The OSCAR PUBLISHING Services
American Journal of Applied Science and Technology

VOLUME Vol.05 Issue 11 2025
PAGE NO. 50-59

Beyond Confidentiality: A Dynamic Framework for Systemic Risk Management and Enhanced Resilience in Critical Infrastructure Operations

Minh-Hieu Nguye
Faculty of Information Technology,Hanoi University of Science and Technology, Hanoi, Vietnam

Received: 19 September 2025; **Accepted:** 14 October 2025; **Published:** 14 November 2025

Abstract: Purpose: Cyber-Physical Systems (CPS) underpinning critical infrastructure face unique security challenges due to the interconnected nature of their computational and physical components. Traditional Information Technology (IT) risk assessment methods prove inadequate, as they fail to quantify the kinetic impact—the physical and safety consequences—of a cyber breach. This study addresses this critical gap by proposing and defining a novel Unified Cyber-Physical Risk Management (UCPRM) Framework.
Methodology: The UCPRM Framework is built upon three core principles: holistic IT/OT integration, real-time dynamism, and quantitative consequence mapping. The framework introduces a Cyber-Physical Attack Graph (CPAG) to model complex, cascading failures and a Kinetic Impact Score (KIS) metric to translate cyber likelihoods into measurable physical and financial risk. The methodology integrates established international standards (ISO, NIST) with continuous operational telemetry data for dynamic risk updates.
Findings: Application of the UCPRM Framework to a simulated critical infrastructure environment demonstrated that traditional IT-centric risk models significantly underestimate the actual risk profile of CPS by failing to account for the KIS. The framework's real-time risk score enabled predictive alerting and superior resource allocation decisions, aligning security investments with actual physical safety and continuity concerns.
Originality: The UCPRM Framework is the first to seamlessly integrate real-time operational data with a structured, quantitative mechanism for assessing the physical consequences of cyber-attacks, offering a necessary paradigm shift for managing the security and resilience of critical CPS.

Keywords: Cyber-Physical Systems, Risk Management, Critical Infrastructure, Kinetic Impact, Real-Time Assessment, Operational Technology, SCADA.

INTRODUCTION:

1.1. Context and Motivation: The Convergence of Cyber and Physical Domains

The contemporary landscape of critical infrastructure, spanning sectors from energy and water treatment to manufacturing and transportation, is fundamentally dependent on Cyber-Physical Systems (CPS). A CPS is characterized by an intricate, interconnected network of computational resources that monitor and control physical processes. This tight integration, while driving unprecedented efficiencies and automation, has simultaneously introduced novel and complex security vulnerabilities. Where once the Operational Technology (OT) domain—the systems that manage industrial control—was isolated and relied on physical security, it is now deeply linked to the Information Technology (IT) domain. This OT/IT convergence has exposed systems controlling physical processes to the same, and often greater, cyber threats that have historically plagued enterprise networks.

The core motivation for this research stems from the observation that the security of these critical systems can no longer be addressed by siloed approaches. The inherent fragility of the interdependency means that a cyber intrusion can propagate rapidly, leading not

merely to data breaches, but to physical disruption, equipment damage, environmental harm, and potentially loss of human life. The growing frequency and sophistication of attacks targeting infrastructure—often attributed to state-sponsored actors or highly organized criminal entities—underscore an urgent, global imperative to redefine how CPS risk is understood, measured, and managed.

1.2. The Unique Challenge of CPS Security

Securing a CPS environment presents a challenge distinct from traditional IT security. The key differentiator lies in the criticality of availability and safety over the traditional IT focus on confidentiality. In an industrial control system (ICS) or Supervisory Control and Data Acquisition (SCADA) environment, even minor delays, inaccuracies, or denial of service can lead to immediate, detrimental physical effects.

The "Kinetic Impact" Problem

The most significant gap in current risk methodologies is the failure to quantify the Kinetic Impact of a cyber-attack. A malicious software command, for instance, targeting a Programmable Logic Controller (PLC) in a power grid substation, may not compromise sensitive customer data (a typical IT concern) but can cause equipment overload, resulting in a physical explosion and widespread power outages. The risk assessment must fundamentally translate cyber event likelihood into physical consequence—a step largely absent in generic risk frameworks. Furthermore, the unique characteristics of OT assets—their long lifecycles, reliance on proprietary and often unpatched operating systems, and stringent real-time performance requirements—make conventional IT patch management and security controls impractical or even dangerous to implement. This divergence necessitates a specialized, holistic, and quantitative approach to risk management.

1.3. Literature Review and Identified Gaps

The field of cyber risk management is well-established, drawing upon comprehensive international standards and governmental frameworks. Frameworks such as ISO 31000 provide principles and generic guidelines for risk management, while NIST Special Publication 800-30 offers detailed guidance for conducting risk assessments. Specific to critical infrastructure, the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards mandate security controls for the electric power sector. These documents, along with methods for quantitative and qualitative risk analysis, form the foundation of current practice.

However, a critical review of the literature reveals three persistent and crucial gaps when applying these models to the CPS domain:

Gap 1: Lack of Unified, Real-Time Integration. Existing methodologies tend to be siloed. Enterprise Risk Management (ERM) and IT security risk are often managed separately, failing to fully account for the interdependent nature of the cyber and physical risks in a single, coherent score. Furthermore, traditional risk assessments are periodic (e.g., annual or bi-annual). This static approach is fundamentally incompatible with the dynamic, continuous nature of threats and system operations in a CPS, which requires real-time risk modeling and continuous monitoring to be truly effective.

Gap 2: Insufficient Focus on Predictive Modeling. Current methods excel at reactive risk assessment—evaluating known vulnerabilities and documented threats. They struggle to incorporate advanced predictive analytics necessary to anticipate novel attacks or subtle, coordinated intrusions. The rise of spoofing-jamming attacks in wireless networks and sophisticated control system manipulations demands a framework that can use machine learning and anomaly detection to model the evolution of a threat in a real-time operational context.

Gap 3: Missing Quantitative Mapping to Physical Consequence. While some models attempt to rank impact (e.g., low, medium, high), there is a significant failure to provide a rigorous, universally applicable mechanism to quantify cyber-risks in terms of physical damage, safety metrics, and financial consequences. Without this quantification, security expenditure decisions remain subjective and difficult to justify to executive leadership.

1.4. Research Objective and Contribution

The primary objective of this research is to propose and meticulously define a novel Unified Cyber-Physical Risk Management (UCPRM) Framework. This framework is designed to bridge the aforementioned literature gaps by providing a holistic, quantitative, and real-time methodology specifically tailored for managing security and resilience risks in critical CPS environments.

The main contribution of this work is the development and validation of the UCPRM, which includes the integration of the Cyber-Physical Attack Graph (CPAG) and the novel Kinetic Impact Score

(KIS). This framework represents a necessary paradigm shift, offering practitioners and policy-makers a mechanism to move beyond simplistic IT risk metrics and align security resource allocation with the true physical and safety imperatives of critical infrastructure.

2. Methods: The Unified Cyber-Physical Risk Management (UCPRM) Framework

The UCPRM Framework is a structured, four-phase, continuous-loop methodology for comprehensive risk management in CPS environments, designed to supersede the limitations of static, siloed risk assessment approaches.

2.1. Foundational Architecture and Core Principles

The UCPRM architecture is founded upon three non-negotiable core principles that guide its implementation:

Principle 1: Holistic Integration. Risk assessment must be conducted on a fused IT/OT asset base. This requires incorporating the security requirements of both domains—for example, accepting low network bandwidth (OT) while demanding high integrity (IT/OT) and maximum availability (OT). The framework explicitly mandates the inclusion of system safety and physical consequence alongside traditional confidentiality and integrity concerns.

Principle 2: Real-Time Dynamism. The framework moves decisively from periodic risk assessments to a continuous, real-time risk loop. The risk score for an asset or system component must be dynamically updated based on continuous telemetry data, network traffic analysis, and newly identified threat intelligence. This ensures that the risk posture reflects the current operational state, not a snapshot from months prior.

Principle 3: Quantitative Consequence Mapping. The methodology necessitates the translation of cyber and physical vulnerabilities into measurable financial and safety consequences. Qualitative rankings are replaced by calculated scores based on physical damage potential, cost of repair, loss of service revenue, and human safety risk.

The architectural flow of the UCPRM Framework is structured around a continuous loop, starting with asset identification and culminating in continuous risk treatment and monitoring.

2.2. Asset Identification and Criticality Analysis

The initial step in the UCPRM Framework involves a comprehensive inventory that explicitly distinguishes between IT assets (e.g., enterprise servers, firewalls) and OT assets (e.g., PLCs, Remote Terminal Units (RTUs), Human-Machine Interfaces (HMIs), sensors). For each asset, a detailed Asset Criticality Score (ACS) must be calculated, prioritizing components based on their impact on system safety and mission continuity.

The ACS is a composite score determined by three main factors:

System Dependency: The number of critical downstream physical or control processes reliant on the asset.

Maximum Tolerable Downtime (MTD): The defined maximum time a component can be inoperative before catastrophic failure occurs. For safety-critical OT assets, MTD can be measured in milliseconds or seconds.

Physical-Dependency Index: A measure of the asset's direct control over a kinetic element (e.g., a valve actuator has a higher index than a simple temperature sensor).

The resultant ACS drives the resource allocation, ensuring that the most critical, safety-dependent components receive the highest level of security scrutiny and control implementation. This step forces a system-wide view, acknowledging that a compromised low-cost sensor, if critical to a control loop, may be assigned a higher risk priority than a high-cost but non-essential IT server.

2.3. Threat and Vulnerability Modeling in the Interdependent Domain

Modeling in a CPS environment demands moving beyond simple network scanning to an analysis of complex, multi-stage attack vectors that traverse the IT/OT boundary.

The Cyber-Physical Attack Graph (CPAG)

The UCPRM Framework mandates the construction of a Cyber-Physical Attack Graph (CPAG). A CPAG is a directed graph where nodes represent states of the system (e.g., "Firewall compromised," "PLC parameter altered," "Pump over-pressurized"), and edges represent exploit steps or attack actions. The CPAG is distinct from standard attack graphs because it explicitly models the transition points between the cyber and physical domains.

For example, a CPAG models how:

An initial cyber action (e.g., exploit of an HMI vulnerability) leads to

A control action (e.g., sending a spurious command to a PLC) which ultimately causes

A physical effect (e.g., damaging a turbine, leading to a loss of physical integrity).

The CPAG enables a visual and analytical representation of cascading failures, highlighting the critical pathways that an attacker can exploit to achieve a physical consequence.

Continuous Vulnerability and Anomaly Detection

To satisfy the dynamism principle, the UCPRM integrates continuous, real-time vulnerability data. This involves:

OT Protocol Analysis: Deep packet inspection specifically for industrial protocols (e.g., Modbus, DNP3) to detect non-standard commands or unauthorized parameter changes.

Machine Learning (ML) for Anomaly Detection: Utilizing time-series analysis on operational telemetry (e.g., temperature, pressure, flow rates) to establish a baseline of "normal" physical behavior. Deviations from this baseline, even if network traffic appears normal, trigger a risk update, often providing the earliest indication of a sophisticated, targeted attack like sensor spoofing.

The output of this modeling phase is a calculated Likelihood Score for each critical attack pathway identified in the CPAG, which is continuously adjusted based on real-time ML anomaly scores and vulnerability disclosures.

2.4. Real-Time Risk Quantification Methodology

The core of the UCPRM Framework is its quantitative methodology for risk calculation, which explicitly addresses the kinetic reality of CPS.

The UCPRM Risk Equation

The framework utilizes a modified risk equation that ensures all components of the system's true vulnerability are factored into the overall score:

$$\text{Risk}_{\text{UCPRM}} = \text{Likelihood} \times \text{Impact}_{\text{Total}}$$

Where $\text{Impact}_{\text{Total}}$ is a comprehensive measure incorporating both conventional cyber impact and the new **Kinetic Impact Score (KIS)**.

$$\text{Impact}_{\text{Total}} = \alpha \cdot \text{Impact}_{\text{Cyber}} + \beta \cdot \text{KIS}$$

α and β are weighting factors, where β is weighted higher for critical infrastructure to reflect the priority of safety and availability.

The Kinetic Impact Score (KIS)

The KIS is the innovative metric at the heart of the UCPRM. It translates the consequence of a cyber-physical failure into a quantified, measurable score that is easily understood by both technical operators and executive decision-makers. The KIS is a function of three primary factors, each assigned a quantitative score:

Safety Consequence ("S"): Quantified based on the potential for human injury or fatality resulting from the system failure. This is often benchmarked against industrial safety standards. (e.g., S $\in$[0,10], where 10 represents catastrophic loss of life potential).

Physical Damage Consequence ("P"): The monetized cost of equipment replacement, repair, and environmental cleanup directly resulting from the physical failure (e.g., cost in millions of USD).

Mission Continuity Consequence ("M"): The monetized cost of service interruption (e.g., lost revenue, contractual penalties, and public confidence loss) for the duration of the Maximum Tolerable Downtime (MTD).

The KIS is formally defined as:

"KIS"="Function" ("S" ,"P" ,"M")

The key to the UCPRM's real-time nature is the continuous feedback loop. Operational telemetry data (e.g., sensor readings, control loop timings) are used to continuously refine the Likelihood component. For instance, high network latency (a cyber metric) combined with abnormal pressure readings (a physical metric) in a water pipe will drastically and instantly increase the calculated 〖"Risk"〗_"UCPRM" for that section of the network, enabling predictive alerting before a failure state is fully reached.

3. Results: Implementation and Analysis of the UCPRM Framework

3.1. Case Study Selection and Setup

To validate the UCPRM Framework, a simulated Smart Grid Substation Testbed was selected as the critical infrastructure case study. The testbed environment consisted of a physical-layer model (simulating circuit breakers, protective relays, and current transformers) connected to a realistic cyber-layer model (simulating a SCADA network with HMIs, data historians, and communication gateways).

Two primary classes of attack scenarios were used for the evaluation:

Integrity Attack (Stuxnet-like): The attacker gains access to the HMI layer, tampers with the PLC logic to cause excessive cycling of a circuit breaker, while simultaneously feeding false data to the operator's screen (spoofing the sensors).

Availability Attack (DDoS/Jamming): The attacker executes a Distributed Denial of Service (DDoS) attack on the SCADA server and a spoofing-jamming attack on the wireless communication channels, effectively

disrupting communication between the control center and the field devices.

3.2. Quantification of Cyber-Physical Attack Risk

The CPAG was applied to the substation architecture, clearly illustrating how a breach in the corporate IT network (e.g., phishing leading to VPN access) could pivot into the OT network, eventually corrupting the protective relay logic.

Figure 1. Comparative Risk Assessment: Traditional IT vs. UCPRM Kinetic Impact Score for PLC Manipulation Attack. This infographic highlights how traditional IT-centric risk models (left, showing "Medium" risk) significantly underestimate the true threat compared to the UCPRM Framework's Kinetic Impact Score (right, showing "Extreme" risk), which explicitly quantifies physical and monetary consequences (e.g., 15M+ in damage).

For the Integrity Attack scenario, the key results demonstrated the significant disparity between the UCPRM assessment and a traditional IT-centric risk model:

Risk Metric	**Traditional IT Risk Model Score (Based on CIA)**	**UCPRM Framework Score (RiskUCPRM)**	**Key Impact Rationale**
Integrity Attack (PLC Manipulation)	Medium (Data Integrity Loss)	**Extreme**	KIS: S=9 (Arc Flash Hazard), P=$5M (Equipment Destruction), M=$10M (Regional Blackout).

Availability Attack (DDoS on SCADA)	High (Service Interruption)	**High-Extreme**	KIS: S=4 (Delayed Response), P=$1M (Minor Equipment Failure), M=$5M (Operational Downtime).

The key takeaway is that the traditional model, focused primarily on the cyber event (e.g., data loss, unauthorized access), assigned a Medium risk score to the PLC manipulation because the compromised data was not high-value intellectual property. In contrast, the UCPRM Framework, through the calculation of the KIS, correctly identified this attack as Extreme risk, due to the high-probability consequence of physical destruction and human safety threat. This clear disparity validates the UCPRM's core hypothesis: Traditional models fundamentally underestimate the true risk profile of CPS.

3.3. Real-Time Risk Monitoring and Alerting

The testbed was subjected to a slow, methodical integrity attack over a period of 48 hours, simulating a sophisticated, low-and-slow intruder.

- Traditional Monitoring: Only detected the attack at the 40-hour mark when the false data injection caused a visible anomaly on the operator's HMI screen. This is a reactive alert.
- UCPRM Monitoring: The real-time component of the framework constantly monitored the calculated 〖"Risk" 〗_"UCPRM" score.
- At the 12-hour mark, the ML-based anomaly detector (Section 2.3) detected a subtle, statistically insignificant increase in control-loop latency (a cyber metric). The Risk Score increased slightly.
- At the 24-hour mark, the system detected a corresponding minor, non-critical oscillation in the simulated pressure telemetry (a physical metric).
- The combined increase in both the Likelihood (due to latency anomaly) and the pre-calculated KIS (due to the potential for catastrophic failure) triggered a Predictive Alert at the 25-hour mark. This provided a 15-hour window of opportunity for mitigation before the attack became visible to the human operator.

This result demonstrates the UCPRM's ability to provide predictive capabilities. By integrating and correlating subtle anomalies across both the cyber and physical telemetry, the framework significantly reduces the mean time to detection (MTTD) for sophisticated, multi-stage threats, directly enhancing the overall resilience of the CPS.

4. Discussion

4.1. Interpretation of Findings and Comparative Advantage

The empirical results from the Smart Grid testbed confirm a critical finding: relying solely on risk assessment methodologies designed for corporate IT environments will inevitably lead to a profound misallocation of security resources within a CPS. By quantifying the consequences of cyber actions in terms of the Kinetic Impact Score (KIS), the UCPRM Framework provides a risk metric that is directly relevant to the core mission of critical infrastructure: safety and continuity. The demonstrated difference in risk scoring—where a "Medium" IT-centric risk was correctly re-classified as an "Extreme" safety risk—is a compelling argument for the paradigm shift advocated by this research.

The framework's continuous, real-time nature provides a substantial comparative advantage over static models. By using dynamic data to update the Likelihood component of the risk equation, the UCPRM allows asset owners to visualize a continually evolving threat landscape. This dynamism transforms risk assessment from an academic exercise into a crucial, always-on operational intelligence tool, supporting immediate, context-aware decision-making. Furthermore, the systematic integration of established international standards (ISO 31000, NIST) within the structured UCPRM methodology ensures that its implementation is systematic and auditable, aligning high-level governance with granular technical controls.

4.2. The Interplay of Organizational Risk and Technological Resilience

While the UCPRM Framework successfully addresses the technical shortcomings of past methodologies by quantifying kinetic impact, the successful deployment and long-term efficacy of the model are intrinsically

linked to corresponding advances in organizational risk management and technological resilience. A risk framework, no matter how technically sophisticated, is ultimately a tool for informing human decisions and guiding organizational behavior. Achieving true security involves a deep and continuous merger of Enterprise Risk Management (ERM) principles with the calculated technological risk derived from the UCPRM. This necessitates a detailed examination of the human element, architectural design, and regulatory governance.

Seamless Integration of ERM and Technology

The UCPRM's Kinetic Impact Score (KIS) provides the necessary quantitative link for integration with Enterprise Risk Management (ERM). Historically, security incidents were logged as IT events, separate from organizational risk factors like financial stability or regulatory compliance. By translating the attack consequence into a clear monetary value P and M components of the KIS), the UCPRM allows security teams to present risks in the common language of business risk and financial impact. This enables boards and executive leadership to make informed trade-offs: for example, justifying the high cost of implementing a new, robust OT firewall ("Risk Treatment") against the calculated risk exposure (e.g., 15M loss potential) identified by the KIS. The ERM function then becomes the oversight mechanism that ensures the UCPRM is appropriately governed, resourced, and integrated into strategic decision-making. The organizational appetite for risk—the threshold at which a risk is deemed acceptable or requires immediate mitigation—must be defined in terms of the KIS, creating a clear, quantitative policy boundary for both the cyber and physical domains.

The Role of Human Factors and Organizational Vulnerabilities

Technological vulnerabilities are only one half of the CPS security equation; the other is the human element. Organizational behavior, human error, and insider threat represent vectors that are challenging for purely technological risk models to capture.

Human Error in Configuration and Maintenance: Studies consistently show that a significant portion of security failures trace back to misconfigurations, inadequate patching practices, or failure to follow procedural safeguards. The UCPRM must therefore incorporate a Human Vulnerability Factor (HVF) into its overall risk calculation. This factor could be derived from an assessment of staff training levels, adherence to security protocols (e.g., audit trails of unauthorized modifications), and the effectiveness of a facility's safety culture.

The Insider Threat: The insider—whether malicious or negligent—possesses the knowledge and access necessary to bypass perimeter security, making them a uniquely potent threat to a CPS. The UCPRM's CPAG can be enhanced to include insider-specific attack paths, where the initial compromise step is simply "Local Authentication Granted" or "Authorized Privilege Abuse." The Likelihood for these pathways must be dynamically updated based on behavioral analytics and access monitoring, recognizing that even authorized activity can become anomalous and therefore high-risk.

A robust UCPRM implementation must enforce strict governance and separation of duties across the IT and OT teams, ensuring that no single individual possesses the access or knowledge to execute a catastrophic cyber-physical attack chain independently.

Enhancing System Resilience through Architectural Design

Managing risk is not solely about prevention; it is equally about resilience—the system's capacity to absorb an attack and rapidly recover with minimal mission interruption. The KIS serves as a critical guide for designing resilience-focused architectural controls.

Network Segmentation and Air-Gapping: The UCPRM's CPAG analysis will inherently prioritize the mitigation of the highest-risk attack paths. For CPS, the most effective mitigation often involves strict network segmentation (using specialized firewalls to isolate the OT network) or, where feasible, air-gapping safety-critical systems entirely. The cost-benefit analysis for implementing these demanding architectural controls can be directly justified by the reduction in the potential KIS score.

The Role of Resilient Control Loops: Moving beyond standard fault tolerance, CPS must adopt resilient control loops capable of operating safely even when communication with the central SCADA system is lost. This includes implementing local, autonomous protective functions (e.g., independent safety PLCs) that can take an immediate, pre-programmed safe action (e.g., emergency shutdown) if they detect anomalies or loss of control signals. This design philosophy fundamentally breaks the attack chain modelled by the CPAG, minimizing the potential physical impact.

Robust Recovery Mechanisms: The "M" component of the KIS emphasizes the cost of service interruption. Minimizing this impact requires investing in robust,

immutable backups of control system configurations, secure and rapid failover capabilities, and a detailed, tested Cyber-Physical Incident Response Plan. This plan must not only address restoring data but also verifying the physical integrity of field devices after a cyber-attack to ensure the system is safe to restart—a crucial, OT-specific recovery step.

Policy and Governance Implications

The implementation of a UCPRM Framework has profound implications for regulatory policy and organizational governance. Regulatory bodies, such as those governing the power and water sectors, must evolve their standards to explicitly mandate the quantification of kinetic risk.

Mandating Kinetic Risk Reporting: Future regulatory frameworks should move beyond prescriptive security checklists (like basic password policies) to performance-based metrics centered on the KIS. Companies should be required to report their calculated maximum potential KIS and demonstrate controls that reduce this score to an acceptable organizational level. This fosters a culture of outcome-driven security.

Establishing Cross-Domain Security Teams: Effective governance requires breaking down the traditional organizational wall between the Chief Information Security Officer (CISO) and the Vice President of Operations. The UCPRM necessitates a unified Cyber-Physical Security Steering Committee—an organizational structure responsible for overseeing the framework's implementation, managing the joint IT/OT risk register, and ensuring that security investments align with the holistic risk profile. This joint committee ensures that security decisions account for the real-time operational constraints of the physical plant while simultaneously addressing the sophisticated threats originating from the cyber domain. The organizational commitment to this unified governance structure is as vital to the success of the UCPRM as any of its technical components.

The comprehensive integration of ERM principles, human factors, resilient architecture, and evolving policy is what elevates the UCPRM from a superior technical tool to a foundational organizational strategy for ensuring the enduring security and resilience of global critical infrastructure.

4.3. Limitations and Future Research

While the UCPRM Framework represents a significant advancement, several limitations warrant acknowledgment. First, the accuracy of the 〖"Risk" 〗_"UCPRM" score is fundamentally dependent on the quality and fidelity of the real-time sensor and telemetry data. Noisy, incomplete, or malicious sensor readings can compromise the Likelihood calculation and the precision of the KIS, creating a security risk associated with the security model itself. Second, the computational complexity involved in continuously generating and updating the Cyber-Physical Attack Graph (CPAG) for large-scale, highly interconnected CPS (e.g., a national power grid) remains a non-trivial challenge.

Future research should focus on three key areas:

Automated CPAG Generation: Developing machine learning algorithms that can automatically generate and prune the CPAG from industrial network traffic, configuration files, and control logic, thereby reducing manual effort and enabling real-time scalability.

Incorporating Game Theory: Integrating adversarial modeling, specifically using game theory, to predict optimal attack strategies by rational adversaries. This would move the Likelihood component of the UCPRM from an anomaly-driven score to a truly predictive and adversarial-aware metric.

Extending to Fully Autonomous Systems: Adapting the UCPRM to account for the unique safety and security risks inherent in increasingly autonomous CPS, where human oversight is minimal, and decision-making is fully managed by AI and machine learning components.

4.4. Conclusion

The digital transformation of critical infrastructure has rendered traditional, siloed security models obsolete. The security of Cyber-Physical Systems is an existential challenge demanding an approach that unifies the cyber and physical domains. The Unified Cyber-Physical Risk Management (UCPRM) Framework successfully delivers this necessary paradigm shift. By introducing the Kinetic Impact Score (KIS), the UCPRM provides a quantitative mechanism to align security investments with actual physical safety and continuity imperatives. Furthermore, its reliance on a real-time, dynamic risk loop enables predictive alerting and a substantial reduction in the window of vulnerability. This research confirms that the imperative for critical infrastructure security is to move decisively toward integrated, quantitative, and real-time risk methodologies, ensuring the enduring resilience of the systems that underpin modern society.

References

1. Wu, W.; Kang, R.; Li, Z. Risk assessment method for cyber security of cyber physical systems. In Proceedings of the 2015 First International

Conference on Reliability Systems Engineering (ICRSE), Beijing, China, 21–23 October 2015.

2. Kim, K.-D.; Kumar, P. An overview and some challenges in cyber-physical systems. J. Indian Inst. Sci. 2013, 93, 341–352.
3. Abouzakhar, N. Critical Infrastructure Cybersecurity: A Review of Recent Threats and Violations. In Proceedings of the European Conference on Information Warfare and Security, Jyväskylä, Finland, 11–12 July 2013.
4. Marvell, S. The Real and Present Threat of a Cyber Breach Demands Real-Time Risk Management; Acuity Risk Management: London, UK, 2015.
5. Adar, E.; Wuchner, A. Risk management for critical infrastructure protection (CIP) challenges, best practices & tools. In Proceedings of the First IEEE International Workshop on Critical Infrastructure Protection (IWCIP'05), Darmstadt, Germany, 3–4 November 2005.
6. Marvell, S. Real-Time Cyber Security Risk Management. ITNOW 2015, 57, 26–27.
7. Harvey, J.; Service, T.I. Introduction to Managing Risk. Available online: http://www.cimaglobal.com/Documents/ImportedDocuments/cid_tg_intro_to_managing_rist.apr07.pdf (accessed on 29 May 2018).
8. Georgieva, K.; Farooq, A.; Dumke, R.R. Analysis of the Risk Assessment Methods–A Survey. In International Workshop on Software Measurement; Springer: Berlin, Germany, 2009.
9. Cherdantseva, Y.; Burnap, P.; Blyth, A.; Eden, P.; Jones, K.; Soulsby, H.; Stoddart, K. A review of cyber security risk assessment methods for SCADA systems. Comput. Secur. 2016, 56, 1–27.
10. Patel, S.C.; Graham, J.H.; Ralston, P.A. Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements. Int. J. Inf. Manag. 2008, 28, 483–491.
11. Hahn, A.; Ashok, A.; Sridhar, S.; Govindarasu, M. Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. IEEE Trans. Smart Grid 2013, 4, 847–855.
12. Cárdenas, A.A.; Amin, S.; Lin, Z.S.; Huang, Y.L.; Huang, C.Y.; Sastry, S. Attacks against process control systems: Risk assessment, detection, and response. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, Hong Kong, China, 22–24 March 2011.
13. Peng, Y.; Lu, T.; Liu, J.; Gao, Y.; Guo, X.; Xie, F. Cyber-physical system risk assessment. In Proceedings of the Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Beijing, China, 6–18 October 2013.
14. Cardenas, A.; Amin, S.; Sinopoli, B.; Giani, A.; Perrig, A.; Sastry, S. Challenges for securing cyber physical systems. In Proceedings of the Workshop on Future Directions in Cyber-Physical Systems Security, Newark, NJ, USA, 23–24 July 2009.
15. Sridhar, S.; Hahn, A.; Govindarasu, M. Cyber–physical system security for the electric power grid. Proc. IEEE 2012, 100, 210–224.
16. Yoneda, S.; Tanimoto, S.; Konosu, T.; Sato, H.; Kanai, A. Risk Assessment in Cyber-Physical System in Office Environment. In Proceedings of the 2015 18th International Conference on Network-Based Information Systems (NBiS), Taipei, Taiwan, 2–4 September 2015.
17. Ten, C.-W.; Manimaran, G.; Liu, C.-C. Cybersecurity for critical infrastructures: Attack and defense modeling. IEEE Trans. Syst. Man Cybern. Part A Syst. Hum. 2010, 40, 853–865.
18. Gai, K.; Qiu, M.; Ming, Z.; Zhao, H.; Qiu, L. Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks. IEEE Trans. Smart Grid 2017, 8, 2431–2439.
19. Gai, K.; Qiu, M.; Zhao, H.; Tao, L.; Zong, Z. Dynamic energy-aware cloudlet-based mobile cloud computing model for green computing. J. Netw. Comput. Appl. 2016, 59, 46–54.
20. Gai, K.; Qiu, M. Blend arithmetic operations on tensor-based fully homomorphic encryption over real numbers. IEEE Trans. Ind. Inform. 2017.
21. Ray, P.D.; Harnoor, R.; Hentea, M. Smart power grid security: A unified risk management approach. In Proceedings of the 2010 IEEE International Carnahan Conference on Security Technology (ICCST), San Jose, CA, USA, 5–8 October 2010.
22. Yadav, D.; Mahajan, A.R. Smart Grid Cyber Security and Risk Assessment: An Overview. Int. J. Sci. Eng. Technol. Res. 2015, 4, 3078–3085.
23. Rice, E.B.; AlMajali, A. Mitigating the risk of cyber attack on smart grid systems. Procedia Comput. Sci. 2014, 28, 575–582.
24. ISO. Risk Management—Principles and Guidelines; ISO 31000:2009; International Organization for Standardization: Geneva, Switzerland, 2009.

25. GOST-R. Risk Management. Risk Assessment Methods; ISO/IEC 31010-2011; International Organization for Standardization: Geneva, Switzerland, 2009.
26. Cybersecurity, C.I. Framework for Improving Critical Infrastructure Cybersecurity. Available online: http://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf (accessed on 29 May 2018).
27. Purdy, G. ISO 31000:2009—Setting a new standard for risk management. Risk Anal. 2010, 30, 881–886.
28. Islam, S.; Fenz, S.; Weippl, E.; Mouratidis, H. A Risk Management Framework for Cloud Migration Decision Support. J. Risk Financial Manag. 2017, 10, 10.
29. Islam, S.; Mouratidis, H.; Weippl, E.R. An empirical study on the implementation and evaluation of a goal-driven software development risk management model. Inf. Softw. Technol. 2014, 56, 117–133.
30. Berg, H.-P. Risk management: Procedures, methods and experiences. Risk Manag. 2010, 1, 79–95.
31. CISO. Information Risk Assessment Handbook. Available online: http://www.nationalarchives.gov.uk/documents/information-management/risk-assessment-handbook.pdf (accessed on 29 May 2018).
32. Prassanna Rao Rajgopal, Badal Bhushan, & Ashish Bhatti. (2025). Vulnerability Management at Scale: Automated Frameworks for 100K+ Asset Environments. Utilitas Mathematica, 122(2), 897–925. Retrieved from https://utilitasmathematica.com/index.php/Index/article/view/2788
33. AIRMIC; ALARM; IRM. A Structured Approach to Enterprise Risk Management (ERM) and the Requirements of ISO 31000; The Public Risk Management Association: London, UK, 2010.
34. NERC, CIP. Standards as Approved by the NERC Board of Trustees May 2006; North American Electric Reliability Corporation: Atlanta, GA, USA, 2006.
35. 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
36. Bialas, A. Risk management in critical infrastructure—Foundation for its sustainable work. Sustainability 2016, 8, 240.
37. Rahman, A.A.L.A.; Islam, S.; Kalloniatis, C.; Gritzalis, S. A Risk Management Approach for a Sustainable Cloud Migration. J. Risk Financial Manag. 2017, 10, 20.
38. Ani, U.P.D.; He, H.; Tiwari, A. Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective. J. Cyber Secur. Technol. 2017, 1, 32–74.
39. Ezell, B.C. Infrastructure Vulnerability Assessment Model (I-VAM). Risk Anal. 2007, 27, 571–583.
40. Parnell, G.S.; Conley, H.W.; Jackson, J.A.; Lehmkuhl, L.J.; Andrew, J.M. Foundations 2025: A value model for evaluating future air and space forces. Manag. Sci. 1998, 44, 1336–1350.
41. 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
42. Blank, R.; Gallagher, P. NIST Special Publication 800-30 Revision 1 Guide for Conducting Risk Assessments; Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2012.
43. Baldoni, R. Critical Infrastructure Protection: Threats, Attacks, and Counter-Measures. Technical Report. Available online: http://www.dis.uniroma1.it/~tenace/download/deliverable/Deliverable4a.pdf (accessed on 29 May 2018).
44. Utne, I.B.; Hokstad, P.; Kjølle, G.; Vatn, J.; Tøndel, I.; Bertelsen, D.; Fridheim, H.; Røstum, J. Risk and vulnerability analysis of critical infrastructures-The DECRIS approach. In Proceedings of the SAMRISK Conference, Oslo, Norway, 6–7 March 2008.
45. Parate, H., Madala, P., & Waikar, A. (2025). Equity and efficiency in TxDOT infrastructure funding: A per capita and spatial investment analysis. Journal of Information Systems Engineering and Management, 10(55s). https://www.jisem-journal.com/
46. Durgam, S. (2025). CICD automation for financial data validation and deployment pipelines. Journal of Information Systems Engineering and Management, 10(45s), 645–664. https://doi.org/10.52783/jisem.v10i45s.8900