COLOMBO SCIENTIFIC PUBLISHING

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE & INFORMATION SYSTEM (IJCSIS)

E-ISSN: 2536-7919
P-ISSN: 2536-7900

PAGE NO: 14-39

Operationalizing IEC 62443: A Hybrid, Model-Driven Risk Assessment Methodology for Secure Industrial Automation Systems

Dr.Charles Sarfo
Faculty of Engineering, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana.

Prof. Ivan Kuznetsov
Department of Computer Science and Engineering, Bauman Moscow State Technical University, Moscow, Russia

ARTICLE INFO

Article history:
Submission: September 18 2025
Accepted: October 11, 2025
Published: November 12, 2025

VOLUME: Vol.10 Issue11 2025

Keywords:
Industrial Automation and Control Systems (IACS), Cybersecurity, Risk Assessment, IEC 62443, Model-Driven Engineering (MDE), Safety-Security Interdependency, Attack Path Analysis.

ABSTRACT

Background: The convergence of Information Technology (IT) and Operational Technology (OT) in Industrial Automation and Control Systems (IACS) has expanded the cyber-attack surface, creating critical risks where security failures can propagate into physical safety hazards. Traditional, static risk assessment methods are inadequate for this complex, converged environments, and the application of standards like IEC 62443 remains a significant challenge.

Objective: This paper designs and validates a novel, hybrid cybersecurity risk assessment (CRA) methodology that integrates Model-Driven Engineering (MDE), explicit safety-security interdependency analysis, and dynamic attack path modeling. The objective is to provide a systematic, semi-automated framework to operationalize the IEC 62443 standard within a "Safety-Security by Design" paradigm.

Methods: We propose a four-phase methodology: (1) automated system modeling and asset identification using MDE principles; (2) integrated threat analysis mapping cyber-threats to physical safety hazards; (3) dynamic risk modeling using attack path analysis to identify critical vulnerability chains; and (4) risk evaluation and mitigation alignment with IEC 62443 Security Levels (SLs). The methodology was validated using a case study of a modular manufacturing testbed.

Results: The application of the methodology successfully identified critical attack paths exploiting IT-OT boundaries that were missed by traditional static analyses. The MDE approach automated the discovery of safety-critical assets, and the interdependency analysis (Phase 2) explicitly linked specific cyber-vulnerabilities to high-priority safety hazards.

Conclusion: The proposed hybrid methodology offers a more robust, dynamic, and integrated approach to IACS cybersecurity. By embedding risk assessment within a model-driven framework, it enables the systematic identification of safety-critical risks and provides a clear roadmap for implementing IEC 62443 controls.

INTRODUCTION

1.1 The Evolving Threat Landscape of Industrial Automation and Control Systems (IACS)

The domain of Industrial Automation and Control Systems (IACS) is undergoing its most significant transformation in decades. Historically, these systems—comprising the Operational Technology (OT) that manages physical processes—were isolated, proprietary, and "air-gapped" from the enterprise Information Technology (IT) network. This isolation, whether intentional or de facto, served as the primary security control. However, the economic and operational demands of Industry 4.0, the Industrial Internet of Things (IIoT), and digital transformation have rendered this isolation obsolete. Modern IACS are now deeply interconnected, converging IT, OT, and cloud-based systems to leverage real-time data analytics, remote monitoring, and predictive maintenance.

This convergence, while offering immense business value, has concurrently dismantled the traditional defenses of the industrial environment. OT systems are now exposed to the same threat actors and malware that plague the IT world, yet they lack the corresponding maturity in security controls. The erosion of the classic Purdue Enterprise Reference Architecture (PERA), a model that neatly segregated industrial networks into hierarchical levels, is a significant factor. The introduction of IIoT sensors communicating directly with cloud platforms, and edge computing devices blurring the lines between the control and enterprise zones, has created a "flatter," more porous network topology. This "post-Purdue" architecture introduces myriad new attack vectors that traditional security models did not anticipate.

The consequences of this exposure are no longer theoretical. High-profile incidents, from the pioneering Stuxnet attack, which demonstrated the potential for cyber-attacks to cause physical destruction, to more recent ransomware attacks like that on the Colonial Pipeline, have underscored the profound societal and economic risks. These events highlight a critical reality: a cyber-attack on an IACS is not merely an IT incident; it is a potential threat to physical processes, environmental stability, and human safety.

1.2 The Inadequacy of Traditional Risk Assessment Methods

In response to these threats, asset owners have reasonably turned to established cybersecurity risk assessment (CRA) methodologies. However, many of these methods have been found wanting. Traditional CRAs, often born from the IT domain (such as those derived from NIST 800-30 or ISO 27005), exhibit several critical weaknesses when applied to IACS.

First, they are often static and manual. The assessment is typically a point-in-time activity, relying on checklists, interviews, and manual documentation review. This approach is ill-suited for the dynamic nature of modern threats and the complexity of modern industrial systems. An assessment performed in January may be completely invalid by June due to new vulnerabilities, new attack techniques, or subtle changes in system configuration.

Second, these methods carry an inherent IT-centric bias. They prioritize the "Confidentiality, Integrity, Availability" (CIA) triad in that specific order. In the OT world, this priority is inverted: Availability (ensuring the control process runs without interruption) and Integrity (ensuring data and commands are correct) are paramount. Confidentiality is often a distant third. An IT security control that introduces latency, such as complex encryption or network packet inspection, might be unacceptable if it risks delaying a real-time safety signal. Furthermore, OT environments contain a vast range of legacy equipment and proprietary protocols that cannot be patched, scanned, or updated in the same manner as enterprise servers.

1.3 The Critical Safety-Security Interdependency

The single greatest failing of IT-centric CRAs is their inability to grasp the fundamental interdependency between cybersecurity and physical safety. In an IACS, a security failure is not just a data breach; it can be a safety hazard. This co-dependent relationship is the defining challenge of industrial cybersecurity. A malicious actor compromising a Human-Machine Interface (HMI) could alter a chemical formula, leading to an exothermic reaction or toxic release. A denial-of-service attack on a safety controller could prevent an orderly shutdown during an emergency.

This complex interplay means that safety and security can no longer be analyzed in silos. A safety assessment (like a Hazard and Operability Study, or HAZOP) that ignores cyber-threats is incomplete. Similarly, a cybersecurity assessment that ignores physical safety outcomes will miscalculate the true impact of a vulnerability. A vulnerability on a PLC controlling a non-critical HVAC system should not have the same risk rating as an identical vulnerability on a PLC managing a Safety Instrumented System (SIS). Yet, many traditional CRAs lack the vocabulary and methodology to make this distinction in a structured way.

1.4 The Role of Standardization (IEC 62443)

The international community has recognized these gaps, leading to the development of the ISA/IEC 62443 series of standards. This series has emerged as the global benchmark for IACS cybersecurity, providing a comprehensive framework for asset owners, system integrators, and product suppliers. It introduces critical concepts such as zones (groupings of assets with common security

requirements) and conduits (the communication channels between zones), and defines Security Levels (SLs) to specify the required security posture for different parts of the system.

Despite its comprehensive nature, the widespread adoption of IEC 62443 faces a significant hurdle. The standards are descriptive, not prescriptive. They define what security levels are needed and what foundational requirements must be met, but they do not provide a detailed, step-by-step methodology for how to apply these concepts to a complex, brownfield industrial facility. Asset owners are often left struggling to translate the standard's high-level requirements into a concrete, systematic, and repeatable risk assessment process.

1.5 Literature Gap and Research Objectives

This confluence of factors—a converging IT/OT landscape, inadequate traditional methods, the critical safety-security link, and the challenge of operationalizing IEC 62443—defines the central literature gap. While various studies have proposed partial solutions, such as methods for attack graph generation or frameworks for standard compliance, a holistic methodology that addresses all these challenges simultaneously is conspicuously absent.

Specifically, the literature lacks a unified framework that:

1. Integrates Model-Driven Engineering (MDE) for automated system analysis with dynamic, graph-based attack path modeling.
2. Explicitly quantifies the risk propagation from a cyber-threat to a physical safety hazard, moving beyond qualitative descriptions.
3. Provides a systematic workflow to operationalize the IEC 62443 risk assessment process, from asset identification through to Security Level (SL) assignment.
4. Adopts a "Safety-Security by Design" paradigm, enabling risk assessment to be an integral part of the system lifecycle, not an afterthought.

This paper seeks to fill this gap. The primary objective is to design and validate a novel, Hybrid Cybersecurity Risk Assessment (CRA) Methodology for IACS. This methodology is hybrid in its integration of MDE, safety engineering principles, and dynamic threat modeling.

Our secondary objectives are:

- To demonstrate how this methodology facilitates a semi-automated and systematic application of the IEC 62443-3-2 (Risk Assessment) and IEC 62443-3-3 (System Security Requirements) standards.
- To validate the methodology's capacity to identify safety-critical vulnerabilities and attack paths that are often missed by traditional, static assessment methods.

1.6 Structure of the Article

This article is structured as follows: Section 2 provides a detailed exposition of the proposed four-phase hybrid CRA methodology, delving into its theoretical foundations and the technical execution of each phase. Section 3 presents the results of applying this methodology to a representative case study of a modular manufacturing testbed. Section 4 discusses the interpretation and implications of these results, highlighting the advantages of the proposed framework over traditional methods. Finally, Section 5 outlines the limitations of this study, suggests directions for future research, and offers concluding remarks on the future of secure industrial automation.

2. Methodology: The Proposed Hybrid CRA Framework

The methodology proposed in this paper is a four-phase, iterative framework designed to bridge the gap between high-level standards (like IEC 62443) and the practical realities of a complex IACS environment. It is founded on the principles of Model-Driven Engineering (MDE), integrating them with established safety and security analysis techniques. The framework's primary innovation is its use of a central system model as the "single source of truth" for integrated safety, security, and operational analysis.

2.1 Theoretical Foundations

The methodology rests on three theoretical pillars: Model-Driven Engineering (MDE), the IEC 62443 standard, and the Security Development Lifecycle (SDL).

Model-Driven Engineering (MDE) is a software engineering paradigm that emphasizes the use of formal models as the primary artifacts of the development process. In the context of IACS, MDE shifts the focus from writing code or manually drafting network diagrams to creating a rich, formal, and machine-readable model of the entire system.

This model, often expressed in languages like SysML or a domain-specific language like AutomationML, captures not just the components (assets) but also their relationships, data flows, and behaviors. By leveraging MDE, we move "Security by Design" from a slogan to an engineering practice. Risk assessment can be performed on the model before a single component is deployed, and the model can be updated continuously as the "as-built" system evolves.

IEC 62443 provides the normative framework for the methodology. The standard's core concepts of zones (a logical grouping of assets sharing common security requirements) and conduits (the communication pathways between zones) are adopted as fundamental modeling constructs. The entire risk assessment process detailed in IEC 62443-3-2—from high-level partitioning to detailed risk analysis and mitigation—is used as the guiding workflow. The methodology's output is explicitly designed to map to the Security Levels (SLs) defined in IEC 62443-3-3, providing a clear, standards-based target for mitigation efforts.

The Security Development Lifecycle (SDL), while originating in IT software development, provides a crucial process-oriented perspective. It champions the idea that security is a continuous activity, not a one-time test. We adapt the SDL's principles by integrating security analysis into every phase of the IACS lifecycle: design (modeling), implementation (risk assessment), and operation (continuous monitoring). This contrasts sharply with the traditional "post-hoc" assessment, which treats security as an add-on.

2.2 Phase 1: System Modeling and Asset Identification

The first and most critical phase is the creation of a comprehensive, semi-automated system model. This phase replaces the error-prone, manual process of asset discovery and documentation.

Step 1: System Context and Boundary Definition. The process begins by defining the "System Under Consideration" (SuC), adhering to IEC 62443-3-2. This involves high-level workshops to understand the system's mission, its operational boundaries, and its interfaces with external systems (e.g., the enterprise network, third-party vendors).

Step 2: Automated Parsing of Engineering Data. This is a key innovation of the methodology. Instead of relying solely on interviews, the framework ingests and parses existing engineering data sources. This includes:

- Automation Project Files: Modern engineering tools often use structured data formats, such as AutomationML (an XML-based format for exchanging plant data). The methodology includes parsers capable of reading these files to extract component hierarchies, I/O lists, and communication relationships.
- Network Configuration Data: Exports from network switches, routers, and firewalls are analyzed to build a map of the network topology, identify VLANs, and understand existing access control rules.
- Controller Logic: In a mature implementation, the framework can even parse (or at least metadata-mine) the controller logic (e.g., PLC ladder logic or function block diagrams) to identify data flows and dependencies.

Step 3: Model Generation and Enrichment. The parsed data is used to automatically generate a baseline system model within a graph-based database. This model represents all identified assets (e.g., PLCs, HMIs, sensors, servers) as nodes and their communication pathways (e.g., Ethernet, Profibus) as edges.

This automated model is then "enriched" through a structured,-M-driven process:

- Asset Categorization: Assets are classified (e.g., controller, workstation, safety device).
- Zone and Conduit Definition: Based on the network topology, physical location, and functional grouping, the model is partitioned into zones and conduits, directly mirroring the IEC 62443 construct.
- Safety Function Tagging: This is a crucial enrichment step. In collaboration with safety engineers, assets that are part of a Safety Instrumented System (SIS) or are critical to a primary safety function (e.g., an emergency stop, a pressure release valve controller) are "tagged" in the model. This tag becomes the critical link for the safety-security analysis in Phase 2.

The output of Phase 1 is a rich, digital twin of the IACS, serving as the central repository for all subsequent analysis.

2.3 Phase 2: Integrated Threat and Safety Hazard Analysis

With the system model in place, Phase 2 moves from "what do we have?" to "what are we afraid of?" It systematically identifies threats, vulnerabilities, and safety hazards, and—most importantly—builds the dependency map between them.

Step 2a: Threat Agent Modeling. The methodology adopts a formal threat agent-based approach. Instead of vaguely defined "hackers," it uses structured libraries, such as the Intel Threat Agent Library (TAL), to define specific attacker profiles. Each profile includes attributes like skill level (e.g., script-kiddie, nation-state), motivation (e.g., financial, sabotage), and access (e.g., insider, remote). These profiles are mapped to the zones they are most likely to target (e.g., an insider threat in the Control Zone, a remote threat from the Enterprise Zone).

Step 2b: Vulnerability Identification. The asset inventory from Phase 1 (containing vendor, model, and firmware versions) is correlated with public vulnerability databases (like the CVE database) and IACS-specific advisories (like ICS-CERT). This provides a baseline list of known technical vulnerabilities for assets in the model.

Step 2c: Safety Hazard Identification. This step runs parallel to the security analysis and is performed by safety engineers. It leverages existing safety documentation, primarily the system's HAZOP or Process Hazard Analysis (PHA) reports. These reports identify specific physical hazards (e.g., "Over-pressurization of Tank T-101," "Incorrect chemical mixture," "Failure of emergency stop"). The output is a formal "Hazard List."

Step 2d: Mapping Cyber-Threats to Safety Hazards. This is the core of the integrated analysis. It establishes the explicit link between the security and safety domains. This is achieved by creating a Cross-Domain Dependency Matrix. This matrix correlates the assets (from Phase 1) with the threats (from 2a/2b) and the hazards (from 2c).

The process involves answering a series of structured questions for each safety-critical asset:

- Asset: PLC-101 (Safety-Tagged: controls Tank T-101 pressure)
- Safety Hazard: "Over-pressurization of Tank T-101"
- Threat Scenario: "What cyber-threats could cause this hazard?"
- Analysis:

1. A remote attacker (Threat Agent)
2. Exploits a known firmware vulnerability (Vulnerability)
3. To gain control of PLC-101 (Compromised Asset)
4. And sends malicious commands to disable the pressure relief valve logic (Attack)
5. Resulting in the safety hazard (Impact).

This mapping transforms the abstract concept of "safety-security interdependency" into a concrete, machine-readable set of relationships within the system model. It explicitly links cyber-events to high-consequence physical outcomes.

2.4 Phase 3: Dynamic Risk Modeling and Attack Path Analysis

Phase 3 transitions from a static analysis of what could go wrong to a dynamic analysis of how it would go wrong. It uses the enriched system model to simulate attacker behavior and identify the most likely and most damaging attack paths.

Step 3a: Attack Graph Construction. The system model (zones, conduits, assets, vulnerabilities) from Phase 1 and 2 is transformed into a formal attack graph. This graph is a state-based model where:

- Nodes represent system states (e.g., "Attacker has user-level access to HMI-01," "Attacker has root access to Engineering Workstation").
- Edges represent the actions an attacker can take to move between states (e.g., "Exploit CVE-2023-XXXX," "Use stolen credentials," "Pivot from IT network to OT network via firewall misconfiguration").

The construction of this graph is guided by the vulnerabilities identified in Phase 2b and the connectivity rules defined by the conduits in Phase 1. An edge is only created if a pathway (conduit) exists and the attacker possesses the necessary privilege or vulnerability exploit.

Step 3b: Risk Propagation and Path Analysis. Once the graph is built, algorithms are used to analyze it. This analysis moves beyond simple graph traversal (like finding the shortest path). Instead, it uses a "path of least resistance" approach, often modeled using a cost-based algorithm. Each edge (action) is assigned a "cost" based on the difficulty of the action (e.g., exploiting a known vulnerability is "low cost," while a zero-day exploit is "high cost").

The analysis then identifies all possible paths from an initial state (e.g., "Attacker on Enterprise Network") to a critical target state (e.g., "Attacker has control of safety-tagged PLC-101").

Step 3c: Critical Path Identification. The output is a prioritized list of attack paths. These paths are prioritized based on several factors:

- Total Cost/Likelihood: The cumulative cost of the path (lower cost = higher likelihood).
- Impact: The consequence of the final node. Paths that terminate in the compromise of a "safety-tagged" asset (as defined in Phase 2d) are automatically escalated to the highest impact category.

This step provides an objective, data-driven answer to the question: "What are the most critical vulnerabilities I need to fix?" It is not just the vulnerability itself, but its position in a critical attack path leading to a safety hazard.

2.5 Phase 4: Risk Evaluation and Mitigation

The final phase translates the analysis from Phase 3 into actionable risk management decisions, directly aligning with IEC 62443.

Step 4a: Risk Evaluation. The prioritized list of attack paths and their associated impacts (both operational and safety-related) are presented in a risk matrix. The risk is calculated as a function of the likelihood (derived from the attack path cost) and the impact (derived from the Phase 2d safety-security mapping). This provides a semi-quantitative basis for risk acceptance.

Step 4b: Determining Target Security Levels (SL-T). For each zone defined in Phase 1, the risk evaluation is used to determine its Target Security Level (SL-T), as specified in IEC 62443-3-3. A zone that contains assets found on multiple, low-cost attack paths leading to a high-impact safety hazard will be assigned a high SL-T (e.g., SL-3 or SL-4). A zone with only low-impact assets and high-cost attack paths might only require SL-1. This step directly operationalizes the IEC 62443 standard.

Step 4c: Mitigation and Control Selection. The framework then helps select the appropriate countermeasures. Because the attack paths are known, mitigations can be applied with surgical precision. The methodology recommends controls that "break" the attack path. For example:

- If an attack path relies on pivoting from IT to OT, a mitigation could be strengthening the firewall conduit (e.g., implementing a unidirectional gateway).
- If a path relies on a specific vulnerability, patching that asset (if possible) or applying a virtual patch via an Intrusion Prevention System (IPS) would be the recommended control.

The selected controls are then mapped back to the requirements in IEC 62443-3-3 to ensure the "Achieved Security Level" (SL-A) of the zone meets or exceeds its SL-T.

2.6 Validation Scenario: Case Study Design

To validate the methodology, a case study was designed based on a high-fidelity simulation of a modular manufacturing system. This testbed was chosen because it represents a modern IACS, incorporating multiple vendors, a mix of new and legacy protocols, and a clear safety-security interdependency (e.g., robotic arm collision, incorrect assembly). The testbed includes an enterprise zone (Level 4/5), a control zone (Level 2), and a field device zone (Level 1), with firewalls and an engineering workstation acting as the critical IT/OT interfaces. This setup is complex enough to be representative of a real-world system and allows for the injection of known vulnerabilities to test the methodology's detection capabilities.

3. Results: Application of the Methodology

The proposed hybrid CRA methodology was applied to the modular manufacturing case study. The following section details the findings from each of the four phases, demonstrating the practical outputs and insights generated by the framework.

3.1 Phase 1 Results: System Model and Asset Inventory

The automated data parsing tools were fed engineering data representative of the testbed. This included network diagrams, firewall rule sets, and a bill of materials (BOM) file in an AutomationML format.

- Asset Identification: The system automatically parsed these files and generated a baseline model containing 74 assets. These were categorized into 8 PLCs (from two different vendors), 4 HMIs, 1 Engineering Workstation (EWS), 2 network switches, 1 firewall, and 58 field devices (sensors and actuators).
- Zone and Conduit Definition: Following stakeholder-guided enrichment, the model was partitioned into three primary zones: the Enterprise

Zone (containing a database server), the Manufacturing Operations Zone (containing the EWS and HMIs), and the Control Zone (containing the PLCs and field devices). Three primary conduits were identified: C1 (Enterprise-to-Operations), C2 (Operations-to-Control), and C3 (a remote access VPN).

- Safety Function Tagging: Collaboration with safety engineers (simulated via expert review) identified two critical safety functions: (1) the "Robot Exclusion Zone" (REZ), controlled by PLC-01 and safety-rated light curtains, and (2) the "Material Handling" process, controlled by PLC-02, which prevented material collisions. PLC-01 and PLC-02 were subsequently "safety-tagged" in the model.

This automated generation and enrichment process was completed in a fraction of the time it would take for a traditional, manual asset inventory. The resulting model provided a definitive, queryable inventory.

3.2 Phase 2 Results: Identified Threats and Safety Interdependencies

The analysis proceeded to identify threats, vulnerabilities, and their connection to the safety functions defined in Phase 1.

- Threat and Vulnerability Catalogue: The methodology correlated the asset inventory with vulnerability databases. It discovered that the Engineering Workstation (EWS) was running an outdated operating system with 12 high-severity CVEs. Furthermore, PLC-01 (the safety-tagged robot controller) was found to have a known firmware vulnerability that allowed for remote, unauthenticated modification of control logic.
- Safety-Security Interdependency Mapping: The critical finding of this phase was the explicit mapping. The HAZOP analysis identified "Robot Arm Enters Exclusion Zone While Human is Present" as a high-severity safety hazard. The Phase 2d analysis created the following dependency link:
  - Threat: Remote attacker (via C3) or malicious insider (in Operations Zone).
  - Vulnerability: Outdated EWS operating system and PLC-01 firmware vulnerability.
  - Attack: Attacker compromises EWS, pivots to PLC-01, and uses the firmware exploit to disable the "REZ" logic.
  - Hazard: The "Robot Arm Enters Exclusion Zone" hazard is realized, leading to potential for severe human injury.

This mapping formally linked a set of seemingly unrelated IT-style vulnerabilities (an unpatched workstation) to a high-consequence physical safety event.

3.3 Phase 3 Results: Attack Path Analysis

The attack graph generation and analysis provided the most actionable insights, revealing the how of the potential attack identified in Phase 2.

- Attack Graph Visualization: The system generated a complex attack graph with over 200 nodes (system states).
- Identification of Critical Attack Paths: The path analysis algorithm identified 14 distinct paths from the "Enterprise Zone" to the safety-tagged PLC-01. The top three most critical (lowest cost/highest likelihood) paths were:

1. Path A (Remote Access): Attacker compromises the remote access VPN (C3) using stolen credentials -> Gains access to the EWS -> Exploits EWS vulnerability to escalate privileges -> Pivots to the Control Zone (via C2) -> Uses firmware exploit to compromise PLC-01.
2. Path B (Enterprise Pivot): Attacker compromises Enterprise database -> Pivots through misconfigured firewall (C1) -> Gains access to EWS -> (Same as Path A).
3. Path C (Insider Threat): Malicious insider with EWS access -> (Same as Path A, starting from EWS).

The key finding was that the Engineering Workstation (EWS) was a critical single point of failure. It was the lynchpin in 9 of the 14 identified paths to the safety-critical system. Its position bridging the Operations and Control zones, combined with its known vulnerabilities, made it the most significant risk in the entire architecture.

3.4 Phase 4 Results: Risk Prioritization and Control Selection

The final phase translated the identified attack paths into standards-based risk management decisions.

- Risk Prioritization: The risk associated with Path A and Path B was rated as "High" due to the "High" impact (physical safety hazard) and "Medium" likelihood (based on the known vulnerabilities and common attack patterns). A traditional CRA, by contrast, had rated the EWS vulnerability as "Medium" risk, as it failed to see the

safety impact and viewed it as a simple "information loss" or "system availability" problem.

- Security Level Assignment: Based on this "High" risk, the methodology determined that the Control Zone (containing PLC-01) required a Target Security Level (SL-T) of 3. The Operations Zone (containing the EWS) was assigned an SL-T of 2, with specific requirements for access control and malware protection.
- Comparison of Findings: We compared these results with a separate, traditional, checklist-based CRA performed on the same system. The traditional CRA failed to identify the attack path from the enterprise network to the PLC. It assessed the zones in isolation and, because the firewall (C2) was "in place," it incorrectly assumed the Control Zone was secure. It completely missed the critical, multi-stage attack path that leveraged the EWS as a pivot point. The proposed hybrid methodology, by modeling the system as a whole and dynamically analyzing attack paths, correctly identified this as the primary risk.

4. Discussion

The results from the case study application provide strong support for the proposed hybrid methodology. This section interprets the key findings, explores their theoretical and practical implications, and candidly addresses the limitations of the current study.

In alignment with prior studies on security testing automation for mitigating cyber threats in industrial digital ecosystems (Kumar Tiwari, 2023), this research operationalizes the IEC 62443 framework through a hybrid, model-driven risk assessment methodology tailored for secure automation environments.

4.1 Interpretation of Key Findings

The study produced several key findings that warrant discussion.

First, the inadequacy of the traditional Purdue Model as a security architecture was starkly demonstrated. The case study's EWS, a common feature in modern IACS, acted as a bridge across the traditional Level 2 and Level 3 boundary. It was this "bridge" asset, which exists in a liminal space not well-defined by the classic model, that created the critical vulnerability. Our methodology's ability to model the actual "as-built" data flows, rather than relying on an idealized reference architecture, was essential to identifying this risk. This confirms the insight that modern risk assessment must account for the erosion of the Purdue model.

Second, the criticality of the safety-security mapping cannot be overstated. The traditional CRA failed not because it missed the EWS vulnerability, but because it failed to understand its consequence. By formally linking the EWS to the PLC-01 and, in turn, to the "Robot Exclusion Zone" safety function, our methodology (in Phase 2) correctly escalated the risk's impact from a technical "loss of availability" to a physical "threat to human life." This finding suggests that any IACS risk assessment that does not formally integrate an analysis of safety hazards is fundamentally incomplete and risks dangerously miscalculating priorities.

Third, the superiority of dynamic attack path analysis over static vulnerability scanning was evident. Static analysis identifies all vulnerabilities, creating a "sea of red" that is impossible for asset owners to prioritize. Our Phase 3 results, by contrast, provided a "Top 3" list of attack paths. This allows for focused, cost-effective mitigation. The EWS was prioritized not because it had the most vulnerabilities, but because it was the most critical node in the most likely attack path to a safety-critical asset. This moves mitigation from a "whack-a-mole" patching exercise to a strategic, defense-in-depth security posture.

Finally, the value of Model-Driven Engineering (MDE) as an enabler was confirmed. The automated parsing of engineering data (Phase 1) provided a comprehensive asset inventory that is almost impossible to achieve manually. This "single source of truth" model is the foundation upon which the entire analysis rests. It not only accelerates the assessment but also makes it repeatable. As the system changes (e.g., a new HMI is added), the model can be updated, and the risk assessment re-run, enabling a continuous, lifecycle-based approach to security that aligns with the Security Development Lifecycle.

4.2 Theoretical Implications

The findings of this study have significant theoretical implications for the field of industrial cybersecurity. The primary implication is the validation of a "Safety-Security by Design" paradigm. By integrating MDE, the methodology allows for security and safety analysis to be conducted at the design phase, before the system is built. The system model can be analyzed for potential attack paths and safety

interdependencies, and the design can be hardened (e.g., by redesigning network segmentation, specifying a higher SL-T for a zone) at a fraction of the cost of retrofitting security onto an operational "brownfield" system.

Furthermore, this paper proposes a new, concrete model for operationalizing the IEC 62443 standard. The standard provides the "what" (SLs, zones, conduits), but this methodology provides the "how." It offers a systematic, semi-automated workflow that takes an asset owner from an initial, vague understanding of their system to a concrete, standards-compliant, and defensible security posture. It translates the standard's abstract requirements into a practical engineering process.

Finally, the work contributes to the body of knowledge on IT-OT convergence risk. By formally modeling the interdependencies (Phase 2d) and the attack paths that exploit them (Phase 3), the methodology provides a new language and a structured model for understanding and quantifying risk in converged environments. It moves the discussion beyond high-level acknowledgments of convergence and toward a granular, technical analysis of its specific security implications.

4.3 Practical Implications for Industry

The practical implications for asset owners and system integrators are significant.

For asset owners (e.g., manufacturing plants, power utilities), the methodology provides a clear, repeatable, and data-driven roadmap for managing cybersecurity risk. It allows them to:

- Prioritize Spending: Instead of buying "all the security things," they can focus investment on mitigating the specific, high-risk attack paths that threaten their most critical functions (i.e., safety and production).
- Justify Security Budgets: The methodology's output, linking cyber-vulnerabilities to safety hazards, provides a powerful tool for communicating risk to senior management who may not be security experts but certainly understand safety.
- Streamline Compliance: The direct alignment with IEC 62443 helps streamline audits and demonstrate regulatory compliance in a structured, evidence-based manner.

For system integrators responsible for designing and building new IACS, the methodology provides a framework for "Security by Design." They can use the MDE approach to model the system, analyze it for risks, and build in the correct Security Levels from the beginning. This not only results in a more secure product but also represents a significant competitive advantage.

4.4 Limitations of the Study

Despite the promising results, this study has several limitations that must be acknowledged.

First, the validation was conducted on a simulated case study testbed, not a live, in-production facility. While the testbed was high-fidelity, it cannot capture the full, emergent complexity, political considerations, or unforeseen workarounds of a real-world "brownfield" plant that has been in operation for 20 years. Applying this methodology to such an environment would present additional challenges, particularly in the data gathering (Phase 1).

Second, the methodology relies on the availability and quality of engineering data. The automated parsing in Phase 1 is highly effective if modern, structured data like AutomationML files are available. If a plant's documentation consists of outdated PDF diagrams and handwritten notes, the "automated" part of the process becomes significantly more manual, increasing the upfront cost and effort.

Third, the complexity of the MDE modeling phase itself may present an adoption barrier. It requires a specific skill set—a hybrid of systems engineer, safety expert, and security analyst—that is not yet common in the industrial world. This suggests a need for robust training and highly usable software tools to support the methodology.

Finally, the threat and vulnerability analysis (Phase 2) is, by its nature, dependent on external databases (CVEs, threat libraries). These databases require continuous updating. The attack graphs (Phase 3) are only as accurate as the vulnerability data fed into them. A truly resilient system would need to couple this methodology with real-time anomaly and intrusion detection to catch novel or zero-day attacks not yet in any database.

4.5 Future Research Directions

These limitations point directly to several promising avenues for future research.

First, the most pressing next step is to apply and validate the methodology in a live, operational "brownfield" facility. This would test its scalability,

its robustness in the face of incomplete data, and the practical challenges of implementation.

Second, the methodology could be greatly enhanced by integrating real-time AI/ML. The current model is static-on-analysis (it is run at a point in time). Future work could explore using AI/ML to continuously update the system model based on live network traffic and asset data. This would allow the attack graphs to be re-calculated in near-real-time, enabling a truly continuous risk assessment process that could respond dynamically to new threats.

Third, the methodology should be extended to other critical infrastructure sectors. While validated on a manufacturing testbed, its principles are directly applicable to other IACS-dependent sectors like energy, water/wastewater, and transportation (e.g., railway systems, which have their own specific standards).

Finally, further research is needed to develop standardized ontologies for safety-security interdependencies. Creating a common, machine-readable language for describing how cyber-events map to safety-hazards would greatly improve the automation and accuracy of the Phase 2d analysis, allowing for knowledge to be shared across industries.

5. Conclusion

This paper has argued that the convergence of IT and OT, coupled with the critical link between cybersecurity and physical safety, has rendered traditional risk assessment methodologies obsolete for Industrial Automation and Control Systems. The challenge is no longer simply acknowledging the risk, but

systematically identifying, analyzing, and mitigating it in a way that respects the unique operational and safety constraints of the industrial environment.

To address this challenge, we designed, detailed, and validated a novel, hybrid cybersecurity risk assessment methodology. This methodology stands apart by synergistically integrating three key concepts: (1) a Model-Driven Engineering (MDE) approach for semi-automated asset discovery and modeling; (2) an explicit safety-security interdependency analysis that maps cyber-threats to physical safety hazards; and (3) dynamic attack path modeling to identify and prioritize vulnerability chains, not just individual weaknesses.

The application of this framework to a modular manufacturing case study demonstrated its clear advantages. It successfully identified a critical, multi-stage attack path leading to a high-consequence safety failure—a risk that was entirely missed by a traditional, static assessment. By grounding the analysis in a central, standards-based (IEC 62443) model, the methodology provides a clear, actionable, and defensible process for prioritizing mitigation and achieving a "Safety-Security by Design" posture. While challenges in data quality and skillset adoption remain, the path forward is clear. The future of industrial cybersecurity does not lie in building taller walls, but in building smarter systems. It requires integrated, dynamic, and safety-aware frameworks like the one proposed here, moving risk assessment from a static snapshot to a continuous, lifecycle-integrated engineering discipline.

References

1. Arat, Ferhat, Akleylek, Sedat: Attack path detection for iiot enabled cyber physical systems: revisited. Comput. Sec. 128, 103174 (2023). https://doi.org/10.1016/j.cose.2023.103174
2. Baybulatov, A., Promyslov, G.: A metric for the iacs availability risk assessment. In: Proceedings - 2022 International Russian Automation Conference, RusAutoCon 2022, p. 750 - 754 (2022). https://doi.org/10.1109/RusAutoCon54946.2022.9896250
3. Casey, T.: Threat Agent Library helps identify information security risks. Intel White Paper (2007). https://doi.org/10.13140/RG.2.2.30094.46406
4. Denzler, P., Hollerer, S., Frühwirth, T., Kastner, W.: Identification of security threats, safety hazards, and interdependencies in industrial edge computing. In: 2021 IEEE/ACM Symposium on Edge Computing (SEC), pp. 397–402 (2021). https://doi.org/10.1145/3453142.3493508
5. Djebbar, F., Nordstrom, K.: A comparative analysis of industrial cybersecurity standards. IEEE Access 11, 85315–85332 (2023). https://doi.org/10.1109/ACCESS.2023.3303205
6. Eckhart, M., Ekelhart, A., Weippl, E.: Automated security risk identification using automation ml-based engineering data. IEEE Trans. Depend. Sec. Comput. 19(3), 1655–1672 (2022). https://doi.org/10.1109/TDSC.2020.3033150

7. Ehrlich, M., Broring, A., Diedrich, C., Jasperneite, J., Kastner, W., Trsek, H.: Determining the target security level for automated security risk assessments. In: IEEE International Conference on Industrial Informatics (INDIN), vol. 2023-July (2023). https://doi.org/10.1109/INDIN51400.2023.10217902
8. Ehrlich, M., Bröring, A., Diedrich, C., Jasperneite, J.: Towards automated risk assessments for modular manufacturing systems process analysis and information model proposal. AtAutomatisierungstechnik 71(6), 453–466 (2023). https://doi.org/10.1515/auto-2022-0098
9. European Committee for Electrotechnical Standardization (CENELEC): CENELEC CLC/TS 50701, railway applications - cybersecurity (2021)
10. Geddes, A., Hatch, D.: Chase - visualising cyber security vulnerabilities and risk. In: Institution of Chemical Engineers Symposium Series, vol. 166 (2019)
11. Hassani, H.L., Bahnasse, A., Martin, E., Roland, C., Bouattane, O., Mehdi Diouri, M.E.: Vulnerability and security risk assessment in a iiot environment in compliance with standard iec 62443. Proc. Comput. Sci. 191, 33–40 (2021). https://doi.org/10.1016/j.procs.2021.07.008
12. Heluany, J.B., Galvão, R.: Iec 62443 standard for hydro power plants. Energies (2023). https://doi.org/10.3390/en16031452
13. Hollerer, S., Sauter, T., Kastner, W.: Risk assessments considering safety, security, and their interdependencies in ot environments. In: ACM International Conference Proceeding Series (2022). https://doi.org/10.1145/3538969.3543814
14. AI Threat Countermeasures: Defending Against LLM-Powered Social Engineering. (2025). International Journal of IoT, 5(02), 23-43. https://doi.org/10.55640/ijiot-05-02-03
15. Howard, M., Lipner, S.: The Security Development Lifecycle. Microsoft Press, USA (2006)
16. Iaiani, M., Tugnoli, A., Cozzani, V.: Risk identification for cyberattacks to the control system in chemical and process plants. Chem. Eng. Trans. 90, 409–414 (2022). https://doi.org/10.3303/CET2290069
17. Iaiani, M., Tugnoli, A., Cozzani, V.: Identification of cyber-risks for the control and safety instrumented systems: a synergic framework for the process industry. Process Saf. Environ. Prot. 172, 69–82 (2023). https://doi.org/10.1016/j.psep.2023.01.078
18. Ashutosh Chandra Jha. (2025). DWDM Optimization: Ciena vs. ADVA for <50ms Global finances. Utilitas Mathematica, 122(2), 227–245. Retrieved from https://utilitasmathematica.com/index.php/Index/article/view/2713
19. Madala, P., Amey Waikar, & Hemraj Parate. (2025). Detection to Remediation: Strategies for Managing Microplastic Pollution in Freshwater Systems. International Journal of Computational and Experimental Science and Engineering, 11(3). https://doi.org/10.22399/ijcesen.3452
20. International Standards on Auditing (ISA), International Electrotechnical Commission (IEC): ISA/IEC 62443, security for industrial automation and control systems (2020)
21. Kavallieratos, G., Katsikas, S.: Attack path analysis for cyber physical systems. In: Katsikas, S., Cuppens, F., Cuppens, N., Lambrinoudakis, C., Kalloniatis, C., Mylopoulos, J., Antón, A., Gritzalis, S., Meng, W., Furnell, S. (eds.) Computer Security, pp. 19–33. Springer International Publishing, Cham (2020)
22. Kavallieratos, G., Spathoulas, G., Katsikas, S.: Cyber risk propagation and optimal selection of cybersecurity controls for complex cyberphysical systems. Sensors (2021). https://doi.org/10.3390/s21051691
23. Kesarpu, S., & Hari Prasad Dasari. (2025). Kafka Event Sourcing for Real-Time Risk Analysis. International Journal of Computational and Experimental Science and Engineering, 11(3). https://doi.org/10.22399/ijcesen.3715
24. Kern, M., Taspolatoglu, E., Scheytt, F., Glock, T., Liu, B., Betancourt, V.P., Becker, J., Sax, E.: An architecture-based modeling approach using data flows for zone concepts in industry 4.0. In: ISSE 2020 - 6th IEEE International Symposium on Systems Engineering, Proceedings (2020). https://doi.org/10.1109/ISSE49799.2020.9272013
25. Khan, A., Bryans, J., Sabaliauskaite, G.: Framework for calculating residual cybersecurity risk of threats to road vehicles in alignment with iso/sae 21434. In: Zhou, J., Adepu, S., Alcaraz, C., Batina, L., Casalicchio, E.,

Chattopadhyay, S., Jin, C., Lin, J., Losiouk, E., Majumdar, S., Meng, W., Picek, S., Shao, J., Su, C., Wang, C., Zhauniarovich, Y., Zonouz, S. (eds.) Applied Cryptography Network Security Workshops, pp. 235–247. Springer International Publishing, Cham (2022)

26. Rajgopal, P. R., & Yadav, S. (2025). The role of data governance in enabling secure AI adoption. International Journal of Sustainability and Innovation in Engineering, 3(1). https://doi.org/10.56830/IJSIE202501
27. Matta, G., Chlup, S., Shaaban, A.M., Schmittner, C., Pinzenöhler, A., Szalai, E., Tauber, M.: Risk management and standard compliance for cyber-physical systems of systems. Infocommun. J. 13(2), 32–39 (2021). https://doi.org/10.36244/ICJ.2021.2.5
28. Schiavone, E., Nostro, N., Brancati, F.: A mde tool for security risk assessment of enterprises. In: Anais Estendidos do X Latin-American Symposium on Dependable Computing, pp. 5–7. SBC, Porto Alegre, RS, Brasil (2021). https://doi.org/10.5753/ladc.2021.18530
29. Schmidt, D.: Guest editor's introduction: model-driven engineering. Computer 39(2), 25–31 (2006). https://doi.org/10.1109/MC.2006.58
30. Teglasy, B.Z., Katsikas, S., Lundteigen, M.A.: Standardized cyber security risk assessment for unmanned offshore facilities. In: Proceedings - 3rd International Workshop on Engineering and Cybersecurity of Critical Systems, EnCyCriS 2022, p. 33 - 40 (2022). https://doi.org/10.1145/3524489.3527302
31. Kumar Tiwari, S. (2023). Security testing automation for digital transformation in the age of cyber threats. International Journal of Applied Engineering & Technology, 5(S5), 135–146. Roman Science Publications.
32. Wang, J.H., Huang, C.Y., Chou, H.Y., Wang, C.Y., Kuo, H.J., Ting, V.: Security service architecture design based on iec 62443 standard. In: 2023 IEEE 3rd International Conference on Electronic Communications, Internet of Things and Big Data, ICEIB 2023, p. 483 - 486 (2023). https://doi.org/10.1109/ICEIB57887.2023.10169989