core functions of NIST CSF 2.0.

4.1. Asset Identification and Inventory of Process PCs for Risk Recognition (Identify)

A fundamental premise of the ZTA is the clear identification and visibility of all assets requiring protection. Notably, effective security policies and least privilege access control cannot be established without a comprehensive understanding of the devices, users, and applications present within a system [12,13].

In smart manufacturing environments, a wide range of process PCs, control systems, and monitoring devices are used across the production lines. Many of these systems operate on outdated OS that no longer receive security updates. In some cases, administrative accounts are undefined or unmanaged, leaving them highly vulnerable to cyber threats.

Therefore, the first and most critical step in applying ZTA to manufacturing environments is the comprehensive identification and asset registration of all production and process control PCs.

The asset inventory step should consider the following key attributes:

1. Device name and functional classification (e.g., production control, inspection equipment, and maintenance systems).
2. OS type and version.
3. Presence and version of installed security solutions.
4. Responsible administrative entity and access control status.
5. Network connectivity status and communication targets.

Production and process control PCs are critical assets that must be protected, as they represent potential security risks. Therefore, it is essential to systematically assess their risk levels. In addition, clearly identifying each device's name and function is crucial for enhancing protection measures through rapid response and continuous risk monitoring.

One effective method for asset identification is OS fingerprint analysis, which can detect the OS used on active network devices. By analyzing Internet Control Message Protocol (ICMP) responses, Transmission Control Protocol (TCP)/IP stack behavior, and open ports through network scanning, this technique enables the accurate identification of OS types and versions. It enables the automatic discovery and cataloging of actively operating devices without manual enumeration by administrators [14].

However, network-based information collection alone cannot collect metadata such as administrators or functional roles. In this study, we propose a lightweight input module embedded in the startup program of the process PC. This module asks the user to input metadata, including the device's function, responsible administrator, and management department, at the time of initial execution. The collected data are stored locally, transferred to the central server, and integrated into the asset database, where administrators can use them to determine the priority of security measures.

In some cases, process control devices are kept offline due to security concerns or operational constraints, making them difficult to identify and monitor. Since ransomware and malware primarily spread through networks, the identification and control of network-connected devices should be prioritized.

4.2. Strategy for Secure File Sharing and Access Control (Protect)

In manufacturing environments, file sharing is critical for tasks such as Manufacturing Execution System (MES) operation, log collection, and process quality data storage. Data transfers between office automation (OA) and production networks are commonly conducted via SMB, File Transfer Protocol (FTP), or external USB devices. However, these file-sharing mechanisms pose significant security threats, particularly when combined with the known vulnerabilities of legacy Windows systems, potentially leading to malware infections and the spread of ransomware [15].

The ZTA treats file sharing as a control target and adopts a verification-based approach to determine whether file sharing should be permitted. By applying this principle to manufacturing environments while considering practical constraints such as the use of EoSL systems, this study proposes a set of practical strategies for secure file sharing and access control as outlined in the following sections.

4.2.1. Centralized Control Architecture Using an SMB Gateway

SMB-based file sharing is common in legacy manufacturing systems, but it introduces risks such as malware infection, ransomware propagation, and data leakage [15,16].

In the proposed ZT architecture, the SMB gateway has a key control role. One of the most serious security issues in manufacturing environments is uncontrolled file movement, which can lead to the installation of malicious code and the leakage of sensitive production data. Once infected files are transferred to an unprotected OT PC, they can quickly spread to other vulnerable systems within the same network segment. At the same time, unauthorized users may gain access to production assets and extract sensitive information.

To mitigate these risks, the proposed architecture enforces strict control over all file movement in the OT network. File movement and copy requests are only allowed through the SMB gateway, which verifies session authorization, performs malware scanning, and enforces policy-based access control (PBAC). With this centralized architecture, the SMB gateway effectively eliminates file propagation vectors and reduces the overall attack surface across the existing OT environment, as illustrated in Figure 3.

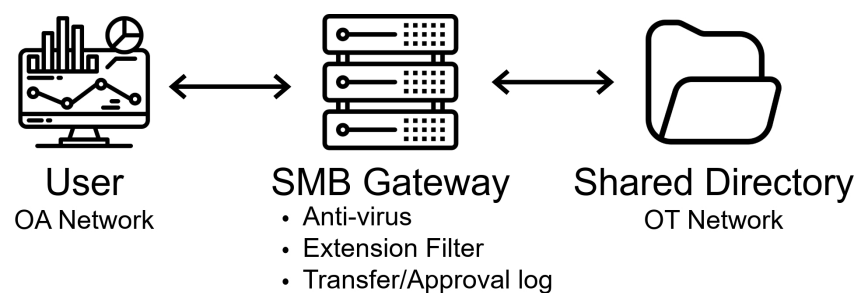


Figure 3. Policy-governed secure file-transfer flow illustrating the sequential enforcement of authentication, authorization, malware scanning, PBAC, and secure file transfer through the SMB gateway. All steps occur within defined trust boundaries between the OA user zone and the OT network.

The detailed operational flow is as follows.

1. Access request handling and authorization: When a file needs to be accessed or transferred to a PC, a request is sent to the SMB gateway. The gateway verifies the request based on the requester's authentication and authorization information (e.g., MFA, IP address, media access control (MAC) address, and device ID), access intent, and session status. PBAC is applied to determine whether the user is authorized to access the requested file.
2. File location resolution and request processing: Once the request is approved, the SMB gateway locates the actual file in remote storage accessible via the SMB, a connected process-control PC, or a file server. Given that the access paths are unified through the gateway, users cannot identify or directly access the physical file location.
3. Malware infection scanning: Prior to transmission, the SMB gateway performs real-time anti-malware scanning of the requested file. It detects spoofing by comparing the file extension with its actual content, performs hash-based integrity verification and if malicious elements are detected, the gateway blocks the file transfer and logs the event.

4. File delivery and logging: If a file is determined to be safe, the gateway sends the file to the user. All steps, including request, verification, and delivery, should be logged on a per-session basis.

This architecture prevents direct communication between users and files, as the SMB gateway inspects and controls all requests.

4.2.2. Establishing ZT-Based Access Policies

The SMB gateway, serving as the foundation for file sharing, should adopt the following PBAC model:

1. Principle of least privilege: Access rights are granted strict granularity by the device and user, restricting the available resources and permitted actions (e.g., read, write, and execute) to the minimum necessary.
2. Session-based authentication: File-sharing sessions require user authentication, including MFA, and enforce session timeouts.
3. Dynamic access policy: The PBAC model is applied to enable dynamic policy adjustments based on asset risk level, location, access time, and other situational factors.

In traditional file transfer scenarios, protocols such as SMB or FTP typically rely on Windows or Active Directory (AD)-based authentication, which restricts flexibility and makes it difficult to enforce stronger authentication mechanisms. By introducing the SMB gateway as a centralized control point, the proposed architecture decouples authentication from the legacy AD domain. This allows the enforcement of enhanced authentication policies, including password-based and MFA, before granting access to shared resources. Thus, MFA is technically feasible and operationally enforceable in legacy manufacturing contexts, addressing a critical limitation of existing file transfer methods.

These policies should be lightweight, centrally deployable, easy to manage, and enforceable in a way that does not disrupt production operations, as illustrated in Figure 4.

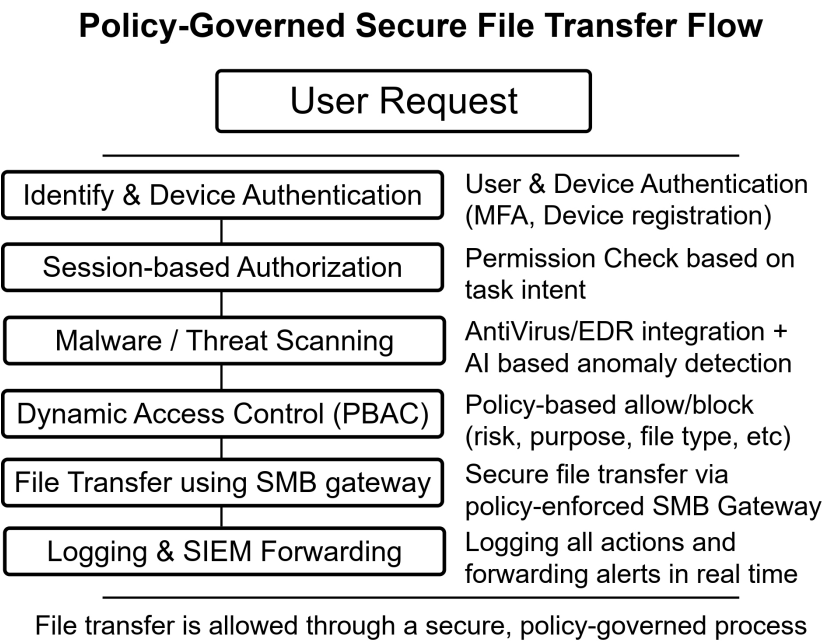


Figure 4. OA-OT file-transfer architecture showing that all files from the OA network pass through the SMB gateway—where antivirus scanning, file-extension filtering, and approval logging are enforced—before reaching the OT shared directory. The dashed arrow represents the controlled flow across the OA-OT trust boundary.

4.2.3. Summary of Technical Measures for Secure File Sharing

Secure file sharing is a core component of manufacturing process security, and traditional convenience-focused sharing methods must be re-engineered from a ZT perspective. Integrating a centrally controlled sharing architecture through an SMB gateway, granular PBAC, and network anomaly-detection mechanisms enables the establishment of a secure file-sharing system that is technically viable, even in environments with EoSL systems, minimizing disruption to ongoing operations. This approach aligns with the “continuous authorization and monitoring” principle defined in the ZTA and offers a practical implementation strategy within manufacturing settings. A summary of the technical components and their implementation objectives for secure file sharing is provided in Table 3.

Table 3. Technical measures for secure file sharing.

Technical Element	Implementation Objective	Application Method
USB port locker	Maintaining a clean environment	Disabling USB usage; allowing only clean USBs when necessary
SMB gateway	Controlling file-level access across network segments	Centralized routing, policy enforcement, file validation
Policy-Based Access Control	Enforcing least privilege	Access rights differentiated by user, device, and purpose
MFA authentication	Strengthening session-level verification	Two-factor authentication required for user access
Network detection	Identifying unauthorized file transfers	Detecting abnormal or unauthorized transmissions
File integrity check	Blocking malware propagation	Hash comparison; extension-content filtering
Behavior-based logging	Ensuring accountability	Detailed logging and storage of user actions

In the proposed design, MFA is required when a user connects to the SMB gateway. Once the connection is established and authentication is completed, a secure session is created and all subsequent file access requests are processed under this session. This approach provides a unified authentication mechanism, ensures that every access passes through the gateway’s centralized control, and enables consistent enforcement of security policies. As a result, safe and reliable file sharing can be achieved in legacy manufacturing environments without disrupting operational continuity.

4.3. Anomaly Detection Strategies Tailored for OT Environments (Detect)

The ZTA is based on the principle that no asset or user is inherently trusted, and that all requests and actions must be continuously verified. Consequently, detection must extend beyond perimeter monitoring to include real-time identification of the context of each action and any violation of defined security policies [1,13].

In manufacturing environments, systems are highly interconnected, and the failure of a single device can disrupt the entire production process. Therefore, early detection and rapid response to individual threats are essential for maintaining operational continuity.

Considering these environmental characteristics, we propose a detection strategy that monitors security policy violations, identifies abnormal traffic, and monitors and restricts external communication behavior in real time.

4.3.1. Detection System for Unauthorized File Transfer and Policy Violations

To enforce a security policy that restricts file transfers and sharing exclusively through the SMB gateway, a real-time monitoring system must be implemented. Accordingly, it is necessary to establish a mechanism—with the following key components—capable of detecting policy violations as they occur:

1. Real-time detection and blocking of unauthorized file transfer traffic: File transfer attempts using prohibited protocols (e.g., SMB and FTP) in restricted network segments are automatically detected and blocked. A real-time alert is generated and sent to the administrator for immediate awareness and response.
2. Logging and analysis of policy violations: Detected actions are immediately logged with detailed information, including the user ID, access time, request path, and target device. These data support forensic analysis and refinement of response policies.

4.3.2. Detection of Malware Propagation and Abnormal Traffic

Following the initial infiltration via the SMB, attacks may manifest in various forms, including file encryption, mass deletion, traffic flooding, or attempts to connect to external command-and-control (C&C) servers. Accordingly, the following anomaly-detection items are defined and monitored in real time:

1. Detection of abnormal traffic spikes: Sudden surges in traffic originating from a single device or user are detected. If predefined thresholds are exceeded, automated alerts and blocking actions are triggered.
2. Detection of external connection attempts (C&C Server Access): If an internal asset attempts to connect to an unauthorized external IP address or domain, especially those not designated for communication, such behavior is detected and either blocked or escalated by administrators according to predefined policies.
3. File system behavior-based detection: Repeated file encryption, deletion, or executable file transfers within a short timeframe are considered a typical indicator of malware propagation. Rule-based detection policies are applied to identify such behaviors.

4.3.3. Structural Integration of Detection, Policy and Governance

Anomaly detection should extend beyond event monitoring to actively enforce organizational policies and trigger immediate responses to policy violations. The proposed detection strategy is structurally linked to subsequent procedures, such as automated blocking, administrator notification, log analysis, and policy update requests, and must be closely integrated with the response presented in Section 4.4 and the governance framework outlined in Section 4.6.

4.4. Policy-Driven Anomaly Response (Respond)

In ZTA, detection and response must operate in tandem. Responses should be automated, policy-driven, and based on observed behavior. In manufacturing environments where operational continuity is critical, immediate threat assessment and rapid containment are essential.

4.4.1. Automated Response to Policy Violations

The architecture automatically blocks events when abnormal behavior is detected, prevents malware from spreading, and minimizes the impact on the entire production process. Given the importance of continuity and real-time operation in manufacturing environments, an immediate and accurate response is essential to prevent production interruptions.

Based on these requirements, this study defines an automated response procedure for handling policy violations and abnormal behavior as follows:

1. Automatic blocking upon detection of unauthorized SMB use: The use of SMB is strictly prohibited outside the SMB gateway-controlled path. If SMB communication is detected in an unauthorized segments, the system automatically terminates the communication session, temporarily restricts network access for the asset attempting to use SMB, and sends an immediate alert to the administrator while creating a log

entry. This response focuses on early containment by eliminating potential malware entry paths during the initial stage.

2. Connection termination upon detection of external C&C access attempts: When an internal asset attempts to connect to an external domain or IP address not permitted by the policy, the system enforces immediate blocking of the relevant communication packets, registers the attempted IP or domain in the internal block list, and sends an automated alert to the network administrator while logging the incident. This procedure is intended to prevent command reception and subsequent attack propagation via C&C server connections.
3. Automated response to abnormal traffic surges: Abnormal traffic surges may signal internal malware propagation, massive data exfiltration, or impending network failures. Therefore, the system executes bandwidth throttling or temporary isolation of the offending device, generates detailed logs that record the time of occurrence and communication targets for forensic tracking, and automatically escalates the asset's threat level upon repeated detection, while notifying the administrator.

These responses contain threats in real time, prevent escalation, and enforce policy-based actions through behavior-driven policy mapping and governance.

While response systems automate threat mitigation, false positives may lead to operational risks; thus, defining the scope of automation, requiring administrator approval, and offering safe-mode fallback procedures are essential for stability.

Integrating a Security Orchestration, Automation, and Response (SOAR) platform can help address these challenges.

4.4.2. Behavior-Based Policy Mapping and Enforcement

Each detection item is mapped to a policy set that specifies appropriate response actions, which are executed automatically. The list of detection items and their associated response actions is summarized in Table 4.

Table 4. Response actions by detection item.

Detection Item	Response Action
Use of unauthorized protocols (e.g., SMB)	Session termination + administrator alert
Traffic exceeding thresholds	Bandwidth throttling or temporary port blocking
Attempt to connect to external servers	Block the connection + update C&C block list
Recurrent policy violations	Asset isolation + threat level adjustment

4.4.3. Integrated Logging of Response Outcomes and Policy Refinement

The architecture should go beyond reactive anomaly handling by incorporating centralized log correlation and historical analysis capabilities. An integrated log management system should record both outcomes and root causes to enable the following activities for systematic policy improvement:

1. Analyzing response success/failure and adjusting thresholds accordingly.
2. Identifying recurring violations and reprioritizing security objectives.
3. Evaluating the effectiveness of policies and identifying areas for improvement.
4. Integrating with governance functions, such as auditing, training, and risk assessment.

The following conditions may necessitate the reconfiguration of detection and policy systems:

1. Re-evaluate the policy's effectiveness in response to recurrent violations.
2. Redefine response methods and conditions when automated responses fail or are bypassed.

3. Enhance detection coverage and refine detection criteria when threats are detected only through manual intervention.

As a core component of a ZTA tailored to the manufacturing environment, this integrated log-management-based response analysis framework facilitates a continuous cycle of detection, response, and policy improvement.

4.5. Clean Image-Based Instant Recovery and Audit-Linked Architecture (Recover)

In manufacturing environments, the primary goals of incident response are to minimize production downtime and rapidly restore operations.

The “recover” function of the ZTA must be adapted to these industrial constraints by integrating two essential capabilities: (1) instant restoration using clean system images and (2) integration with audit processes for post-incident analysis.

4.5.1. Clean Image-Based Instant Recovery Architecture

PCs typically operate with minimal configuration changes and consistent software environments over extended periods. Rather than relying on frequent incremental backups, it is more effective to pre-configure a clean system image with verified integrity and restore the system from this image if an incident occurs [17].

1. Standard image configuration: A clean image containing the OS, process-control software, drivers, and security settings is created and validated via integrity checks. These images are standardized by equipment type and centrally managed.
2. Restoration method: Upon detection of infection or abnormal activity, the affected device is isolated and restored from the clean image, either automatically or with the administrator’s approval. Recovery can often be completed within minutes (depending on the environment) by using local recovery tools or USB-based restoration utilities.
3. Identification of restoration targets: When high-risk anomalies are detected by the SMB gateway, the anomaly detection system, or the log analysis platform, the corresponding device is automatically identified, and its recovery process is triggered.
4. Deploy pre-configured replacement devices: When affected hardware is found to be unreliable or physically damaged, it should be immediately replaced with a pre-configured device preloaded with a validated clean image. This enables rapid recovery without requiring on-site reinstallation, thereby minimizing operational disruption.

4.5.2. Audit-Based Incident Analysis and Recovery Integration

Even when rapid recovery is achieved, it is essential to analyze pre- and post-incident activity logs to determine the root cause of a security incident and prevent its recurrence. Therefore, an integrated architecture is required to correlate behavioral records with recovery processes.

1. Pre- and post-incident log preservation: SMB file-sharing logs, user access records, authentication logs, file movement histories, and administrator approval logs should be backed up or transferred to a central server before system recovery to ensure data retention.
2. Audit-forensic integration: Even after system restoration, audit mechanisms must support forensic analyses based on historical session logs to identify the timelines, attack vectors, and techniques employed. The resulting insights can be used to refine detection rules, update security policies, and improve user training programs.
3. Visualization of recovery history: Records detailing which device was restored, the timing and reason for recovery, the version of the clean image used, responsible

administrators, and incident causes should be stored in a centralized database to enable traceability and asset-specific recovery history management.

This integrated architecture combines clean image-based recovery with audit-driven analysis to provide a practical response strategy that ensures rapid restoration, operational continuity, and forensic traceability within a sustainable ZTA framework.

4.6. Governance Framework for Enhancing Manufacturing Process Security (Govern)

ZTA cannot be achieved through technology alone; it requires organizational oversight, clearly defined roles and responsibilities, and a security-oriented organizational culture.

Thus, this study proposes a security governance framework consisting of four core pillars to ensure the sustainable application of ZT in such environments.

4.6.1. Institutionalization of Asset and Access Control Policies

1. Standardized asset registration procedures: Asset registration and administrator designation must be enforced whenever new equipment is installed, OS is reinstalled, or production processes are modified. Metadata such as device name, function, network connectivity, and administrator information must be collected and integrated with the asset database.
2. Structured privilege management: User accounts, access permissions, and file movement rights must be reviewed quarterly, with all approval histories recorded. An automated privilege revocation mechanism must be implemented for resigned or reassigned personnel either through HR database integration or workflow-based processes.

4.6.2. Reinforcement of File Sharing and System Access Approval Processes

1. Approval Workflow via SMB gateway: All critical file transfers must be approved by an authorized administrator, with the file's purpose, name, and destination explicitly specified. All processing results must be logged for auditability.
2. Dual Authorization for High-Risk System Access: Access to systems running EoSL OS or critical infrastructure should be restricted using a dual control mechanism that combines MFA and administrative approval. All access events must be recorded and linked to device-specific audit logs.

The proposed architecture is scoped to user-initiated file transfers and access requests. Its primary focus is on verifying and approving these requests through the SMB gateway, ensuring that all file exchanges are subject to centralized control and inspection. The architecture does not address strict real-time file-transfer requirements since those are outside the functional scope of the gateway. Real-time data exchanges, such as process data flows between production equipment, are managed by manufacturing execution systems (MES) or engineering control systems (ECS). Accordingly, the architecture emphasizes security assurance for user-driven file sharing and system access, while real-time communication remains within the domain of production systems.

4.6.3. Security Operations Responsibility Structure and Implementation Review System

Effective real-time security incident response requires clearly defined roles spanning detection, containment, and reporting. To ensure stable and continuous security operations, policy-driven role definitions must cover ongoing responsibilities such as asset identification, access authorization, and compliance auditing. Accordingly, the roles and responsibilities (R&R) of asset managers, approvers, and security managers should be formally documented, including the specific actions each must take during an incident. Regular reporting and governance meetings should be held for the security operations and information

security committees. Table 5 outlines the detailed responsibilities of each stakeholder group. This role structure must be consistently maintained and overseen by the organization's security department and the Chief Information Security Officer (CISO) to ensure accountability and policy enforcement.

Table 5. Defined roles and responsibilities in security operations.

Role	Primary Responsibilities	Key Tasks
Asset Manager	Equipment registration and metadata recording Designation of responsible administrators Asset status monitoring and change approval	Register new devices in the asset database Manage device purpose, location, and network configuration
Access Approver	Approve file transfer/access requests Pre-approve high-risk operations Record and report approval history	Process approvals via SMB gateway Evaluate access requests to high-risk systems
Security Officer	Operate security policies and review audit logs Analyze detection results and respond to anomalies Conduct access rights review and adjustment	Terminate sessions after failed authentications Perform quarterly reviews of user privileges Verify integrity of collected logs
System Operator	Manage system settings and recovery processes Maintain clean system images Execute backup and recovery operations	Isolate and restore systems upon anomaly detection Verify image integrity Maintain recovery history records
Training Coordinator	Plan and deliver security training Develop training content Monitor completion rates and retrain violators	Conduct monthly security training sessions Deliver targeted training to users with violation history Report departmental training statistics
CISO	Oversee governance structure Approve and revise policies Develop audit and inspection plans Lead incident reporting and external coordination	Report quarterly policy implementation outcomes Form incident response teams and approve reports Prepare for external audits

Policy compliance monitoring and performance evaluation should be conducted regularly, with key performance indicators—such as policy enforcement rates, anomaly response times, and missing log entries—systematically reviewed.

4.6.4. Security Awareness Enhancement and Cultural Institutionalization Strategy

1. Regular training and practice: Training programs should cover core ZT principles, adherence to approval protocols, and recognition of security anomalies. Risk awareness should be reinforced through real-world manufacturing security incident cases, such as those involving Toyota and TSMC.
2. Structured policy violation response: A structured warning and re-education process should be implemented for violations such as unauthorized access, unapproved file transfers, and the creation of unregistered shared folders.
3. Quantification and feedback mechanism for security awareness: The user security posture is quantified using metrics such as training completion rates, missed approval requests, and policy violations. Periodic assessments of departmental security culture should be conducted using feedback from line managers.

This governance structure serves to elevate technology-based security controls into codified organizational rules and an embedded culture. When policies and procedures are not confined to documentation but are actively integrated into daily workflows and user behavior, ZTA becomes a sustainable operational architecture, even in constrained manufacturing environments.

The ZTA-based security architecture for manufacturing environments is structured around the six core security functions defined in NIST CSF 2.0—identify, protect, detect, respond, recover, and govern. It integrates technical controls with policy enforcement, role-based accountability, and organizational culture to provide a practical and comprehensive approach to strengthening cybersecurity under real-world industrial constraints.

5. Expected Benefits of Security Architecture Implementation

5.1. Conformance Evaluation Based on NIST CSF 2.0

The architecture proposed in this study aligns structurally with NIST CSF 2.0, and suggests potential validity and practical applicability as a strategic security model [2]. Table 6 maps the proposed security components to the CSF functions and categories, demonstrating that the architecture fulfills the requirements of a standards-based security framework. This alignment provides a structural basis indicative of technical efficacy against internationally recognized standards.

As summarized and mapped above, the proposed architecture aligns structurally with the six core functions of NIST CSF 2.0, establishing its validity as a standards-based integrated cybersecurity architecture.

The following section reinforces the technical effectiveness of the proposed model by referencing the quantitative empirical findings of previous research and examining whether this structural foundation translates into measurable security outcomes.

Table 6. Mapping of proposed security measures to NIST CSF 2.0 functions and categories.

Function	Category (CSF Abbreviation)	Summary of Implementation
Identify	Asset management (ID.AM)	Identification of process assets and metadata collection (Section 4.1)
	Risk management strategy (ID.RM)	Risk classification of EoSL devices and policy prioritization (Section 4.1)
	Supply chain risk management (ID.SCRM)	Not applicable
	Governance (ID.GV)	Definition of security responsibilities and role allocation (Section 4.6.3)
	Threat and vulnerability management (ID.TV)	OS fingerprinting and vulnerable asset registration (Section 4.1)
	Information protection strategy (ID.IM)	Design of file control and integrity validation mechanisms (Section 4.2)
Protect	Access control (PR.AC)	PBAC and least privilege enforcement (Section 4.2.2)
	Data security (PR.DS)	Malware scanning and integrity verification via SMB gateway (Section 4.2.1)
	Awareness and Training (PR.AT)	Security education and retraining of violators (Section 4.6.4)
	Information protection processes and procedures (PR.IP)	Approval workflows for file movement and access control (Sections 4.2.2 and 4.6.2)
	Maintenance and technical protection (PR.MA)	Not applicable
Detect	Anomalies and events (DE.AE)	Detection of unauthorized SMB usage and abnormal traffic (Sections 4.3.1 and 4.3.2)
	Continuous security monitoring (DE.CM)	Real-time alerts and log analysis integration (Section 4.3.3)
	Detection processes (DE.DP)	Integrated detection–response–policy linkage (Section 4.3.3)
Respond	Response planning (RS.RP)	Establishment of policy-driven automated response system (Section 4.4)
	Communications (RS.CO)	Alerting system and administrator notification for SMB violations (Sections 4.3.1 and 4.4.1)
	Analysis (RS.AN)	Log analysis and root cause analysis (RCA)-based policy mapping (Section 4.4.2)
	Mitigation (RS.MI)	Blocking SMB sessions and external C&C attempts (Section 4.4.1)
	Improvements (RS.IM)	Policy revisions and reconfiguration after failed responses (Section 4.4.3)
Recover	Recovery planning (RC.RP)	Clean image-based instant restoration structure (Section 4.5.1)
	Improvements (RC.IM)	Audit log analysis and policy refinement post-recovery (Section 4.5.2)
	Communications (RC.CO)	Visualization of recovery history and administrator alerting (Section 4.5.2)
Govern	Policy and regulation (GV.PO)	Asset registration, approval policy, and privilege review framework (Section 4.6.1)
	Roles and responsibilities (GV.RR)	Defined responsibilities for asset/security/approval roles (Section 4.6.3)
	Oversight and decision-making (GV.OV)	Regular reviews, reporting processes, and committee operations (Section 4.6.3)
	Security culture and internalization (GV.CU)	Training, violation response, and security culture integration (Section 4.6.4)

5.2. Anticipated Technical Benefits

The proposed architecture is expected to provide the following technical benefits:

1. Technical enhancement of SMB restriction policies: The SMB gateway is introduced as a technical alternative that allows for controlled use of the SMB protocol while restricting its general usage.

2. Minimization of the impact of security incidents: In the event of a security breach, the system automatically isolates only the affected device, helping to prevent lateral movement and contain the spread of attacks.
3. Technical foundation for security governance: To support security governance, the architecture incorporates integrated log collection and policy violation monitoring, enhancing the visibility and accountability of operational activities.

5.3. Expected Operational Benefits

1. Gradual implementation without operational disruption: The proposed architecture can be deployed incrementally on the existing network without requiring system replacement or downtime.
2. Standardization of work-related file sharing procedures: Previously unregulated file sharing is replaced with a controlled process using an SMB gateway and approval-based access, ensuring operational clarity and traceability.
3. Foundation for policy automation: By integrating asset identification, access control, and anomaly detection logs into a unified structure, the architecture facilitates future linkage with automation platforms such as SIEM and SOAR.

5.4. Expected Administrative Benefits

1. Improved efficiency in integrated asset management: By combining network-based OS fingerprinting with administrator-supplied metadata, the system enables the real-time visibility and streamlined management of production assets across the organization.
2. Enhanced accountability through auditability: Access sessions, file transfers, and approval actions are comprehensively logged, supporting a robust audit trail that allows for the rapid identification of responsible parties in the event of a security incident.
3. Improved organizational awareness of security: Administrative processes such as access approvals and privilege reviews, along with user training, contribute to improving employees' awareness and compliance with security policies.

5.5. Comprehensive Analysis and Scalability

The proposed architecture's advantages over legacy security structures can be summarized in Table 7.

Table 7. Effectiveness of the proposed architecture.

Category	Conventional Security Structure	Proposed Model	Expected Benefits
EoSL systems	Unprotected	Policy-based access control enabled	Minimized risk of compromise
Ransomware propagation	Limited full internal network exposure	Centralized SMB control via gateway	Effectively eliminates lateral spread risk
Anomaly detection	Incapable of detection	Log-based detection within hours	Significant reduction in detection time
File sharing	Numerous unauthorized shares	Approval- and log-based structure	Traceability of misuse and leakage
Asset management	Manual tracking	Automated identification and classification	Improved management efficiency

Furthermore, this study presents several directions for future scalability.

1. Development of industry-specific ZTA (e.g., semiconductor, automotive, and precision manufacturing sectors).
2. Expansion into a unified security architecture covering both cloud and IT assets.

6. Validation

6.1. Simulation Method and Scenarios

In this study, a Python-based simulation was conducted to verify the effectiveness of the proposed security architecture. This architecture consists of two components: the enhanced control system within OT and the SMB gateway-based perimeter security.

The practical challenges associated with conducting experiments involving the propagation of malware, including EoSL equipment, can be attributed to the following constraints:

1. Recent hypervisors and virtualization platforms have been observed to demonstrate low kernel and driver compatibility with end-of-support operating systems. Consequently, the normal operation in VM environments cannot be guaranteed.
2. It is important to note that empirical research in the field of malware may potentially incur risks with regard to the prevailing principles of research ethics and the regulations governing industrial control network security.

Accordingly, the present study modeled the lateral movement and boundary spread of malware by quantifying factors such as OT asset vulnerability (EoSL), high-risk assets (Critical Node), and policy strength (Posture Level) as variables, thereby presenting them as a practical alternative.

The verification consists of the following two scenarios:

1. Scenario 1: Evaluation of the effectiveness of internal OT controls in suppressing lateral malware propagation.
2. Scenario 2: Evaluation of the combined impact of SMB gateway boundary protection and internal propagation when the gateway fails to detect malicious activity.

6.2. Scenario 1—Validation of Malware Suppression by OT Internal Control

6.2.1. Objective

The objective of Scenario 1 is to strengthen the security of OT internal endpoints by enforcing file transfer control, and to quantitatively evaluate the extent to which such control can suppress the lateral propagation of ransomware and other malware within the OT environment.

6.2.2. Simulation Environment Configuration

The simulation was implemented using SimPy, an event-driven Python framework (Python 3.13.9, Python Software Foundation, Wilmington, DE, USA). Each node was modeled as an asynchronous agent that independently performs infection, detection, isolation, and recovery events. Scenario 1 (EoSL Defense Impact Simulation) was conducted on an industrial network consisting of 1000 nodes over a period of 60 min (3600 s). The defense level of EoSL nodes was incrementally increased to 20%, 40%, 60%, and 80% to analyze the effectiveness of infection suppression. The main simulation parameters are summarized in Table 8.

Table 8. Key simulation parameters for Scenario 1.

Item	Symbol/Value	Description
Total number of nodes	$N = 1000$	Total nodes in the simulation environment.
EoSL ratio	$P_{\text{EoSL}} = 0.60$	Proportion of end-of-support (EoSL) assets ($n = 600$).
Non-EoSL ratio	$1 - P_{\text{EoSL}} = 0.40$	Proportion of up-to-date managed assets ($n = 400$).
Critical asset ratio	$P_{\text{Critical}} = 0.20$ ¹	Ratio of critical assets (e.g., PLC, MES, HMI; $n = 200$).
Simulation time	$T = 3600$ s	Observation period (60 min) ² .
Initial infection source	1 EoSL node	Attack initiated from a randomly selected EoSL node.
Attack attempt rate	$\lambda = 0.1$ attempts/s	Average attack attempt rate per infected node (one attempt every 10 s).
Infectious delay	$t_{\text{inf_delay}} = 60$ s	Delay before an infected node can propagate infection (1 min).

Table 8. Cont.

Item	Symbol/Value	Description
Detection rate	$P_{\text{detect}} = 0.90$	Probability of detecting infection (horizontal movement detection in monitored OT network).
Detection delay	$t_{\text{detect}} \in [2, 10]$ s	Random delay range until detection event occurs.
Isolation delay	$t_{\text{isolate}} = 3$ s	Average delay from detection to isolation.
Mean time to recovery	MTTR = 900 s	Average time to recovery after isolation (15 min).
Baseline defense (Non-EoSL)	$p_{\text{non_eosl}} = 0.98$	Fixed defense probability of Non-EoSL nodes.
Recovery policy (Non-EoSL)	Reinforced reinjection ($\times 1.5$, capped at 0.99)	Reintroduced with strengthened defense after recovery.
Recovery policy (EoSL)	Remain offline	EoSL nodes are not reintroduced within the simulation period.
Defense posture level	$P_{\text{posture}} = \{0.20, 0.40, 0.60, 0.80\}$	Defense-level variation scenarios for EoSL nodes.
Repetitions per level	20 runs/level	Average and standard deviation reported after 20 iterations per level ³ .

¹ Critical assets are assigned a $1.2\times$ defense weighting (up to 100%) to reflect higher protection priority.

² Simulation termination occurs when any of the following conditions are met: (i) time T is reached, (ii) no more nodes can be infected, or (iii) propagation stagnation (no new infections after 5000 consecutive attack attempts).

³ Key performance indicators include R_{Block} (blocking rate), $N_{\text{Infected_Total}}$, $N_{\text{Infected_EoSL}}$, $N_{\text{Infected_NonEoSL}}$, $N_{\text{Infected_Critical}}$, MTTD, and MTTR.

6.2.3. Algorithm

Algorithm 1 is the algorithm used to validate Scenario 1.

Algorithm 1 EoSL vs. Non-EoSL malware defense simulation.

```

1: Input:  $N = 1000$  nodes,  $P_{\text{EoSL}} = 0.6$ ,  $P_{\text{Critical}} = 0.2$ ,  $T = 3600$  s,  $\lambda = 0.1/\text{s}$ ,  $t_{\text{inf\_delay}} = 60$  s
2:
3: Initialization
4: for each node  $i \in [1, N]$  do
5:   Assign EoSL status ( $p_{\text{base}} = P_{\text{posture}}$ ) or Non-EoSL ( $p_{\text{base}} = 0.98$ )
6:   Assign Critical status (adds  $1.2\times$  defense multiplier)
7: end for
8: Infect one random EoSL node at  $t = 0$ 
9:
10: Infection Spread Loop
11:  $t \leftarrow 0$ 
12: while  $t < T$  and active infections exist do
13:   Find active_infected = {nodes infected, not isolated,  $\geq t_{\text{inf\_delay}}$  elapsed}
14:   if active_infected =  $\emptyset$  then
15:      $t \leftarrow t + 60$ ; continue
16:   end if
17:
18:    $\delta \sim \text{Exp}(\lambda \times |\text{active\_infected}|)$ ;  $t \leftarrow t + \delta$ 
19:   Select random source  $\in$  active_infected, target  $\in$  uninfected
20:
21:    $p_{\text{def}} \leftarrow p_{\text{base}}[\text{target}] \times (1.2 \text{ if Critical else } 1.0)$ 
22:   if Uniform(0,1) <  $p_{\text{def}}$  then
23:     continue // Attack blocked
24:   end if
25:
26:   Infection Success
27:   Mark target as infected; Record infection metrics
28:
29:   if Uniform(0,1) < 0.9 then // Detect SOURCE attack behavior
30:      $t_{\text{detect}} \leftarrow t + \text{Uniform}(2, 10)$ 
31:      $t_{\text{isolate}} \leftarrow t_{\text{detect}} + 3$  // Detect + isolate delay
32:     Schedule isolation at  $t_{\text{isolate}}$  (record MTTD =  $t_{\text{detect}} - t_{\text{infect}}$ )
33:     Schedule recovery at  $t_{\text{isolate}} + \text{Exp}(900)$  (record MTTR =  $t_{\text{recover}} - t_{\text{infect}}$ )
34:     At recovery time: EoSL nodes stay offline; Non-EoSL harden and return ( $p_{\text{base}} \times 1.5$ , capped at 0.99)
35:   end if
36: end while
37:
38: Output: Infection rates (Total, EoSL, Non-EoSL, Critical), MTTD, MTTR

```

6.2.4. Evaluation Metrics

To evaluate the effectiveness of the proposed defense model, several quantitative metrics were defined. Table 9 summarizes the formulas and descriptions of these evaluation metrics.

Table 9. Definition of evaluation metrics for Scenario 1.

Metric	Formula	Description
Blocking rate	$R_{\text{Block}} = \left(1 - \frac{N_{\text{success}}}{N_{\text{attempt}}}\right) \times 100$	Percentage of attacks successfully blocked (%).
Total infection rate ¹	$R_{\text{Infected}} = \frac{N_{\text{infected, total}}}{N} \times 100$	Cumulative proportion of infected nodes among all nodes.
EoSL infection rate ²	$R_{\text{EoSL}} = \frac{N_{\text{infected, EoSL}}}{N_{\text{EoSL}}} \times 100$	Cumulative proportion of infected EoSL nodes.
Non-EoSL infection rate ²	$R_{\text{NonEoSL}} = \frac{N_{\text{infected, NonEoSL}}}{N_{\text{NonEoSL}}} \times 100$	Cumulative proportion of infected Non-EoSL nodes.
Critical asset infection rate ²	$R_{\text{Critical}} = \frac{N_{\text{infected, Critical}}}{N_{\text{Critical}}} \times 100$	Cumulative infection rate of production-critical assets.
Mean time to detect ³	$\text{MTTD} = \text{mean}(t_{\text{detect}} - t_{\text{infect}})$	Average delay between infection and detection (s).
Mean time to recovery	$\text{MTTR} = \text{mean}(t_{\text{recover}} - t_{\text{infect}})$	Average time from infection to full recovery (s).

¹ All infection rates represent cumulative ratios based on uniquely infected nodes during the simulation period.

² N denotes the total number of nodes, while N_{EoSL} , N_{NonEoSL} , and N_{Critical} represent the number of nodes for each respective category. ³ MTTD is calculated only for nodes where detection occurred, measured as the average delay from infection to detection time.

6.2.5. Summary of Results

According to the simulation results ($T = 3600$ s, $N = 20$), as the defense level of EoSL nodes was gradually increased from 20% to 80%, both the overall infection rate and the infection rate of critical assets decreased significantly. The key findings are as follows:

- Reduction in overall infection rate: When the defense level was 20%, the average infection rate across all nodes was $78.51\% \pm 3.95\%$. As the defense level increased to 80%, it dropped to $22.91\% \pm 13.87\%$, representing a reduction of approximately 70%. This demonstrates a substantial suppression of network-wide malware propagation.
- Protection of critical assets: The infection rate of production and control layer assets (R_{Critical}) decreased from $59.66\% \pm 3.88\%$ at 20% defense to $7.32\% \pm 6.31\%$ at 80%, indicating an improvement of roughly 88%. This result suggests that limited security investments can be highly effective when strategically focused on high-value or mission-critical nodes.
- Penetration attempts and blocking efficiency: The overall blocking rate (R_{Block}) remained above 90% across all levels; however, lower defense levels resulted in higher penetration success rates. Even at 80% defense, the penetration success rate was $8.91\% \pm 5.16\%$, but the resulting infection spread was minor, leading to limited overall impact.
- Detection and recovery performance: The mean time to detect (MTTD) remained stable at approximately 6 s, while recovery efficiency improved as the defense level increased. Specifically, the mean time to recovery (MTTR) decreased by about 25%, from 682.8 s at 20% defense to 515.5 s at 80%.

In summary, the increase in defense level not only suppressed infection propagation but also improved the efficiency of recovery processes. The quantitative outcomes of these observations are summarized in Table 10. Based on these findings, the following practical implications can be drawn:

1. Necessity of single-point isolation policies for EoSL assets: The sharp decline in both overall and critical asset infection rates at the 80% defense level supports the validity

of a security architecture that enforces single-point connectivity through policy-based gateways (e.g., SMB gateway). For legacy assets that are difficult to replace, such boundary enforcement serves as a key structural factor in mitigating systemic risks within OT environments.

2. Complementarity between detection–recovery processes and defense policies: At lower defense levels, rapid detection and recovery alone were insufficient to suppress propagation. However, when combined with strengthened defense policies, infection spread was reduced by over 70%. This demonstrates that the integrated operation of defensive postures and response mechanisms is essential for RMF-based risk mitigation.

Table 10. Summary of Scenario 1 results (mean $\pm$ standard deviation, $N = 20$).

EoSL Defense (%)	R_{Block} (%)	R_{Critical} (%)	R_{Infected} (%)	Success/Attempt (%)	Isolated	MTTD (s)	MTTR (s)
20	94.91 $\pm$ 0.95	59.66 $\pm$ 3.88	78.51 $\pm$ 3.95	4.90 $\pm$ 0.28	728 $\pm$ 40	6.05 $\pm$ 0.03	682.80 $\pm$ 45.69
40	93.80 $\pm$ 2.23	60.94 $\pm$ 2.76	76.89 $\pm$ 4.46	5.66 $\pm$ 0.38	709 $\pm$ 47	6.02 $\pm$ 0.04	633.54 $\pm$ 58.95
60	91.15 $\pm$ 4.76	53.38 $\pm$ 12.87	66.20 $\pm$ 15.50	6.68 $\pm$ 1.54	601 $\pm$ 142	6.01 $\pm$ 0.05	558.43 $\pm$ 59.90
80	90.58 $\pm$ 0.85	7.32 $\pm$ 6.31	22.91 $\pm$ 13.87	8.91 $\pm$ 5.16	207 $\pm$ 125	5.98 $\pm$ 0.12	515.52 $\pm$ 89.97

Each value represents the mean $\pm$ standard deviation from 20 repeated simulation runs using identical parameter settings. R_{Infected} denotes the cumulative infection ratio among all nodes, R_{Critical} indicates the infection ratio of critical production assets, and Success/Attempt (%) represents the overall penetration success rate across all attack attempts. MTTD refers to the mean time to detection (from infection to detection event), and MTTR represents the mean time to recovery (from infection to full restoration).

6.3. Scenario 2—Validation of Boundary Protection Effectiveness Based on SMB Gateway

6.3.1. Objective

This scenario proposes an SMB gateway architecture that enables secure file transfer operations within the OT environment, where file exchanges are often inevitable for production efficiency and essential operations. The proposed gateway is designed to inspect and block malicious payloads during file transfer while minimizing the impact on legitimate file delivery and operational continuity. In this study, the detection performance of the gateway (e.g., True Positive Rate and False Positive Rate) and its inspection latency are quantitatively evaluated through simulation to analyze their impact on the infiltration of malware into the OT network and its subsequent lateral propagation.

This scenario is guided by the following research question:

“The SMB gateway is equipped with an APT detection solution that identifies malicious or abnormal files during file transfers. Given a realistic detection performance level of the APT solution, to what extent can the SMB gateway reduce the inflow of malware into the OT network, and if undetected malware bypasses the gateway, how extensively can it propagate within the OT environment (Scenario 1)?”

The objective of this scenario is to evaluate the boundary-blocking effectiveness of the SMB gateway and to quantitatively analyze the extent of potential damage propagation when malicious files infiltrate the OT network due to gateway detection failures.

6.3.2. Simulation Environment Configuration

This scenario assumes a dual-threat model in which malicious external files enter the OT network via an SMB gateway and subsequently propagate through internal EoSL nodes. All file transfers are forced to pass through the gateway, which determines maliciousness using an embedded APT detection engine.

The detection engine is modeled with realistic operating characteristics and the following performance metrics:

- True Positive Rate (TPR): The proportion of malicious files correctly detected and blocked.
- False Positive Rate (FPR): The proportion of benign files incorrectly classified and blocked.

File inspection at the gateway incurs an average delay of G_{LATENCY} seconds, representing a trade-off between operational efficiency and security. Malicious files that bypass the gateway are treated as infection seeds, and the internal propagation and recovery processes follow the same procedures as in Scenario 1. The key parameters used in this boundary-only evaluation are summarized in Table 11.

Table 11. Key simulation parameters for Scenario 2 (boundary-only performance evaluation).

Item	Symbol/Value	Description
Network size/composition	$N = 1000$, EoSL 60%, Critical 20%	Node composition ratios in the simulated network.
File transfer rate	$\lambda_f = 0.2 \text{ s}^{-1}$	Frequency of external $\rightarrow$ OT file transfers.
Malicious file proportion	$p_{\text{mal}} = 0.10$	Fraction of transferred files that are malicious.
gateway detection rate	$G_{\text{TPR}} \in \{60, 80, 90, 98\}\%$	Sensitivity of the gateway in detecting (and blocking) malicious files.
gateway false positive rate	$G_{\text{FPR}} = 2.0\%$ (fixed)	Rate at which benign files are incorrectly blocked.
File inspection latency	$G_{\text{LATENCY}} = 0.2 \text{ s}$	Average processing delay introduced by the gateway.
Internal propagation mode	Inactive ($\lambda_{\text{int}} = 0$)	Only seed infections occur; lateral movement is not modeled in this boundary-only evaluation.
EoSL defense posture	$P_{\text{posture}} \in \{20, 40, 60, 80\}\%$	Defense-level weighting for EoSL nodes (applied as in Scenario 1).

6.3.3. Algorithm

Scenario 2 represents a multi-layered defense model that integrates boundary protection via the SMB gateway with internal malware propagation. Files arriving from external sources at an average interval of λ_f^{-1} seconds pass through the gateway inspection process, which is parameterized by the True Positive Rate (G_{TPR}), False Positive Rate (G_{FPR}), and inspection latency (G_{LATENCY}). If a malicious file is not detected by the gateway, it is delivered into the OT network and subsequently activates the internal propagation algorithm defined in Scenario 1.

The blocking rate of the gateway is defined as

$$R_{\text{Block,gateway}} = \left(1 - \frac{\text{Delivered}_{\text{mal}}}{\text{Total}_{\text{mal}}}\right) \times 100,$$

where $\text{Delivered}_{\text{mal}}$ denotes the number of malicious files delivered to the OT network, and $\text{Total}_{\text{mal}}$ represents the total number of malicious files attempted. Malicious files that bypass the gateway trigger internal infections, from which the number of infection cases $N_{\text{Infections,gateway}}$ and the infection rate of critical production assets $R_{\text{Success,Critical}}$ are measured. For each parameter combination, the simulation is repeated 10 times, and the mean and standard deviation are calculated to quantitatively analyze how the gateway's detection performance (G_{TPR} , G_{FPR}) and internal defense level (P_{posture}) interact to influence the overall damage scale.

The algorithm used to validate Scenario 2 is described in Algorithm 2.

Algorithm 2 SMB gateway + Internal Defense Layered Security.

```

1: Input:  $N$  nodes, gateway(TPR, FPR), File rate  $\lambda_f$ ,  $p_{\text{mal}}$ , Internal( $\lambda$ ,  $p_{\text{detect}}$ ,  $t_{\text{inf\_delay}}$ )
2:
3: Initialization
4: Initialize nodes with EoSL/Non-EoSL defense, Critical status
5: infected_ids  $\leftarrow \emptyset$ , uninfected_ids  $\leftarrow \{1, \dots, N\}$ 
6:
7: Concurrent Processes:
8:
9: Process A: gateway (Boundary Defense)
10: while  $t < T$  do
11:   Draw  $M \sim \text{Bernoulli}(p_{\text{mal}})$   $\triangleright M=1$  if malicious
12:   Draw  $\Delta t \sim \text{Exp}(\lambda_f)$ ;  $t \leftarrow t + \Delta t$ 
13:   Wait  $G_{\text{LATENCY}}$   $\triangleright$  gateway inspection delay
14:   if  $M = 1$  then
15:     Draw  $B \sim \text{Bernoulli}(G_{\text{TPR}})$   $\triangleright B=1$  means blocked
16:   else
17:     Draw  $B \sim \text{Bernoulli}(G_{\text{FPR}})$ 
18:   end if
19:   if  $(B = 0) \wedge (M = 1)$  then
20:     Seed infection: randomly infect one uninfected node
21:   end if
22: end while
23:
24: Process B: Internal Spread (Lateral Movement)
25: while  $t < T$  do
26:   active_infected  $\leftarrow \{\text{infected, not isolated, } \geq t_{\text{inf\_delay}} \text{ elapsed}\}$ 
27:   if active_infected =  $\emptyset$  or uninfected_ids =  $\emptyset$  then
28:     Skip or break
29:   end if
30:   Next attack:  $\delta \sim \text{Exp}(\lambda \times |\text{active\_infected}|)$ ,  $t \leftarrow t + \delta$ 
31:   Select random source  $\in$  active_infected, target  $\in$  uninfected_ids
32:    $p_{\text{def}} \leftarrow p_{\text{base}}[\text{target}] \times (1.2 \text{ if Critical})$ 
33:   if Uniform(0,1)  $< p_{\text{def}}$  then
34:     continue // Blocked
35:   end if
36:   Infect target; Update infected_ids, uninfected_ids
37:   if Uniform(0,1)  $< p_{\text{detect}}$  then
38:     Isolate SOURCE at  $t + \text{Uniform}(2,10) + 3$ 
39:     Recover at  $t + \text{Exp}(900)$ : EoSL offline, Non-EoSL harden & return
40:   end if
41: end while
42:
43: Output: gateway blocks, Internal infection rates (Total, Critical, EoSL), MTTD, MTTR

```

6.3.4. Evaluation Metrics

The performance of the boundary simulation was quantitatively assessed using multiple detection, blocking, and infection-related indicators. Table 12 summarizes the definitions and measurement formulas of these evaluation metrics.

Table 12. Evaluation metrics for Scenario 2 (definitions and units).

Metric	Formula/Definition	Description (Unit)
gateway TPR	$\text{TPR} = \frac{\text{TP}}{\text{TP} + \text{FN}} \times 100$	Detection (blocking) sensitivity for malicious files (%).
gateway FPR	$\text{FPR} = \frac{\text{FP}}{\text{FP} + \text{TN}} \times 100$	False alarm rate for benign files (%).
gateway blocking rate (log-based)	$R_{\text{Block,gateway}} = \left(1 - \frac{\text{Delivered}_{\text{mal}}}{\text{Total}_{\text{mal}}}\right) \times 100$	Empirical blocking efficiency ($=1 - \text{inflow ratio}$), directly derived from simulation logs (%).

Table 12. Cont.

Metric	Formula/Definition	Description (Unit)
Malware delivered via gateway	$GW_Deliv_Mal = Delivered_{mal}$	Number of malicious files that passed through the boundary and entered the OT network (count).
Seed infections via gateway	$GW_Seed_Inf = N_{seed}$	Initial infection instances triggered immediately after gateway infiltration (count). ¹
Total infection rate	$R_{TotalInf} = \frac{N_{infected,total}}{N} \times 100$	Cumulative infection ratio across the entire OT network including internal propagation (%).
EoSL infection rate	$R_{EoSL} = \frac{N_{infected,EoSL}}{N_{EoSL}} \times 100$	Cumulative infection ratio among EoSL assets (%).
Critical asset infection rate	$R_{Critical} = \frac{N_{infected,Critical}}{N_{Critical}} \times 100$	Cumulative infection ratio among critical production assets (%).
Internal blocking rate	$R_{Block,Internal} = \left(1 - \frac{N_{success,int}}{N_{attempt,int}}\right) \times 100$	Rate of lateral-movement suppression achieved by internal detection and isolation processes (%).
Average file-processing latency	$\bar{L} = \text{mean}(t_{deliver} - t_{sent})$	Average delay introduced by gateway inspection (s).
Operational cost of false positives (optional)	$C_{FPR} = FP \cdot c_{review}$	False-positive handling cost (count $\times$ cost per review); used for policy evaluation (e.g., KRW/min).

¹ In this simulation, each malicious file that bypasses the gateway is modeled to generate one seed infection, resulting in $GW_Seed_Inf \simeq GW_Deliv_Mal$. Future work can extend this model by incorporating host-level security and user-behavioral factors so that $GW_Seed_Inf \leq GW_Deliv_Mal$.

6.3.5. Summary of Results

The simulation results consistently demonstrate that as the gateway detection performance (GW TPR) increases, both the number of malicious files delivered to the OT network (GW Deliv Mal) and the resulting overall infections (Total Inf) decrease sharply. For example, when the EoSL defense level is 20% and GW TPR is 60%, the number of delivered malicious files is 30.9 (per network), resulting in Total Inf = 3.09%. However, when GW TPR improves to 98% under the same EoSL condition, the number of delivered files drops to 0.8, and Total Inf decreases to 0.08%. In addition, most parameter combinations report an internal blocking (Int Block) rate of 0%, indicating that, within this experimental setup, the gateway's blocking performance functions as the dominant factor in mitigating internal damage.

The simulation findings regarding the deployment of the SMB gateway suggest the following practical implications:

1. Prioritizing the enhancement of SMB gateway performance: Improvements in GW TPR directly reduce the number of initial infection seeds (malicious files) entering the OT environment, leading to a substantial decrease in overall damage. For instance, in an EoSL 20% environment, increasing GW TPR from 60% to 98% reduced Total Inf from 3.09% to 0.08%, representing approximately a 97% reduction. This demonstrates that strengthening boundary detection capability is the most immediate and effective investment area for damage reduction.
2. Complementarity with internal defense posture: Higher internal defense levels (EoSL Def) show a marginal reduction in infection rates under the same GW performance. However, the overall mitigation effect is primarily governed by improvements in gateway detection accuracy. Thus, while reinforcing internal asset security in parallel remains important, prioritizing boundary detection enhancement is more cost effective for risk reduction.
3. Monitoring of critical parameter regions: In configurations where GW TPR ranges between 60–80% and internal defenses are weak (EoSL 20–60%), even a small number of undetected malicious files can rapidly propagate within the OT network, resulting in noticeable damage. This range can be defined as a critical region, requiring proactive

mitigation measures such as enhanced network segmentation and the prioritized replacement of critical assets.

The quantitative outcomes of the boundary simulation, according to the EoSL defense level and gateway detection performance, are summarized in Table 13.

Table 13. Summary of Scenario 2 simulation results. (Representative values according to EoSL defense level and gateway detection performance, all values are derived from simulation results.)

EoSL Defense (%)	GW TPR (%)	GW Block (%)	GW Deliv Mal ¹	GW Seed Infections ¹	Int Block (%)	Total Inf (%)	Critical Inf (%)	EoSL Inf (%)	GW FPR (%)
20	60	58.96	30.9	30.9	0.00	3.09	3.22	2.90	1.90
20	80	78.46	14.4	14.4	0.00	1.44	1.76	1.36	1.74
20	90	90.48	6.8	6.8	0.00	0.68	0.67	0.64	1.98
20	98	98.80	0.8	0.8	0.00	0.08	0.05	0.10	2.19
40	60	58.89	28.8	28.8	0.00	2.88	2.68	2.60	1.96
40	80	80.76	12.9	12.9	0.00	1.29	1.52	1.12	1.87
40	90	88.69	7.5	7.5	0.00	0.75	0.63	0.69	2.12
40	98	98.75	0.8	0.8	0.00	0.08	0.05	0.10	1.92
60	60	59.30	28.0	28.0	0.00	2.80	2.62	2.62	2.43
60	80	80.53	13.4	13.4	0.00	1.34	1.29	1.56	1.74
60	90	90.37	6.7	6.7	0.00	0.67	0.85	0.77	2.11
60	98	98.74	0.8	0.8	0.00	0.08	0.14	0.05	1.96
80	60	60.54	26.5	26.5	0.00	2.65	2.66	2.58	1.74
80	80	79.11	14.6	14.6	0.00	1.46	1.13	1.44	2.14
80	90	90.88	6.4	6.4	0.00	0.64	0.45	0.52	1.84
80	98	98.45	1.0	1.0	0.00	0.10	0.00	0.07	2.22

¹ Terminology: GW Deliv Mal/GW Seed Inf denote the number of malicious files delivered through the gateway and the corresponding initial seed infections. Metrics such as Total Inf (%) represent percentages relative to the total network size ($N = 1000$ nodes).

6.4. Integrated Result Analysis

A comprehensive analysis of the simulation results confirms that enhancing the internal security level of the OT environment alone has limited effectiveness in suppressing overall threats. Substantial defensive efficacy is achieved only when boundary protection mechanisms that block external threat vectors are implemented in parallel.

In Scenario 1 (EoSL Defense Impact Simulation), strengthening the defense level of EoSL nodes from 20% to 80% reduced the overall infection rate from 78.51% to 22.91%, corresponding to an approximately 70% threat-suppression effect. The infection rate of critical production and control assets decreased from 59.66% to 7.32%, achieving roughly an 88% reduction in damage. These results demonstrate that hardening internal assets can significantly slow the rate of infection propagation; however, under conditions where malicious traffic continuously enters from external sources, complete isolation remains difficult to achieve.

In Scenario 2 (SMB gateway Defense Simulation), improving the gateway's detection rate (True Positive Rate, TPR) from 60% to 98% reduced the proportion of malicious files delivered into the OT network from 3.09% to 0.08%, indicating an additional suppression effect of approximately 97%. This reduction directly results from minimizing the entry of external threats, thereby fundamentally lowering the potential for internal lateral spread. The findings verify the complementary relationship between internal hardening and boundary-level control.

By integrating the results of both scenarios, the cumulative threat-suppression rate achieved when combining internal defense enhancement (EoSL hardening) with gateway-based boundary protection can be calculated as follows:

$$1 - (1 - 0.708) \times (1 - 0.974) \approx 0.992$$

This corresponds to approximately 99% overall threat suppression and 98% protection of critical assets, quantitatively demonstrating that the proposed layered security architecture can achieve both high scalability and resilience across large-scale OT environments.

7. Limitations and Considerations

7.1. Technical Limitations

1. Limited detection accuracy in agentless environments: This study proposes a lightweight model that focuses on network-based identification and access control, but when it comes to advanced persistent threats (APTs), additional endpoint solutions such as endpoint detection and response (EDR) or host-based intrusion detection systems (HIDS) may be required to help the SMB gateway fulfill its role more effectively in behavior-based detection.
2. Difficulty in identifying non-networked assets: There are structural limitations when applying asset management and security policies to standalone devices that are not connected to a network.

7.2. Organizational and Operational Considerations

1. Operator acceptance and differences in security awareness: ZT requires a change in organizational philosophy and security culture. Therefore, managers and field operators may perceive new requirements such as access authorization, strict access control, and multi-factor authentication as burdensome or disruptive to existing workflows.
2. Policy design and administrative overhead: Implementing PBAC requires a granular definition of permissions by assets and users. This requires collaboration between the IT and security teams and operational units, particularly during the initial design phase. Small- and medium-sized manufacturers may face additional challenges due to a lack of dedicated security personnel.
3. Need for balance between security and productivity: While improving security, there is a risk that overly stringent authentication or file-sharing approval processes may hinder operational efficiency. Therefore, designing policies that strike an appropriate balance between security and workflow performance is critical.

7.3. Policy and Regulatory Considerations

1. Low priority for enforcement due to the lack of legal obligations: Most production systems are currently not subject to mandatory cybersecurity requirements under existing regulations. As a result, security investments are often deprioritized at the executive level in favor of immediate operational concerns.
2. Lack of standardized guidelines for ZT in OT environments: Although ZT is increasingly adopted across sectors, a standardized architecture that specifically addresses the unique requirements of OT environments remains underdeveloped. International standardization initiatives are in progress; however, domain-specific implementation guidelines remain scarce.

The proposed security architecture must overcome various technical and organizational challenges during implementation. In particular, initial tasks such as asset identification, access policy definition, and approval workflow design can be burdensome. Therefore, effective change management strategies are essential to support user adaptation and ensure the successful adoption of enhanced security measures.

7.4. Future Considerations

While this study suggests the feasibility of a ZTA tailored for legacy manufacturing systems, further research is required to enhance its rigor and practical applicability. Several concrete directions are identified based on the findings of this work.

First, future studies should focus on advancing the technical maturity of the proposed architecture by integrating intelligent monitoring and forensic readiness mechanisms. For instance, logs from the SMB gateway, records from the Access Approver, and MFA authentication traces can be systematically correlated through advanced analytics or learning-based approaches to enhance situational awareness and traceability. Such integration would not only improve incident investigation efficiency but also contribute to proactive threat detection and continuous assurance. Furthermore, recent studies on Age of Information (AoI) have highlighted the importance of maintaining temporal freshness in data-driven decision processes [18,19]. Incorporating such concepts into OT data collection and policy evaluation cycles could further enhance the responsiveness and resilience of legacy environments.

Second, instead of performing a full proof-of-concept—which is infeasible due to the difficulty of reconstructing End-of-Service-Life (EoSL) operating systems—the study will proceed with limited pilot implementations at Plant A and Plant B. These pilots will evaluate its deployability, policy-enforcement efficiency, and operational impact of the proposed Zero Trust Architecture under real manufacturing conditions.

Third, the framework will be expanded across multiple international standards, including IEC 62443 [20] (zones, conduits, and security levels) and ISO/IEC 27001 [21] OT profiles, to ensure broader interoperability and applicability beyond the NIST CSF 2.0 perspective.

Fourth, as wireless and mobile technologies become increasingly integrated into manufacturing systems, the potential exposure to traffic- and RF-based side-channel threats is expected to rise. Recent studies [22,23] have demonstrated how encrypted or ambient wireless signals can inadvertently reveal application-level behaviors and user activities through advanced fingerprinting or energy-harvesting-based inference techniques. Although these works primarily focus on mobile and open-world contexts, they highlight emerging risks that should be considered as OT environments increasingly adopt wireless connectivity and portable maintenance devices. Future research should therefore examine detection and mitigation strategies to ensure that Zero Trust principles and forensic readiness mechanisms remain effective across hybrid wired–wireless industrial networks.

Finally, future work will explore the integration of Security Orchestration, Automation and Response (SOAR) capabilities within the proposed model. This includes defining adaptive automation thresholds, safe-mode fallback mechanisms, and human-in-the-loop escalation policies to enhance operational resilience and automated defense coordination in manufacturing environments.

8. Conclusions

This study proposes a method for enhancing security in legacy manufacturing environments—where applying security patches and replacing systems are often difficult—through the application of ZTA. We designed a comprehensive architecture that integrates asset-centric protection, PBAC, centralized file transfer control, behavior-based monitoring, and the process-oriented management controls.

The main contributions of this study are as follows:

1. We propose a ZTA specifically designed for manufacturing environments, considering constraints such as the use of End-of-Support-Life (EoSL) systems and the need for continuous operations.

2. We introduce a risk-based asset identification and classification scheme that combines automatic network-based detection with user-provided metadata, thereby defining protection policies based on risk priorities.
3. We strengthen file-sharing security by applying a centrally managed SMB gateway architecture, thereby mitigating risks such as ransomware proliferation, unauthorized data leakage, and authentication bypass.
4. To support sustainable enterprise-wide security management, we integrate technical and administrative security operations—including identity verification, access authorization, log management, and user training—into a unified governance framework.

In conclusion, this study suggests that ZTA can provide a practical framework to improve the security of legacy manufacturing environments. It offers a foundational basis upon which ZTA can evolve into an operational standard for industrial cybersecurity, while recognizing that further empirical validation is required.

Author Contributions: Conceptualization, writing—original draft, methodology, project administration, C.-H.M.; writing—review and editing, validation, D.-H.K. and H.Y.; supervision, funding acquisition, J.K. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by Electronics and Telecommunications Research Institute(ETRI) grant funded by ICT R&D program of MSIT/IITP[RS-2024-00438597, Development of an Automation Tools for Compliance Assessment of Defense Cyber Security Risk Management Framework], and supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No.RS-2024-00400302, Development of Cloud Deep Defense Security Framework Technology for a Safe Cloud Native Environment).

Data Availability Statement: The plant-level OS distribution data are not publicly available due to confidentiality agreements but are available from the corresponding author upon reasonable request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. *NIST SP 800-207; Zero Trust Architecture*; National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2020. [CrossRef]
2. National Institute of Standards and Technology. *NIST CSWP 29; The NIST Cybersecurity Framework (CSF) 2.0*; National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2024. [CrossRef]
3. Shimazu, T. Cyberattack That Halted Toyota's Factories Exposes Supply Chain Attack Risks. 2022. Available online: <https://xtech.nikkei.com/atcl/nxt/mag/nc/18/092400133/030900072/> (accessed on 16 June 2025).
4. Kardon, S. Florida Water Treatment Plant Hit with Cyber Attack. 2023. Available online: <https://www.industrialdefender.com/blog/florida-water-treatment-plant-cyber-attack> (accessed on 16 June 2025).
5. Goud, N. Olympus Suffers Another Ransomware Attack Within a Month. 2021. Available online: <https://www.cybersecurity-insiders.com/olympus-suffers-another-ransomware-attack-within-a-month/> (accessed on 16 June 2025).
6. Morales, C. Cyber Security Incident Forced Shutdowns, Financial Losses. 2018. Available online: <https://www.mbtmag.com/home/blog/21102105/cyber-security-incident-forced-shutdowns-financial-losses> (accessed on 16 June 2025).
7. Lim, G.N. Manufacturing Security Response Strategy. 2023. Available online: <https://automation-world.co.kr/news/article.html?no=66289> (accessed on 16 June 2025).
8. Klinghammer, L. 10 Strategies for Securing Your Operational Technology (OT). 2023. Available online: <https://dxc.com/us/en/insights/perspectives/paper/the-other-cybersecurity-10-strategies-for-securing-your-operational-technology-ot> (accessed on 16 June 2025).
9. Won, B.C. 2024 OT Security Report: OT Security Stirs—A Signal Flare for Full-Scale Activation. 2024. Available online: <https://m.boannews.com/html/detail.html?idx=127211> (accessed on 16 June 2025).
10. Staniszewski, M. Addressing Cybersecurity Risks in Legacy OT Systems: A Practical Guide. 2024. Available online: <https://gca.isa.org/blog/addressing-cybersecurity-risks-in-legacy-ot-systems-a-practical-guide> (accessed on 16 June 2025).
11. Paul, B.; Rao, M. Zero-Trust Model for Smart Manufacturing Industry. *Appl. Sci.* **2023**, *13*, 221. [CrossRef]
12. Garey, L. What Is Zero Trust Security. 2024. Available online: <https://www.oracle.com/security/what-is-zero-trust/> (accessed on 16 June 2025).

13. National Cyber Security Center. Zero Trust Architecture Design Principles. Available online: <https://www.ncsc.gov.uk/collection/zero-trust-architecture/assess-user-behaviour-service-and-device-health> (accessed 16 June 2025).
14. Allen, J.M. OS and Application Fingerprinting Techniques. 2007. Available online: <https://www.giac.org/paper/gsec/8496/os-application-fingerprinting-techniques/113048> (accessed on 16 June 2025).
15. VanKirk, B. 2025 Cyber Threat Report. 2025. Available online: <https://www.sonicwall.com/resources/white-papers/2025-sonicwall-cyber-threat-report> (accessed 16 June 2025).
16. Rathnayake, D. SMB Protocol Explained: Understanding Its Security Risks and Best Practices. 2023. Available online: <https://www.tripwire.com/state-of-security/smb-protocol-explained-understanding-its-security-risks-and-best-practices> (accessed on 16 June 2025).
17. MSP360. System Image Backup and Recovery Explained. Available online: <https://www.msp360.com/resources/blog/image-backup-and-recovery> (accessed on 16 June 2025).
18. Ma, Y.; Ma, R.; Lin, Z.; Zhang, R.; Cai, Y.; Wu, W.; Wang, J. Improving Age of Information for Covert Communication with Time-Modulated Arrays. *IEEE Internet Things J.* **2025**, *12*, 1718–1731. [CrossRef]
19. Zhang, G.; Wei, X.; Tan, X.; Han, Z.; Zhang, G. AoI Minimization Based on Deep Reinforcement Learning and Matching Game for IoT Information Collection in SAGIN. *IEEE Trans. Commun.* **2025**, *73*, 5950–5964. [CrossRef]
20. IEC 62443; Industrial Communication Networks—Network and System Security. IEC: Geneva, Switzerland, 2018.
21. ISO/IEC 27001; Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements. ISO: Geneva, Switzerland, 2022.
22. Li, J.; Zhou, H.; Wu, S.; Luo, X.; Wang, T.; Zhan, X.; Ma, X. FOAP: Fine-Grained Open-World Android App Fingerprinting. In Proceedings of the 31st USENIX Security Symposium (USENIX Security 22), Boston, MA, USA, 10–12 August 2022; pp. 1579–1596.
23. Ni, T.; Lan, G.; Wang, J.; Zhao, Q.; Xu, W. Eavesdropping Mobile App Activity via Radio-Frequency Energy Harvesting. In Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23), Anaheim, CA, USA, 9–11 August 2023; pp. 3511–3528.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.