Applied Human Factors and Ergonomics (AHFE2025), Vol. 199, 2025, 2316–2325
https://doi.org/10.54941/ahfe1007044

Risk-Based Model for OT Security Technology Implementation and Segmentation

Hiroshi Sasaki[1,2] and Kenji Watanabe[1]

[1]Nagoya Institute of Technology, Gokiso-cho, Showa, Nagoya, Japan
[2]Manufacturing and Innovation DX Laboratory, Nagoya Institute of Technology, Gokiso-cho, Showa, Nagoya, Japan

ABSTRACT

As digital connectivity expands within factory systems and supply chains, cybersecurity risks have become increasingly critical. This study builds upon previous work that addressed governance and awareness gaps through OT (Operational Technology) risk assessment tools and workshops. It shifts focus to the "Technology" domain of OT security and proposes a practical, risk-based model to support technology selection and segmentation strategies in factories. A classification framework is introduced using two key dimensions: threat detection capability (known vs. unknown) and automation level of incident response. These axes define four technology models: X (manual response to known threats), X+ (automated response to known threats), Y (manual response to unknown threats), and Y+ (automated response to unknown threats). Each model is mapped to real-world security solutions such as antivirus software, Unified Threat Management (UTM) systems, OT-IDS (Intrusion Detection Systems for OT), application whitelisting and so on. These mappings help clarify which types of technologies align with various OT risk scenarios and operational priorities. The study also introduces a network segmentation strategy as a complementary technique to localize incidents and reduce business risk. By dividing factory networks into operational zones, it becomes possible to tailor security controls to each zone's criticality, supporting both scalability and cost-efficiency. This framework contributes to bridging the gap between abstract risk awareness and practical implementation. It also aligns technical countermeasures with business continuity goals, offering a scalable approach that supports security planning across a range of industrial maturity levels.

Keywords: Operational technology security, Risk-based cybersecurity design, Network segmentation strategy

INTRODUCTION

The rapid digitalization of manufacturing has delivered notable efficiency gains but has also exposed Operational Technology (OT) systems—originally designed for isolated, deterministic environments—to a growing spectrum of cyber threats. Modern OT is increasingly interconnected with Information Technology (IT) networks, cloud platforms, and external services to enable

functions such as predictive maintenance, remote operations, real-time production monitoring, and carbon footprint tracking.

However, this integration has amplified vulnerabilities. High-profile incidents, such as ransomware attacks that caused complete production halts—including one involving a Japanese automotive parts supplier—demonstrate that a single point of compromise in the supply chain can disrupt operations across multiple enterprises.

While large manufacturers can invest in comprehensive cybersecurity programs, small and medium-sized enterprises (SMEs)—critical nodes in industrial supply chains—often lack the budget, expertise, and governance structures to address evolving risks. The current study responds to this challenge by focusing on the "Technology" domain of OT security. It introduces a risk-aligned framework for selecting and deploying security technologies, combined with a network segmentation strategy that aligns protection measures with operational risk priorities, aiming to enhance resilience while controlling implementation costs.

PRIOR RESEARCH

Cybersecurity in industrial contexts has often been guided by frameworks like the NIST Cybersecurity Framework (CSF), which organizes best practices into five core functions: Identify, Protect, Detect, Respond, and Recover (NIST, 2018). While versatile, the NIST CSF does not provide specific implementation depth or prioritization criteria, leaving such decisions to the implementing organization. This flexibility benefits mature IT environments but can create uncertainty for SMEs and OT-focused operations with limited security expertise. Moreover, it does not fully address OT-specific constraints such as real-time operation, safety-critical processes, and limited tolerance for downtime.

The recent research presents a comprehensive taxonomy of manufacturing-specific cyber-physical vulnerabilities, structured in relation to defense layers (Rahman et al., 2024). The Defense-in-Depth-driven framework categorizes vulnerabilities across cyber, human, inspection, monitoring, and organizational domains. While this defense- and vulnerability-management-oriented perspective is particularly relevant for manufacturing systems, it still requires significant security expertise, which can be burdensome for SMEs.

To address these gaps, the authors have developed tailored methods for factory environments. A central element is a 32-item OT security checklist issued by Japan's Ministry of Economy, Trade and Industry (METI, 2022), covering People, Process, Technology, and Supply Chain Management for Factory Asset (FA SCM). This checklist was implemented as a web- based diagnostic tool (GitHub, 2023), enabling 225 factories to self-assess their security posture (Sasaki and Watanabe, 2023). Analysis revealed that over 80% of participants showed insufficient readiness, particularly in governance-related areas such as risk assessment, policy enforcement, and cross-departmental coordination.

To deepen understanding, the authors conducted follow-up interviews and OT risk workshops, which helped factory staff map business-critical processes to plausible cyber threat scenarios (Sasaki et al., 2024). These sessions highlighted that the primary bottlenecks were organizational rather than technical—specifically, unclear roles and decision-making authority in incident response. Building on these findings, the current study advances into the Technology domain, proposing a structured classification and deployment approach for OT security solutions tailored to factory risk profiles.

METHODOLOGY

This study presents a structured classification framework that translates the resilience concept into practical guidance for selecting and deploying OT security technologies. The framework is designed to support risk- informed decision-making, particularly in small and medium-sized factories where financial, technical, and human resources for cybersecurity are often constrained. By linking operational risk priorities to technology characteristics, the framework enables a targeted and cost-effective security roadmap.

1. Resilience Concept as the Basis

The resilience concept, developed in prior research (Sasaki, 2024), is built around two complementary pillars: prevention and incident response (Fig. 1).

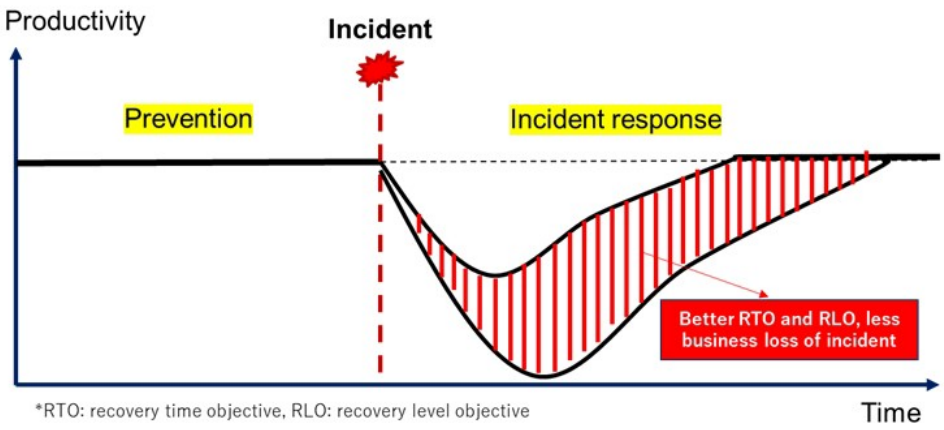

Figure 1: Productivity resilience concept (Sasaki, 2024).

Prevention aims to reduce the likelihood of incidents by detecting potential threats as early and as accurately as possible. From a technical perspective, this requires enhancing detection capabilities—especially toward unknown threats that cannot be captured by traditional signature-based methods.

Incident response focuses on minimizing disruption and business losses after an incident occurs. Technologically, this is enabled by reducing the

time required to contain and remediate an incident. Automated responses can accelerate these processes, thereby improving Recovery Time Objective (RTO) and Recovery Level Objective (RLO).

The prevention axis reflects the scope of threat detection, while the incident response axis reflects the speed and effectiveness of recovery. These two axes form the foundation of the proposed technology classification.

2. Axes of Classification

The framework uses two dimensions to categorize OT security technologies:

Threat Detection Capability**:**

Known threats: Solutions relying on predefined indicators such as virus signatures, static rules, or fixed pattern matching.

Unknown threats**:** Solutions detecting anomalies or suspicious behavior without relying on prior signatures, including zero-day attacks, insider misuse, and abnormal system operations.

Automation Level of Response:

Manual response: Alerts require human interpretation and action before countermeasures are applied.

Automated response: Systems can execute predefined actions—such as isolation, blocking, or process shutdown—without human intervention, reducing incident containment and recovery time.

3. Four Technology Models

Combining these two axes produces four distinct models (Fig. 2):

- **Model X**: Known threats + Manual response
- **Model X+**: Known threats + Automated response
- **Model Y**: Unknown threats + Manual response
- **Model Y+**: Unknown threats + Automated response

These models represent increasing capability and operational complexity. Model X provides a basic, low-cost baseline, while Model Y+ delivers the highest level of protection but requires robust governance, skilled staff, and thorough testing to prevent operational disruption.

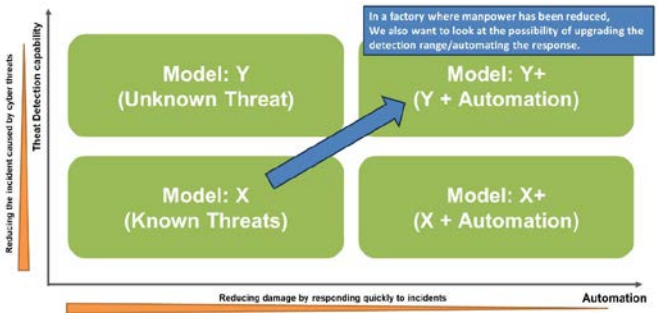

Figure 2: Four technology models based on resilience concept.

4. Application and Integration

This framework supports phased implementation. Factories may initially deploy Model X solutions across all systems, then selectively upgrade critical production zones—such as supervisory control or safety systems— to X+, Y, or Y+. In highly sensitive operations where downtime has severe consequences, Model Y+ may be justified despite higher cost and complexity.

Importantly, the framework integrates with the METI 32-item OT security checklist and its associated diagnostic tool from prior research. Each checklist item can be mapped to one of the four models, allowing:

- Clear visualization of current technology coverage and gaps
- Prioritization of investments based on risk
- Alignment between self-assessment results and technology deployment planning

By grounding technology selection in a resilience-based model, factories can strengthen both their preventive measures and incident response capabilities, achieving a balanced improvement in overall cybersecurity posture.

MAPPING OF TECHNOLOGIES

The four-model classification from the previous section is here applied to real-world OT (Operational Technology) security solutions to illustrate its practical use. This mapping helps factory stakeholders select technologies suited to their operational risks, constraints, and resources.

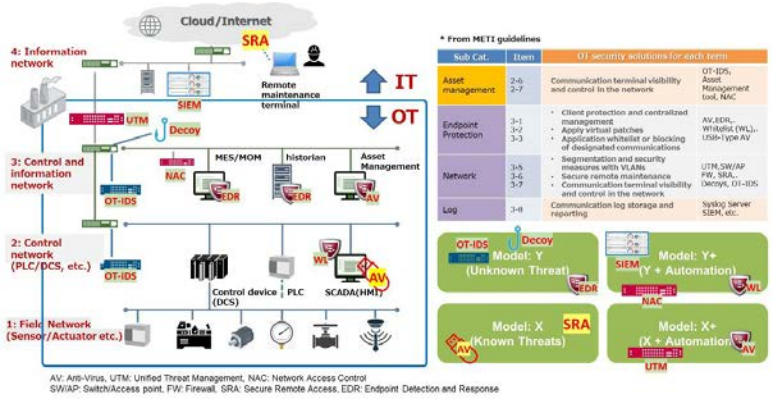

Figure 3: Mapping of OT security technologies to the four-model framework.

Model X: Manual Response to Known Threats

Technologies addressing well-known threats and requiring human action. Example: USB-based antivirus tools relying on predefined signatures and manual scanning. While easy to deploy, they lack real-time monitoring and are ineffective against advanced or fast-moving attacks.

Model X+: Automated Response to Known Threats

Adds automation to Model X. Example: Unified Threat Management (UTM) appliances and endpoint protection platforms that automatically block known threats using signature databases or heuristic analysis. Suitable for SMEs seeking compact solutions combining firewall, antivirus, VPN, and intrusion prevention.

Model Y: Manual Response to Unknown Threats

Detects emerging threats via behaviour analysis or anomaly detection. Example: OT-IDS monitoring network traffic for suspicious activity. Effective for identifying zero-day exploits or insider threats but requires human judgment due to false positives and potential operational impact.

Model Y+: Automated Response to Unknown Threats

Most advanced category, capable of autonomous action against previously unseen threats. Example: application whitelisting or lockdown systems blocking unapproved execution. Highly effective against zero-day attacks but demands rigorous testing to avoid disrupting legitimate operations.

This mapping enables:

- Clear matching of technologies to risk profiles and operational zones
- Identification of coverage gaps and prioritization of upgrades
- Improved communication of cybersecurity strategy to non-technical stakeholders

By framing technologies within this resilience-based classification, organizations can align technical measures with business priorities, particularly in environments challenged by legacy systems, limited staffing, and tight budgets.

SEGMENTATION STRATEGY AND APPLICATION

While the classification of security technologies into Models X, X+, Y, and Y+ provides a basis for selecting countermeasures, their effectiveness is enhanced when combined with a structured network segmentation strategy. In OT environments—where safety, production continuity, and system stability are critical—segmentation localizes incidents and prevents lateral movement of threats.

In IT, segmentation limits access and reduces attack surfaces. In OT, the stakes are higher: an infection in a low-priority system (e.g., DX supportive devices) can spread to production lines or safety controllers if networks are flat. Segmentation isolates functional areas, contains threats, and enables differentiated security measures, applying stricter controls only where needed.

1. Purpose of Segmentation in OT

In IT, segmentation limits access and reduces attack surfaces. In OT, the stakes are higher: an infection in a low-priority system (e.g., DX devices) can spread to production lines or safety controllers if networks are flat. Segmentation isolates functional areas, contains threats, and enables differentiated security measures, applying stricter controls only where needed.

2. Example Segmentation Structure

We assume the factory automation system in OT (Fig. 4). The systems shall be logically segmented into three Areas: Production Process Management, Parts Management, and DX Promotion, based on the OT risks.

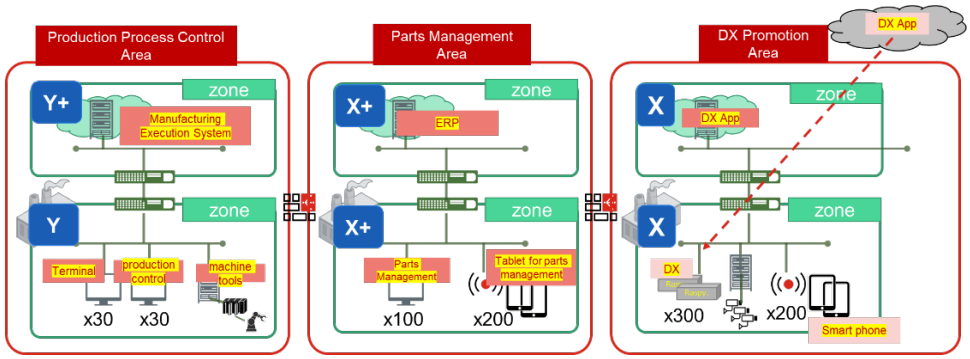

Figure 4: Sample segmentation plan.

Production Process Control Area – Highest priority; includes control terminals for the production and Manufacturing Execution System (MES). Requires strict availability and integrity.

Upper zone: Model Y+ for automated incident response against unknown threats.

Lower zone: Model Y for manual response to unknown threats in production control terminals and machine tools.

Parts Management Area – Manages logistics and inventory: slightly more tolerant to downtime.

Upper zone: Model X+ for Enterprise Resource Planning (ERP) systems.

Lower zone: Model X+ for automated detection and response in parts management terminals.

DX Promotion Area – Cloud-connected and experimental systems; less critical but more exposed.

Both upper and lower zones: Model X for known threat protection with manual response, prioritizing cost control.

Zones are logically separated via virtual local area networks (VLANs), firewalls, or data diodes, with inter-zone access restricted to essential flows and fully monitored.

3. Benefits of Zone-Specific Model Application

By aligning each zone with an appropriate model, organizations can:

Allocate stronger defenses (Y, Y+) to high-impact areas without overspending on lower-priority zones.

Clarify operational responsibilities and expected protection levels. Support incident response SOPs by limiting the scope of potential breaches. When a security breach occurs, unaffected segments can be restored quickly, reducing downtime and operational loss.

In summary, segmentation provides the structural foundation for deploying the four security models in a risk-prioritized, cost-effective manner.

CHALLENGES AND DISCUSSION

While the proposed classification model and segmentation strategy provide a practical OT cybersecurity framework, their implementation faces technical, organizational, and cultural challenges—especially in SMEs.

1. Operational Burden of Y / Y+ Models

Unknown-threat detection (Y, Y+) generates many alerts, including false positives, requiring specialized OT knowledge for evaluation. In critical environments, excessive alerts or automation errors risk disrupting production, limiting adoption of fully autonomous responses.

2. Capability Gaps

OT incident handling demands localized expertise that is difficult to outsource. SMEs often lack trained OT security personnel, making phased deployment and skill development essential.

3. Segmentation Complexity

Effective segmentation requires accurate asset prioritization and stakeholder agreement on zones, responsibilities, and acceptable risk. Without alignment, even sound designs may fail.

4. Role of OT Risk Workshops

OT Risk Workshops of our prior development help identify unacceptable outcomes, map them to zones/models, and improve cross-functional communication, ensuring technology and segmentation choices align with business priorities.

In summary, the framework is a flexible guide, not a rigid standard. By addressing these challenges, organizations can progress from reactive measures toward a coherent, risk-based OT cybersecurity strategy.

CONCLUSION

This study introduced a structured, risk-based framework for selecting and implementing cybersecurity technologies in Operational Technology (OT) environments. The framework is designed to support practical decision-making in factories, particularly small and medium-sized enterprises (SMEs), where security resources and expertise are limited but operational impact from cyber incidents can be severe.

The core of the proposed framework is a two-axis classification model that organizes technologies according to (1) their capability to detect known or unknown threats, and (2) whether they support manual or automated response. This yields four distinct models—X, X+, Y, and Y+—that guide selection based on the risk characteristics and criticality of the system in question.

To complement this classification, the study also emphasized the role of network segmentation. By dividing factory networks into logical zones based on operational roles and business priorities, organizations can implement

differentiated security controls and confine threats to specific areas. This not only enhances resilience but also optimizes investment by focusing resources where they are most needed.

Together, the classification model and segmentation strategy provide a flexible, scalable, and actionable path for OT cybersecurity enhancement. Their integration with governance mechanisms and OT risk workshops further ensures that technical measures are aligned with business objectives and operational realities.

While the framework offers a versatile foundation, future research is needed to develop industry-specific deployment guidelines. Different sectors exhibit varying degrees of risk, digital maturity, and operational constraints, which influence the applicability of each model. Some suggested directions include:

Small and Medium-Sized Enterprises (SMEs): Many SMEs lack cybersecurity staffing and budgets. For them, Models X and X+ may offer the most realistic starting points. Over time, with appropriate support and education, they can transition toward more advanced models.

Industries with Low Tolerance for Downtime: In sectors such as automotive manufacturing, semiconductor production, and food processing, even brief interruptions can result in significant losses. These industries should prioritize the implementation of Models X+ and Y+ in high-priority zones.

High-Dependency Environments: In continuous-process industries like steel production (e.g., blast furnaces) or chemical plants, shutdowns may be unacceptable under any circumstance. In these environments, Model Y or Y+ may be essential, despite the higher cost and operational risk.

Integration with Supply Chain Risk Management: Future work could explore how external vendor risk, component sourcing, and logistics platforms can be incorporated into the model, particularly for digitally integrated ecosystems.

Toolkits and Decision Aids: Additional tools—such as risk modeling software, visualization dashboards, or policy templates—can help practitioners operationalize the framework more effectively.

Ultimately, the proposed model aims to help bridge the gap between abstract cybersecurity theory and the everyday operational decisions faced by factory managers, engineers, and technicians. By providing clear structures and practical guidance, the framework supports sustainable, risk-aligned cybersecurity improvements across diverse industrial settings.

ACKNOWLEDGMENT

This research has been partially supported by Information-Technology Promotion Agency, Japan, however all remaining errors belong to the authors. It was also supported by Fortinet Japan G.K., who contributed technical knowledge and collaborative feedback throughout the development of the risk assessment model and workshop methodologies. The authors are especially grateful for their cooperation in validating the practical feasibility of the proposed approach within factory environments.

We would also like to thank the participating factories and organizations who contributed data through the web-based diagnostic tool and engaged in the OT risk workshops. Their input and reflections were instrumental in shaping the segmentation strategy and risk-based model.

Finally, the authors extend their appreciation to the peer reviewers and academic advisors who provided critical insights and constructive comments that improved the clarity and robustness of the manuscript.

REFERENCES

GitHub. (2023). OT Security Simple Assessment Tool. https://github.com/OTSec-Hiroshi-Sasaki/en-ot-security-simple-assessment.

METI (Ministry of Economy, Trade and Industry, Japan). (2022). Cyber/Physical Security Framework for Factory Systems (Draft Version 1.0). Tokyo, Japan: METI.

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, MD: National Institute of Standards and Technology. Rahman, M. H. and Shafae, M., 2024. Cyber-Physical Security Vulnerabilities Identification and Classification in Smart Manufacturing – A Defense-in-Depth Driven Framework and Taxonomy. arXiv preprint arXiv:2501.09023.

Sasaki, H., & Watanabe, K. (2023). Development of Easy Risk Assessment Tool for Factory Cybersecurity. In: Industrial Cybersecurity Workshop (Short Paper).

Sasaki, H., Watanabe, K., & Koshijima, I. (2023). Analysis of Cybersecurity Risk for Factory Systems. In: AHFE International Conference on Human Factors in Cybersecurity.

Sasaki, H., Watanabe, K., & Koshijima, I. (2024). Development of Approach for Improving Cybersecurity Governance for Factory Systems. In: AHFE International Conference on Human Factors in Cybersecurity.