

AI-Powered Adaptive Threat Intelligence and Risk Mitigation Framework for Secure SAP S/4HANA Manufacturing Integration

Daniel Okonkwo¹

¹ Intelligent Computing and Data Analytics Group, Applied AI Research Institute, Nigeria

ABSTRACT: The increasing integration of SAP S/4HANA manufacturing environments with enterprise applications, supply-chain platforms, industrial systems, and external digital services has expanded the attack surface of manufacturing organizations. Traditional security approaches based primarily on static rules and isolated monitoring are insufficient for identifying dynamically evolving threats across heterogeneous integration channels. This research proposes an AI-Powered Adaptive Threat Intelligence and Risk Mitigation Framework for secure SAP S/4HANA manufacturing integration. The framework combines threat intelligence, machine-learning-based anomaly detection, supply-network risk propagation, contextual risk scoring, and adaptive mitigation across RFC, IDoc, and API communication channels. The conceptual foundation integrates supply-chain analytics, predictive intelligence, dynamic manufacturing coordination, and probabilistic risk assessment. The proposed framework is structured around six functional layers: integration telemetry, threat-intelligence enrichment, AI-based detection, contextual risk analysis, adaptive response, and continuous learning. The analysis indicates that combining communication-level security with operational and supply-network context can improve the prioritization of integration threats compared with isolated event detection. The framework also emphasizes explainability, controlled automation, and risk-aware response to reduce the possibility of disrupting legitimate manufacturing processes. Kalal's SAP manufacturing integration threat-modeling approach provides a direct security foundation for identifying and mitigating risks associated with RFC, IDoc, and API communication (Kalal, 2024). The resulting architecture provides a research-oriented foundation for adaptive cybersecurity in digitally integrated SAP S/4HANA manufacturing environments.

KEYWORDS: SAP S/4HANA, Artificial Intelligence, Threat Intelligence, Cybersecurity, Risk Mitigation, Manufacturing Integration, RFC, IDoc, API Security, Machine Learning.

1. Introduction

1.1 Background

Digital manufacturing increasingly depends on integrated information systems that connect production planning, procurement, inventory, logistics, suppliers, and operational processes. SAP S/4HANA can function as a central enterprise platform within this environment, while communication with external and internal systems occurs through multiple integration mechanisms. Such connectivity improves coordination but also creates security dependencies across application interfaces, enterprise networks, and supply-chain participants.

The security problem is therefore not limited to identifying malicious messages or unauthorized access. A compromised integration point can potentially propagate risk into downstream manufacturing activities, supplier coordination, inventory decisions, or

production scheduling. Supply-chain research demonstrates that operational decisions are highly interconnected, meaning that disruption in one node can influence other nodes through dependencies and propagation mechanisms (Chopra & Meindl, 2016; Simchi-Levi et al., 2008). Consequently, cybersecurity analysis for SAP manufacturing integration should incorporate both technical indicators and operational context.

Machine learning and predictive analytics offer an opportunity to transform security monitoring from predominantly reactive inspection toward adaptive risk identification. Carbonneau et al. (2008) demonstrate the applicability of machine-learning techniques to supply-chain forecasting, while Waller and Fawcett (2013) emphasize the strategic role of data science and predictive analytics in supply-chain decision-making. These principles can be transferred conceptually to cybersecurity, where historical integration events and

contextual signals can support detection of abnormal behavior.

1.2 Problem Statement

Conventional integration security may treat RFC calls, IDoc exchanges, and APIs as separate technical assets. Such separation can obscure relationships between apparently low-risk events occurring across multiple interfaces. Furthermore, static security policies may fail to distinguish legitimate operational changes from coordinated malicious behavior.

Kalal (2024) specifically emphasizes threat modeling and mitigation for RFC, IDoc, and API communication within SAP manufacturing integration. Building on this security foundation, the present research addresses the additional problem of how artificial intelligence and adaptive threat intelligence can continuously evaluate integration events according to their technical characteristics and manufacturing context.

1.3 Research Relevance and Objectives

The central objective is to develop a conceptual framework capable of integrating AI-driven threat detection with contextual risk mitigation for SAP S/4HANA manufacturing integration. The research specifically aims to establish a layered architecture for collecting integration telemetry, enriching events with threat intelligence, detecting anomalous behavior, calculating contextual risk, selecting mitigation actions, and learning from subsequent outcomes.

A second objective is to connect cybersecurity risk with supply-network dependencies. Garvey et al. (2015) demonstrate that supply-network risks can propagate through interconnected structures, while Qazi et al. (2016) show how Bayesian networks can support risk management in complex environments. These concepts provide a theoretical basis for treating cybersecurity events as potentially interconnected operational risks rather than isolated technical incidents.

1.4 Scope and Significance

The proposed framework focuses on SAP S/4HANA manufacturing integration and considers RFC, IDoc, and API communication as principal integration channels. It addresses detection and mitigation rather than implementation of a particular commercial security product. The framework is conceptual and analytical; therefore, its findings represent architectural and methodological conclusions rather than experimentally measured production performance.

Its significance lies in combining AI-based prediction with security threat modeling and supply-network risk analysis. Such integration can enable organizations to prioritize security events according to

potential manufacturing consequences rather than merely technical severity.

2. Literature Review

2.1 Supply-Chain Analytics and Intelligent Decision-Making

Supply-chain management is inherently dependent on coordination among suppliers, manufacturers, logistics providers, and customers. Chopra and Meindl (2016) characterize supply-chain performance as a system-level problem in which decisions in one area influence other activities. Simchi-Levi et al. (2008) similarly emphasize the importance of integrated planning and coordinated supply-chain decisions.

These perspectives are important for cybersecurity because a manufacturing integration event can have consequences beyond the immediate application interface. For example, manipulation of an inventory-related message could influence replenishment decisions, while disruption of production-related information could affect scheduling and downstream logistics.

Carbonneau et al. (2008) demonstrate that machine-learning methods can be applied to demand forecasting, establishing the broader feasibility of data-driven prediction within supply-chain environments. Waller and Fawcett (2013) extend this perspective by positioning data science and predictive analytics as transformative capabilities for supply-chain design and management. Their work supports the theoretical proposition that large volumes of operational data can be converted into predictive intelligence.

2.2 Big Data and Operational Analytics

Choi et al. (2018) examine big-data analytics in operations management and emphasize the analytical value generated when operational data are systematically processed. For SAP S/4HANA integration security, this suggests that security telemetry should not remain isolated within technical logs. Integration frequency, message patterns, transaction timing, source systems, destinations, and operational conditions can collectively provide useful signals for identifying abnormal behavior.

However, the application of analytics to cybersecurity introduces a critical distinction. A statistically unusual event is not necessarily malicious. Manufacturing environments frequently experience legitimate changes caused by production schedules, supplier disruptions, maintenance activities, and demand fluctuations. Therefore, an AI security framework must incorporate contextual information rather than classify anomalies solely on statistical deviation.

2.3 Dynamic Manufacturing and Integration Risk

Ivanov et al. (2016) demonstrate the importance of dynamic models and short-term scheduling in smart-factory environments. Manufacturing systems therefore operate under changing conditions in which operational behavior can legitimately vary over time. This dynamic characteristic creates a challenge for static cybersecurity baselines.

An adaptive threat-intelligence system should consequently distinguish between normal variability and malicious deviations. For example, a sudden increase in IDoc traffic may be expected during a production transition but suspicious when it originates from an unauthorized source outside the normal operational pattern.

2.4 Supply-Network Risk Propagation and Probabilistic Assessment

Garvey et al. (2015) provide a foundation for understanding how risk can propagate through supply networks. Their perspective is particularly relevant to cybersecurity because an integration compromise may spread across connected systems. Qazi et al. (2016) further demonstrate the applicability of Bayesian networks to project complexity and risk management. Together, these studies support a probabilistic approach in which multiple indicators contribute to an overall risk assessment.

Kalal (2024) provides the closest direct foundation for the present research by addressing threat modeling and mitigation for RFC, IDoc, and API communication in SAP manufacturing integration. The proposed research extends this perspective conceptually by adding adaptive AI-driven intelligence and contextual risk prioritization (Kalal, 2024).

2.5 Research Gap

The reviewed literature establishes four complementary capabilities: supply-chain coordination, predictive analytics, dynamic manufacturing modeling, and risk propagation. However, these capabilities are not integrated into a unified AI-driven cybersecurity architecture for SAP S/4HANA manufacturing integration. Existing security-oriented reasoning also requires stronger linkage between interface-level threats and operational consequences.

The research gap can therefore be characterized as the absence of a unified framework that connects SAP integration threat telemetry, AI-based anomaly detection, threat-intelligence enrichment, probabilistic risk assessment, supply-network propagation, and adaptive mitigation. The proposed framework addresses this gap.

3. Methodology

3.1 Research Design

This study adopts a conceptual framework-development methodology based on structured synthesis of the supplied literature. The methodology maps concepts from machine learning, predictive analytics, supply-chain risk, dynamic manufacturing, and SAP integration security into a unified architecture.

The framework is designed around the principle that a security decision should be based on three dimensions: technical abnormality, threat intelligence, and operational impact. This prevents the system from treating every anomaly as equally dangerous.

3.2 Proposed Adaptive Threat Intelligence Architecture

The proposed architecture consists of six interconnected layers.

Layer 1: Integration Telemetry

The first layer collects security-relevant events from RFC, IDoc, and API communication. Relevant attributes include source identity, destination, transaction characteristics, frequency, timing, authentication context, message type, interface behavior, and historical communication patterns.

For example, an IDoc originating from a normally authorized production system may be considered low risk when its message frequency corresponds to an established production schedule. The same message type originating from an unusual source and outside the normal operational window should receive greater scrutiny.

Layer 2: Threat-Intelligence Enrichment

Raw events are enriched with contextual indicators. Threat intelligence can include known malicious behavioral patterns, unusual source characteristics, historical incidents, and organizational security knowledge. Rather than producing an isolated alert, this layer transforms an event into a contextual security observation.

Kalal's (2024) threat-modeling perspective is particularly relevant here because RFC, IDoc, and API channels possess different attack surfaces and security considerations. The proposed framework therefore maintains channel-specific security characteristics while applying a common risk-analysis process.

Layer 3: AI-Based Detection

The third layer applies machine-learning techniques to identify deviations from learned behavioral patterns. The conceptual detection model can be expressed as:

$$A = f(X, H, C)$$

where A represents anomaly likelihood, X represents current integration-event features, H represents historical behavior, and C represents operational context.

A key methodological principle is that anomaly detection should not automatically equal threat confirmation. This distinction is essential because dynamic manufacturing environments can produce legitimate deviations, as indicated by the dynamic scheduling characteristics discussed by Ivanov et al. (2016).

Layer 4: Contextual Risk Scoring

The framework combines anomaly probability with threat intelligence and operational impact. A conceptual risk function is:

$$R = w_1A + w_2T + w_3I + w_4P$$

where A is anomaly score, T is threat-intelligence relevance, I is operational impact, and P is propagation potential. The weights can be calibrated according to organizational risk tolerance.

This model incorporates the supply-network risk perspective of Garvey et al. (2015) and the probabilistic reasoning supported by Qazi et al. (2016). A technically moderate anomaly can therefore receive a high risk score when it affects a highly connected manufacturing process.

Layer 5: Adaptive Mitigation

Risk scores are mapped to response levels. Low-risk events can be monitored, medium-risk events can trigger enhanced authentication or additional validation, and high-risk events can initiate containment, interface isolation, or human approval.

The framework intentionally avoids unrestricted autonomous response. Manufacturing systems have operational dependencies, so aggressive automated blocking could interrupt legitimate production. Controlled automation therefore provides a balance between rapid response and operational continuity.

Layer 6: Continuous Learning

The final layer records the outcomes of security decisions. Confirmed incidents, false positives, legitimate operational exceptions, and analyst decisions become feedback for future model refinement.

This continuous-learning principle is consistent with the broader role of predictive analytics in supply-chain decision-making described by Waller and Fawcett (2013). The objective is not merely to detect more anomalies but to improve the quality of risk discrimination over time.

3.3 Channel-Specific Threat Analysis

RFC communication requires attention to unauthorized function execution, abnormal transaction behavior, privilege misuse, and unexpected communication relationships. IDoc communication requires analysis of message origin, message type, volume, timing, and unexpected modifications. APIs require consideration of authentication behavior, request patterns, endpoint access, and abnormal consumption.

Kalal (2024) provides the security threat-modeling foundation for these three integration mechanisms. The proposed framework does not replace channel-specific controls; instead, it places their security events into an adaptive intelligence pipeline.

3.4 Risk Propagation Model

A manufacturing integration threat should also be analyzed according to its potential downstream consequences. A conceptual dependency graph can represent relationships among SAP services, production planning, inventory, procurement, suppliers, and logistics.

If node i is compromised, propagation risk can be represented conceptually as:

$$P_i = \sum (D_{ij} \times V_j \times C_j)$$

where D_{ij} represents dependency strength, V_j represents vulnerability exposure, and C_j represents the operational consequence associated with dependent node j .

This model connects cybersecurity with supply-network risk propagation and supports more meaningful prioritization than interface-level severity alone.

3.5 Hypothetical Operational Example

Consider an API used to synchronize supplier delivery information with SAP S/4HANA. An abnormal burst of requests occurs from a previously infrequent source. The AI detector identifies statistical deviation, while threat-intelligence enrichment increases the security relevance. The risk engine then observes that the API influences material availability and production scheduling. Because the propagation potential is high, the system assigns a high contextual risk score.

Instead of immediately disabling the entire integration, the adaptive response may require stronger authentication, temporarily restrict the source, increase monitoring, and request human validation. This illustrates how the framework seeks to balance cybersecurity protection with manufacturing continuity.

4. Results

The analytical evaluation of the proposed framework

produces several principal findings. First, integration security is more informative when technical anomalies are interpreted in operational context. A standalone anomaly detector can identify unusual RFC calls, IDoc patterns, or API requests, but abnormality alone cannot reliably distinguish malicious activity from legitimate manufacturing variability. This finding follows from the dynamic characteristics of smart-factory scheduling described by Ivanov et al. (2016) and the predictive orientation of supply-chain analytics described by Carbonneau et al. (2008).

Second, the framework demonstrates the importance of risk propagation analysis. An integration event should receive greater priority when it affects a highly connected process. The supply-chain literature emphasizes interconnected decision structures and dependencies (Chopra & Meindl, 2016; Simchi-Levi et al., 2008). Garvey et al. (2015) further establish the relevance of risk propagation across supply networks. Consequently, the proposed architecture evaluates not only whether an event appears suspicious but also what operational systems could be affected.

Third, AI and threat intelligence serve different but complementary purposes. AI contributes behavioral detection and predictive scoring, while threat intelligence provides contextual security relevance. Combining them reduces dependence on either static signatures or purely statistical models. This is consistent with the broader observation that data science and predictive analytics can transform supply-chain decision-making (Waller & Fawcett, 2013).

Fourth, probabilistic risk assessment improves prioritization. Qazi et al. (2016) demonstrate the value of Bayesian-network reasoning for complex risk management. Applying the same conceptual principle to SAP integration enables multiple indicators to contribute to a unified risk score. Consequently, an event with moderate anomaly characteristics can become high priority when combined with significant operational impact and propagation potential.

Fifth, the framework supports adaptive rather than uniformly disruptive mitigation. High-confidence, high-impact events may justify automated containment, whereas uncertain events should trigger enhanced monitoring or human validation. This distinction is particularly important in manufacturing because excessive security intervention can itself create operational consequences.

Finally, the framework strengthens the security model described by Kalal (2024) by positioning RFC, IDoc, and API threats within a continuous intelligence cycle. The resulting architecture connects threat modeling, AI detection, contextual risk evaluation, mitigation, and feedback rather than treating these

functions as isolated security activities (Kalal, 2024).

5. Discussion

The findings indicate that secure SAP S/4HANA manufacturing integration should be conceptualized as a socio-technical risk-management problem rather than solely an interface-security problem. RFC, IDoc, and API communication channels provide technical pathways, but their importance derives from the manufacturing processes and supply-network dependencies that they support. This distinction changes how security priorities should be established.

From a theoretical perspective, the proposed framework combines concepts that are generally treated separately. Machine learning provides behavioral intelligence, while supply-chain research provides a model of interconnected operational consequences. Carbonneau et al. (2008) and Waller and Fawcett (2013) support the use of predictive analytics, while Choi et al. (2018) establish the importance of big-data analytics for operations management. These perspectives collectively justify the use of high-volume operational and integration data for adaptive security analysis.

The framework also addresses the challenge of dynamic manufacturing behavior. Ivanov et al. (2016) demonstrate that smart-factory scheduling can change over short time horizons. Consequently, a static behavioral baseline can become inaccurate as production conditions evolve. An adaptive model that continuously incorporates validated events is theoretically better aligned with this environment. Nevertheless, continuous learning introduces its own risks. Poorly validated feedback or contaminated training data could cause the system to learn malicious behavior as legitimate. Human oversight and controlled model updates are therefore important safeguards.

The supply-network perspective introduces another important trade-off. Greater integration creates improved coordination but simultaneously increases dependency and potential propagation pathways. Chopra and Meindl (2016) and Simchi-Levi et al. (2008) emphasize the interconnected nature of supply-chain operations, while Garvey et al. (2015) demonstrate how risk can propagate through supply networks. Therefore, organizations should not necessarily seek to minimize integration; instead, they should seek to make integration observable, risk-aware, and controllable.

The proposed risk-scoring mechanism also has limitations. Assigning weights to anomaly probability, threat intelligence, operational impact, and propagation potential requires organizational calibration. Incorrect weights can produce either excessive alerts or insufficient response. Bayesian reasoning, as discussed by Qazi et al. (2016), can provide a stronger probabilistic foundation,

but it also requires reliable probability estimates and relevant historical data.

In practical terms, the framework extends the channel-specific threat-modeling foundation of Kalal (2024). Rather than replacing security controls for RFC, IDoc, and APIs, it creates an intelligence layer capable of correlating their events and determining their broader consequences. This distinction is significant because no AI model can compensate for fundamentally inadequate access control, authentication, authorization, or interface governance.

A further limitation is that the present research is conceptual rather than experimentally validated. No production SAP dataset, benchmark corpus, or controlled attack dataset was supplied. Therefore, claims regarding detection accuracy, false-positive rates, latency, or security improvement should not be interpreted as experimentally established performance. Future research should evaluate the framework using realistic integration telemetry, simulated attack scenarios, and longitudinal manufacturing workloads.

Overall, the framework's principal contribution is its integration of adaptive AI detection, threat intelligence, operational impact assessment, and supply-network propagation analysis into a unified SAP manufacturing security architecture.

6. Conclusion

This research proposed an AI-Powered Adaptive Threat Intelligence and Risk Mitigation Framework for secure SAP S/4HANA manufacturing integration. The framework addresses the limitations of isolated and static security monitoring by combining integration telemetry, threat-intelligence enrichment, AI-based anomaly detection, contextual risk scoring, adaptive mitigation, and continuous learning.

The analysis demonstrates that cybersecurity events should be evaluated according to both their technical characteristics and their potential manufacturing consequences. Supply-chain dependencies, dynamic production behavior, and risk propagation make contextual prioritization essential. The framework also provides a systematic extension of SAP manufacturing integration threat modeling for RFC, IDoc, and API communication (Kalal, 2024).

The principal research contribution is therefore a unified architecture that connects cybersecurity intelligence with manufacturing and supply-network risk. Its practical value lies in supporting risk-aware responses that protect critical integration pathways without unnecessarily disrupting legitimate operations.

Future research should validate the framework using real or realistically simulated SAP S/4HANA

telemetry, compare alternative machine-learning approaches, develop explainable risk-scoring mechanisms, and evaluate automated response policies under controlled manufacturing scenarios. Particular attention should also be given to model drift, adversarial manipulation, false positives, and human-in-the-loop governance.

References

1. Carbonneau, R., Laframboise, K., and Vahidov, R. "Application of machine learning techniques for supply chain demand forecasting." *European Journal of Operational Research*, 2008.
2. Choi, T. M., Wallace, S. W., and Wang, Y. "Big data analytics in operations management." *Production and Operations Management*, 2018.
3. Chopra, S., and Meindl, P. *Supply Chain Management: Strategy, Planning, and Operation*. Pearson, 2016.
4. Garvey, M. D., Carnovale, S., and Yeniyurt, S. "An analytical framework for supply network risk propagation." *International Journal of Production Economics*, 2015.
5. Ivanov, D., Dolgui, A., Sokolov, B., Ivanova, M., and Werner, F. "A dynamic model and an algorithm for short-term supply chain scheduling in the smart factory industry 4.0." *International Journal of Production Research*, 2016.
6. Kalal, M. (2024). *Secure SAP Manufacturing Integration Threat Modeling and Mitigation for RFC, IDoc, and API Communication*. Published in *International Journal of Communication Networks and Information Security (IJCNIS)*, 16(4).
7. Qazi, A., Quigley, J., Dickson, A., and Kirytopoulos, K. "Project complexity and risk management using Bayesian networks." *International Journal of Project Management*, 2016.
8. Simchi-Levi, D., Kaminsky, P., and Simchi-Levi, E. *Designing and Managing the Supply Chain*. McGraw-Hill, 2008.
9. Waller, M. A., and Fawcett, S. E. "Data science, predictive analytics, and big data: a revolution that will transform supply chain design and management." *Journal of Business Logistics*, 2013.