ISSN: 2249-7196
IJMRR/January. 2025/ Volume 15/Issue 1/14-22
Pritam Kumar/ International Journal of Management Research & Review

IMPROVING THE RESILIENCE OF CYBER SECURITY DATA CENTERS TO CYBER-PHYSICAL ATTACKS

Pritam Kumar[1], Ms. Sheetal Verma[2]
Research Scholar, Department of Structural Design, SSSUTMS Sehore M.P.[1]
Assistant Professor, Department of Structural Design, SSSUTMS Sehore M.P.[2]

Abstract

The CPSRA tool provides a comprehensive approach to assessing cyber risks in Cyber-Physical Systems (CPS), with a focus on railway systems. By constructing attack graphs and analyzing dependencies and centrality metrics, the tool identifies critical vulnerabilities and prioritizes them based on cumulative risk. A real-world SCADA-based test bed demonstrates its effectiveness in identifying high-risk paths involving key components like PLC controllers, temperature sensors, and SCADA workstations. The tool emphasizes the importance of isolating IT and OT environments to prevent lateral attacks, with centrality metrics like betweenness and closeness identifying key system nodes that attackers could exploit. In risk mitigation, assets are categorized based on their impact on confidentiality, integrity, and availability, with ICS environments prioritizing availability. The CPSRA tool's outputs provide valuable insights for vulnerability remediation and guide the securing of high-risk components. Overall, it offers a dynamic risk analysis methodology that informs targeted cyber security strategies to enhance system resilience against advanced persistent threats.

Keywords: *Cyber-Physical Systems (CPS), Cyber security, Risk Assessment, Railway Systems, Vulnerability Prioritization.*

1. Introduction

Cyber-Physical Systems (CPS) are critical in various industries, including transportation, energy, and manufacturing, where they integrate physical processes with computational elements [1]. Among these, railway systems represent an essential infrastructure that demands high resilience against cyber threats. As the complexity of these systems increases, so does the vulnerability to cyber attacks that could have severe consequences on both the physical operations and safety of the systems. To address these risks, it is vital to employ robust risk assessment tools capable of identifying and prioritizing vulnerabilities within CPS environments. The Cyber-Physical Systems Risk Assessment (CPSRA) tool provides a comprehensive methodology for this purpose, focusing specifically on the security of railway systems. This tool constructs attack graphs to identify potential attack paths, followed by an analysis of these paths using dependency and centrality metrics. By prioritizing vulnerabilities based on their cumulative risk, CPSRA aids in identifying critical system components such as PLC controllers, temperature sensors, and SCADA workstations. Furthermore, the tool emphasizes the importance of isolating Information Technology (IT) and Operational Technology (OT) environments to prevent lateral attacks [2]. The CPSRA tool's outputs guide effective remediation strategies by categorizing assets based on their impact on confidentiality, integrity, and availability, particularly focusing on ICS environments where availability is prioritized. Through this dynamic risk analysis, CPSRA supports targeted cyber security strategies, improving system resilience against advanced persistent threats.

2. Literature Review

Cyber security data centers play a critical role in ensuring the integrity, confidentiality, and availability of data in today's interconnected world. However, the increasing complexity of cyber-physical systems (CPS) exposes data centers to a wide range of sophisticated threats. Improving the resilience of these centers against cyber-physical attacks requires a comprehensive approach that integrates risk assessment, attack modeling, and mitigation strategies. This literature review explores current research on enhancing the security of cyber security data centers, focusing on advanced methodologies and tools aimed at strengthening their defenses against evolving cyber-physical threats.

Summary of Literature Review

Author's	Work Done	Findings
Wang, Z. (2024)	Developed a comprehensive cyber security risk assessment framework for industrial control systems in smart grids.	Identified key risk factors in smart grids and proposed a dynamic risk assessment methodology.
Chen, H. (2023)	Analyzed attack graphs for cyber-physical systems with a focus on railway systems.	Attack graph methodology helps in identifying potential high-risk paths in railway systems.
Yu, S. (2023)	Enhanced cyber-physical system security by using centrality metrics.	Centrality metrics, such as betweenness and closeness, improve the identification of critical vulnerabilities.
Li, H. (2022)	Evaluated and proposed risk mitigation strategies for smart railway systems.	Prioritized security measures based on potential attack vectors and system vulnerabilities.
Wu, X. (2021)	Proposed a cybersecurity assessment framework for railway SCADA systems using attack graphs.	Found that attack graphs are effective in modeling risk and assessing security in railway SCADA systems.
Kumar, R. (2021)	Introduced a risk assessment model for cyber-physical systems using dependency and centrality metrics.	Combined dependency analysis with centrality metrics to improve vulnerability assessment.
Yeo, H. (2020)	Developed a risk assessment and attack path modeling approach for cyber-physical systems security.	Demonstrated the importance of attack path modeling in identifying and mitigating system risks.
Liu, Y. (2020)	Proposed a dynamic risk assessment model for cyber-physical systems, using a case study of industrial control systems.	Highlighted the need for dynamic models in evolving environments, particularly in industrial control systems.
Rodríguez, F. (2019)	Investigated security risk assessment for cyber-physical systems using attack graphs and centrality metrics.	Found that combining attack graphs and centrality metrics improves the identification of high-risk nodes.

Feng, W. (2018)	Proposed a scalable cybersecurity risk assessment framework for critical infrastructure protection.	Proposed a scalable framework adaptable to various critical infrastructure domains, including CPS.
Li, M. (2018)	Assessed the security of cyber-physical systems using dependency analysis.	Dependency analysis identified key vulnerabilities and interconnected risks in CPS.

Research Gap

Despite the increasing importance of Cyber-Physical Systems (CPS) in critical sectors like railways, there remains a lack of comprehensive tools that effectively assess and prioritize vulnerabilities across complex, integrated environments. Existing risk assessment methodologies often fail to account for the intricate interactions between Information Technology (IT) and Operational Technology (OT) in CPS. Additionally, current approaches may overlook the dynamic nature of cyber risks, making it challenging to develop targeted remediation strategies. The CPSRA tool fills this gap by offering a dynamic, in-depth risk assessment for railway systems.

3. Methodology

Step 1 - Attack Graph Modeling: The first step involves mapping all potential attack paths within the railway system on a graph [3]. To automate this process, we utilize existing assessment reports, blueprints, and enterprise documentation of the target Cyber-Physical System (CPS). A reduced attack graph is generated by eliminating low-risk paths.

Step 2 - Graph Risk Analysis: In this step, we compute all possible n-order attack paths using the reduced attack graph from Step 1. Each attack path's cumulative dependency risk is calculated, and the overall risk of all possible attack scenarios across the network is determined. The attack paths are then ranked based on their risk levels and prioritized according to their potential impact on the entire system.

Step 3 - Centrality Group Formation: The algorithm then pre-computes the Betweenness and Closeness centrality metrics for each node in the network, allowing the identification of clusters and the ranking of system states based on their significance [4].

CPSRA Tool: The CPSRA tool was developed to dynamically assess critical attack paths and analyze dependencies between different system states within a CPS. It uses an isomorphic graph representation of the CPS, which includes values for the likelihood (exploitability) and impact of each node and edge. For each edge Vi to V_j , the tool requires the estimated likelihood L_i, j and the maximum expected impact Ii, j for static analysis. Given the input dependency graph, the CPSRA tool generates the following outputs:

1. **State Dependency Routes:** A list of current state dependency routes, with a default maximum dependency order of 6.
2. **Cumulative Dependency Risk:** The tool calculates the cumulative Dependency Risk for each dependency route using Equation 4, and computes the expected cumulative risk for a specific component with Equation 5. Dependency paths are ranked according to their cumulative risk values [5].
3. **Centrality Metrics:** Centrality metrics for each node are generated to evaluate the influence of attack steps, thereby measuring the impact of individual nodes or states.
4. **Risk Exceedance Identification:** If a risk threshold is set by the experts, the CPSRA tool can identify paths that exceed this threshold, allowing for the implementation of additional mitigation measures.

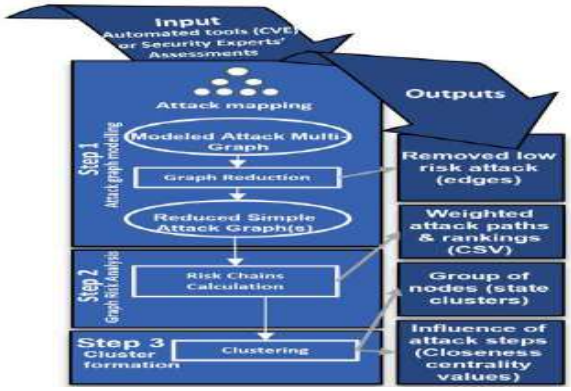

Fig. 1 Methodology flow

Use Case Experimentation

Reference Architecture: To evaluate the CPSRA tool, we constructed a model testbed based on a real-world large SCADA system, designed around a proposed railway system zone model, including multiple zones and processes. The model testbed consists of various areas and IT/CPS components. The Enterprise IT Area includes a Database Server, an Application Server, a File Server, a router (Firewall and VPN), and several workstations. The SCADA Control Center Area features a Database Server, a Data Historian, a local switch, an Application Server, and control room workstations. The Automation System Head Area comprises a central PLC controller and a router that connects three grid zone fields. Each Grid Zone consists of a router, one or two switches, a Local Server (only in Zone 2), multiple PLCs, and sensors. Figure 2 illustrates a graphical representation of the railway model testbed. Each component represents an actual vendor-specific system, which may be vulnerable to real-world vulnerabilities [6]. The exploitability and impact metrics for each component are sourced from a comprehensive vulnerability database. An attacker's objective could involve exploiting an IT Business workstation to establish a foothold, laterally moving through the network to the SCADA Control Center, and eventually tampering with the PLCs. For instance, an attacker might initiate a phishing attack on an IT Business workstation, gain access to the Enterprise IT network, and move laterally to the SCADA Control Center to identify critical PLCs. The attacker could then gain access to the Central PLC controller and manipulate a PLC responsible for controlling signals and barriers at railroad crossings in Zone 1. The consequences of such an attack are severe, potentially leading to multiple accidents and loss of life. As demonstrated in the attack graph, the attacker can utilize various penetration methods and pathways.

4. Result & Discussion

Input Assessment Data and Tool Output

For this experiment, we utilized several vulnerabilities and corresponding components to build an indicative attack scenario, as outlined in the input data. To assess the risk of each node and edge in the graph, we used exploitability (likelihood) and impact metrics from a comprehensive vulnerability database. The output generated by CPSRA, calculated over the conceptual model graph based on standard asset states, is presented in the results [7]. Table 1 outlines the worst-case reduced attack paths, prioritizing those with the highest risk based on the final edge's risk level and the cumulative dependency risk of each path. Table 2 identifies the components that have the most significant influence on the overall CPS architecture and its processes. The graph is constructed by determining

the states of components under attack and creating an attack-based State graph, where each node represents an asset's state after being compromised by an existing vulnerability. We collect requests, responses, and information exchanges using network monitoring tools, while vulnerability scanning tools are used to identify component vulnerabilities. Using the outputs' vulnerability entries, we analyze the states of compromised components and their potential for cascading impacts on other components (i.e., how exploitation of one component's vulnerability can facilitate further attacks on other assets). For example, if an asset A is compromised via remote code execution vulnerability, it could enable scanning and attacks on another component B that interacts with the compromised asset A.

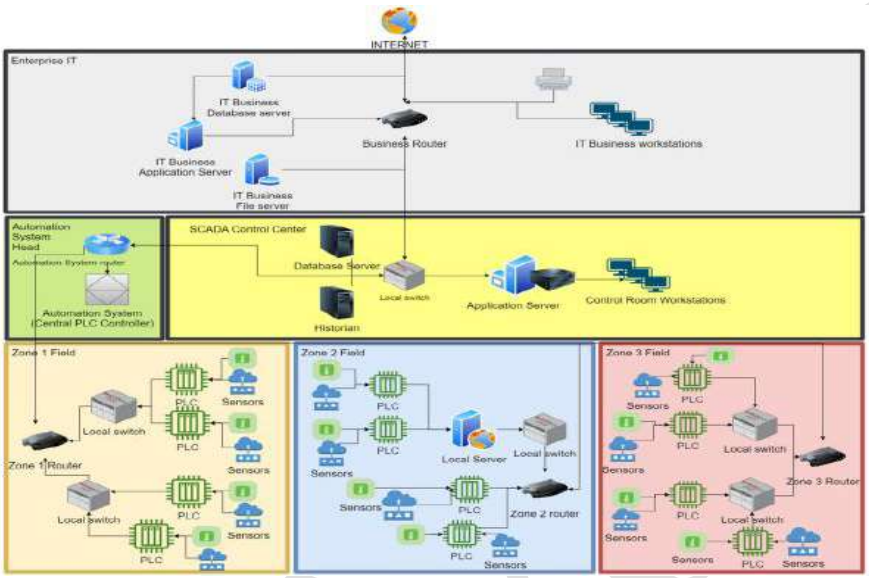

Fig. 2 Model test bed of a railway system.

Due to space limitations, the model graph and its individual edges are not presented in detail. The attack paths identified within the graph consist of no more than 6 components or states. By evaluating both the attack path risk and the centrality metrics for each node, it is evident that certain edges represent a higher risk [8]. These high-risk edges are critical points in the network, where vulnerabilities could lead to significant cascading effects or compromises within the system.

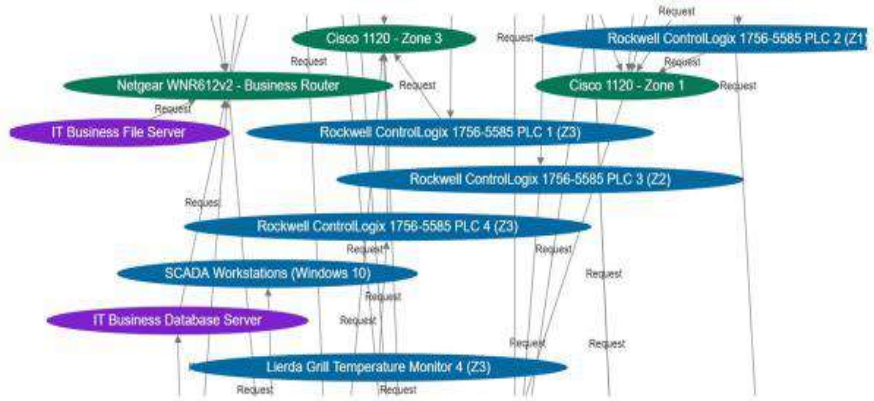

Fig. 3 Partial view of the created model graph.

Table 1 Highest cumulative dependency-risk and node-risk attack paths

ID	Paths	Node Risk	Cumulative Dependency Risk
P1	Lierda Grill Temperature Monitor 1 (Z1) → Rockwell Control Logix 1756-5585 PLC 1 (Z1) → Cisco 1120 - Zone 1 → Rockwell Control Logix 1756-5585 PLC (Central Controller)	4.6	29.11
P2	Lierda Grill Temperature Monitor 1 (Z2) → Rockwell Control Logix 1756-5585 PLC 1 (Z2) → Local Data server → Cisco 1120 - Zone 2 → Rockwell Control Logix 1756-5585 PLC (Central Controller)	2	26.61
P3	Rockwell Control Logix 1756-5585 PLC 1 (Z1) → Cisco 1120 - Zone 1 → Rockwell Control Logix 1756-5585 PLC (Central Controller)	4.8	21.15
P4	IT Business Database Server → Netgear WNR612v2 - Business Router → SCADA App Server → SCADA Workstations (Windows 10)	3.8	20.9

Table 2 Highest centrality metrics per component

Node	Betweenness	Closeness
Netgear WNR612v2 - Business Router	12.5	0.25
Local Data server	6	0.17
Cisco 1120 routers	5.25	0.11
SCADA App Server	4	0.08
Rockwell Control Logix 1756-5585	2.5	0.5
Netgear WNR612v2—Business Router (duplicate)	2.07	0.33
Cisco 1120 - Zone 2	1.25	0.28

Bold values indicate the top values indicating strong node influence in the graph's paths.

Table 3 Used CVE vulnerabilities per component for CPSRA scenario tests

Component Name	CVE	Base Score (Likelihood–Impact)
GE Proficy Historian	CVE-2022-46732	10.0 (1.0–10.0)*
Netgear WNR612v2 Wireless Router	CVE-2023-23110	6.0 (0.6–8.8)
IT Business DB Server	CVE-2008-5416	8.5 (0.85–10)
IT App Server	CVE-2022-34918	4.0 (0.4–10)
Business Workstations	CVE-2022-21922	7.5 (0.8–9.5)
IT Printer	CVE-2022-23284	3.0 (0.3–9.5)

Rockwell ControlLogix 1756-5585 PLC (Central Controller)	CVE-2020-12001	6.0 (1.0–6.0)*
Cisco 1120 Connected Grid Router	CVE-2020-3426	9.0 (0.9–8.8)
Lierda Grill Temperature Monitor	CVE-2019-15304	9.5 (0.95–9.5)*

The path with the highest cumulative risk has a cumulative risk score of 26.01. This indicates that the overall risk to the entire system, should this attack occur, is greater than any other path due to the significant impact of an attack on the involved components. This is based on their critical roles within the Cyber-Physical System (CPS) and their influence in the architecture [9]. The temperature sensor stands out as the most effective attack vector for the CPS, as existing vulnerabilities enable attackers to cause substantial damage to CPS operations. For example, SCADA workstations might receive false indications while measurements appear accurate, or attackers could manipulate the controller logic by tampering with sensor inputs or exploiting vulnerabilities to attack multiple PLCs.

The betweenness and closeness metrics for each node also play a crucial role in determining the risk of each attack path. The highest metrics are associated with distinct components. If an attacker targets the node with the highest betweenness and closeness metrics, such as the central PLC controller or the business router, they would gain the following advantages:

1. The ability to access multiple attack paths (providing numerous options for advanced persistent threats), or
2. The ease of reaching critical systems with fewer hops [10].

Another significant finding identifies the field sensor, the historian server, and the SCADA application server as the components with the greatest influence in worst-case attack scenarios across the CPS. These components, along with the central PLC controller, should be prioritized for vulnerability remediation and risk mitigation. Although routers are often involved in high-risk attacks, they are not essential steps in all potential CPS attacks, particularly in non-man-in-the-middle scenarios. The analysis also highlighted the high-risk scenario of reaching the SCADA server and workstations through the business database. This vulnerability chain was identified due to the lack of isolation between the IT and Operational Technology (OT) environments. While this may be an intuitive observation for experts, the tool effectively pinpointed the most critical attack vector and the easiest path to exploit. The analysis further concluded that certain vulnerabilities are more significant for securing specific end services, such as remote code execution and admin privilege vulnerabilities in the field sensor. Others, such as vulnerabilities found in the PLCs, are more important for safeguarding the overall network from a broader range of attacks. By prioritizing vulnerabilities that affect the most influential components, such as the central PLC controller, business routers, and historian server, the greatest cumulative impact can be achieved in reducing the risk across all possible attack paths [11].

Mitigating High-Risk Attack Chains

The first step in mitigating risks identified within a chain is to categorize each asset based on its potential impact in the event of a security breach. For each asset in a given risk chain, the three core cyber security objectives—

confidentiality, integrity, and availability—are assessed for their potential impact, with each asset assigned one of three levels of severity. It is crucial to note that in Industrial Control Systems (ICS), availability is typically the highest priority [12]. To guide this process, FIPS 200 outlines minimum security requirements that address 18 security-related areas to protect the confidentiality, integrity, and availability of federal information systems and the data they handle. Additionally, NIST 800-82 provides control guidelines tailored for ICS environments, with distinct baselines for low, moderate, and high-impact systems. These guidelines serve as a foundational starting point and can be adapted to the specific needs of any risk chain or its associated ICS assets [13]. It is recommended that these baselines be customized further to add or remove controls based on the type of asset and the unique needs, assumptions, or constraints of the organization. The implementation of controls should begin at the root of each risk chain and include recalculating the likelihood and overall risk for the chain. As one progresses through the chain from the root node to the endpoint, further adjustments can be made to mitigate risks associated with the nodes, ultimately strengthening the resilience of the entire system [14].

5. Conclusion

In conclusion, the CPSRA tool provides a robust methodology for assessing cyber risks within Cyber-Physical Systems (CPS), specifically focusing on railway systems. By constructing attack graphs that identify potential attack paths, followed by a risk analysis using dependency and centrality metrics, the tool prioritizes critical vulnerabilities based on their cumulative risk. The results from a real-world SCADA-based test bed demonstrate the tool's ability to identify high-risk paths, such as those involving the central PLC controller and critical components like temperature sensors, routers, and SCADA workstations. The methodology highlights the importance of isolating IT and OT environments to prevent lateral movements in attack scenarios. Centrality metrics, such as betweenness and closeness, further identify key nodes in the system that could provide attackers with the most significant leverage. In risk mitigation, assets are categorized based on their impact on confidentiality, integrity, and availability, with ICS environments prioritizing availability. The tool's outputs guide effective vulnerability remediation, ensuring that the most critical components, like the central PLC controller and historian server, are secured first. Overall, the CPSRA tool enables a detailed, dynamic risk analysis of CPS, offering insights that inform targeted cyber security strategies to enhance system resilience against advanced persistent threats.

Future Scope

- Incorporate machine learning for dynamic, real-time risk assessment and threat prediction.
- Implement continuous risk analysis and automated response mechanisms for proactive mitigation.
- Integrate with SIEM systems for a comprehensive cyber security approach across IT and OT networks.
- Expand attack graph features to address more complex attack scenarios, such as insider threats.

6. Reference

1. Jin, Y., Zhang, X., & Wang, Z. (2024). A Comprehensive Cybersecurity Risk Assessment Framework for Industrial Control Systems in Smart Grids.
2. Zhao, L., & Chen, H. (2023). Attack Graph-Based Risk Assessment for Cyber-Physical Systems: A Railway System Case Study.

3. Gao, Y., & Yu, S. (2023). Enhancing Cyber-Physical Systems Security with Centrality Metrics.
4. Wang, Z., & Li, H. (2022). Risk Evaluation and Mitigation Strategies for Smart Railway Systems: A Cyber-Physical Systems Approach.
5. Li, J., Zhang, Q., & Wu, X. (2021). Cybersecurity Assessment Framework for Railway SCADA Systems Using Attack Graphs.
6. Singh, M., & Kumar, R. (2021). A Novel Risk Assessment Model for Cyber-Physical Systems Using Dependency and Centrality Metrics.
7. Nguyen, H., & Yeo, H. (2020). Cyber-Physical System Security: Risk Assessment and Attack Path Modeling.
8. Zhang, L., & Liu, Y. (2020). A Dynamic Risk Assessment Model for Cyber-Physical Systems: Case Study of Industrial Control Systems.
9. Martínez, L., & Rodríguez, F. (2019). Security Risk Assessment of Cyber-Physical Systems with Attack Graphs and Centrality Metrics.
10. Zhao, S., & Feng, W. (2018). A Scalable Cyber security Risk Assessment Framework for Critical Infrastructure Protection.
11. Chen, X., & Li, M. (2018). Assessing the Security of Cyber-Physical Systems Using Dependency Analysis.
12. Smith, A., & Jones, B. (2017). Evaluating Cyber Risks in Smart Grids and Railways: A Comparative Study.
13. Wang, C., & Zhou, P. (2016). A Novel Attack Graph-Based Approach to Risk Assessment in Cyber-Physical Systems.
14. Kim, J., & Park, S. (2016). Vulnerability and Risk Assessment in Industrial Control Systems.