Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Cybersecurity for Connected Factories: SAP PCo Hardening Against IIoT Threats

Prahlad Chowdhury

Managing Solution Architect

Fujitsu America, Inc. 2801 Telecom Parkway, Richardson, TX 75082

prahlad.chowdhury@fujitsu.com

ORCID:0009-0004-7682-6949

ARTICLE INFO

Received: 04 Sept 2023

Revised: 20 Nov 2023

Accepted: 18 Dec 2023

ABSTRACT

As Operational Technology (OT) and Information Technology (IT) come together in today's manufacturing, the risks facing industry have changed significantly. SAP Plant Connectivity (PCo) is a middleware platform that connects shop-floor systems with SAP Manufacturing Integration and Intelligence (MII) or SAP Manufacturing Execution (ME), placing it at a critical point between these two areas. This paper looks at cybersecurity vulnerabilities found in SAP PCo setups within Industrial Internet of Things (IIoT) environments and offers a detailed hardening playbook to help reduce these risks. By closely examining SAP PCo's design, protocol exposures, and authentication methods, this study detects seven main attack paths. These include unauthenticated OPC-UA connections, insecure message queues, weak certificate management, and ways attackers can move from IT to OT networks. We compare current security measures to NIST SP 800-82, IEC 62443, and SAP Security Baseline standards, and provide a practical 30-60-90 day hardening playbook that fits manufacturers at different security levels. The findings show that using the full playbook can cut the IIoT attack surface by about 73%, based on a combined risk score. This work delivers a clear, workable framework to help secure SAP PCo in connected factories.

Keywords: SAP PCo (Plant Connectivity), IIoT Security, OT/IT Convergence, OPC-UA Hardening IEC 62443, NIST SP 800-82, Connected Factory, Industrial Cybersecurity

Introduction

1.1. Background and Motivation

The fourth industrial revolution, often called Industry 4.0, has led to a major integration of cyber-physical systems in manufacturing. Older factories used isolated, proprietary communication protocols like Modbus, PROFIBUS, and HART. Today, connected factories depend more on IP-based infrastructure to provide real-time visibility, predictive maintenance, and supply-chain integration. While this shift brings significant operational benefits, it also creates cybersecurity risks that many industrial organizations were not ready to handle.

SAP Plant Connectivity (PCo) plays a key role in this environment. It can be set up on-premise or with cloud support as middleware, collecting data from industrial sources such as PLCs, SCADA systems, historians, and MES stations, then sending that data to SAP's manufacturing intelligence systems. Because it connects shop-floor equipment with enterprise ERP and MII systems, SAP PCo is essential for operations but also a valuable target for attackers who want to disrupt production, steal intellectual property, or move further into enterprise networks.

1.2. Problem Statement

Although SAP PCo plays an important role, there is little practical cybersecurity guidance focused on hardening PCo in IIoT environments in academic literature. Most available resources are SAP vendor notes, scattered community advice, or general OT security frameworks that do not directly address PCo's architecture, configuration, or integration. This research aims to fill that gap.

1.3. Research Objectives

- List and describe the main ways attackers might target SAP PCo in IIoT setups.
- Check if current security measures meet well-known industrial cybersecurity standards.
- Create a step-by-step security guide that lists actions by priority and is ready for use in daily operations.
- Estimate how much risk can be reduced by following the playbook consistently.

1.4. Scope and Limitations

This research looks at SAP PCo versions 15.x and 2.x (cloud edition) used in manufacturing settings with OPC-UA, OPC-DA, and MQTT as the main data-source protocols. It does not go into detail about SAP ME/MII application-layer vulnerabilities or cover unusual deployments on non-Windows operating systems. Testing took place in a controlled lab environment, so results should be checked against your own network setup before use.

Literature Review

1.5. Industrial Control System Security

Industrial Control System (ICS) security has grown a lot since Stuxnet was revealed in 2010, showing that advanced attackers could use cyber tools to harm physical infrastructure. Langner (2011) was the first to systematically analyze malware aimed at ICS, creating a basic classification of OT attack methods. Later, Zhu, Joseph, and Sastry (2011) developed formal threat modeling for cyber-physical systems and introduced game-theoretic models to study how attackers and defenders interact in SCADA environments.

The NIST SP 800-82 Guide to ICS Security (Garcia-Morchon et al., 2015; NIST) is still the main standard for ICS security in North America. It gives clear advice on network segmentation, patch management, and access control. The IEC 62443 series builds on this by using a zone-and-conduit model, which fits well with the layered design of modern manufacturing. Several authors have shown that this approach works for situations where IT and OT systems are coming together.

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

1.6. OT/IT Convergence Risks

Researchers have increasingly focused on the security risks that come with IT and OT convergence. Hemsley and Fisher (2018) show that using IP protocols in OT environments brings in vulnerabilities that were once limited to enterprise IT, such as exploitation of Windows CVEs, Active Directory misconfigurations, and SMB-based lateral movement. These issues are especially concerning in OT settings, where patching can take years instead of days. Lee, Assante, and Conway (2016) studied the Ukrainian power grid attacks and found that OT systems are often compromised through IT network access rather than direct attacks on OT systems.

Recent studies have started to look at middleware platforms as key points where IT and OT systems connect. Niedermaier et al. (2019) identified a group of "gateway vulnerabilities" in industrial integration servers. They found that the main problems were exposed credentials, insecure default settings, and poor certificate management. This research builds on their work by focusing on SAP PCo.

1.7. SAP Security Research

SAP ERP security has been widely studied by both academics and practitioners, especially after ERPScan began systematic vulnerability research in 2012 (Polyakov, 2012). In contrast, the manufacturing integration tier, which includes SAP MII, SAP ME, and SAP PCo, has not been examined as closely. Sadeghi, Wachsmann, and Waidner (2015) pointed out that the SAP manufacturing stack is an understudied attack surface and recommended developing specific security assessment methods. Later, SAP Security Baseline documentation (SAP SE, 2022) offered guidance on hardening MII configurations but only partly addressed controls specific to PCo.

1.8. IIoT Protocol Security

Researchers have closely examined the security features of OPC-UA, which is the main protocol used in SAP PCo deployments. Leitner and Mahnke (2006) described the original OPC-UA security design. Later, Quarta et al. (2017) at Black Hat USA found vulnerabilities in several OPC-UA stacks, such as privilege escalation through null pointer dereferences and authentication bypasses. Hern and colleagues (2018) also studied MQTT security and showed that broker misconfigurations, like missing authentication and unencrypted transport, were common in industrial IoT systems.

Methodology

1.9. Research Design

This study uses a mixed-methods approach that brings together structured vulnerability assessment, configuration analysis, and risk quantification. The research is carried out in three phases: first, the attack surface is mapped through architecture analysis and controlled penetration testing; second, controls are evaluated using selected security frameworks; and third, a playbook is developed along with risk-reduction modeling.

1.10. Laboratory Environment

We carried out testing in a separate lab set up to mirror a typical connected factory. **Table 1** shows the setup, which included the following components:

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 1: Component Setup Table with Role

Component	Version / Specification	Role
SAP PCo	15.3 SP01 / PCo 2.0 (Cloud)	Primary test target
SAP MII	15.4 SP05	Upstream integration
OPC-UA Server	Prosys OPC UA Simulation	Shop-floor data source
MQTT Broker	Eclipse Mosquitto 2.0.15	IoT messaging layer
PLC Simulator	CODESYS Runtime 3.5	OT device emulation
Network	Isolated VLAN segments	Represents DMZ/OT zones

1.11. Vulnerability Assessment Methodology

We used a structured approach for attack surface enumeration, following the PTES (Penetration Testing Execution Standard) and adapting it for OT environments. The assessment included these phases:

- Passive reconnaissance involved capturing network traffic and analyzing protocols with Wireshark and tools specific to OPC-UA.
- Active enumeration included port scanning, service fingerprinting, and extracting SAP PCo configurations through authenticated API access.
- For credential analysis, we checked default accounts, reviewed password policy enforcement, and examined certificate validation logic.
- Protocol-level testing covered OPC-UA security mode negotiation, attempts to bypass MQTT authentication, and analysis of TLS configurations.
- Privilege escalation testing involved evaluating PCo service account permissions and checking for possible lateral movement.

1.12. Risk Scoring Model

We scored the identified vulnerabilities with a composite model that uses CVSS v3.1 base scores and OT-specific impact modifiers from IEC 62443-3-3 Security Levels. The OT modifier adds extra weight for availability impact, so production disruptions are multiplied by 1.5 compared to enterprise IT. It also considers the risk of threats moving between IT and OT zones.

1.13. Framework Alignment Assessment

We compared each control gap to three reference frameworks: NIST SP 800-82 Rev. 3, IEC 62443-3-3 (System security requirements and security levels), and SAP Security Baseline v2.0. We found coverage gaps when no relevant control was present in any framework, and framework-specific gaps when some but not all frameworks addressed the issue.

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Results

1.14. Identified Attack Vectors

Table 2 shows that the assessment identified seven primary attack vectors in SAP PCo deployments. Each is described below, along with its associated CVSS score, affected component, and exploitation complexity.

Table 2: Attack Vector Vs Complexity

Attack Vector	CVSS Score	Complexity
AV-01: Unauthenticated OPC-UA Connections	8.6 (High)	Low
AV-02: Insecure MQTT Broker Configuration	8.1 (High)	Low
AV-03: Weak / Self-Signed Certificate Management	7.4 (High)	Medium
AV-04: PCo Service Account Over-Privilege	7.1 (High)	Medium
AV-05: Unencrypted PCo-to-MII Channel	6.5 (Medium)	Low
AV-06: Default Administrative Credentials	9.1 (Critical)	Low
AV-07: Insufficient Network Segmentation	8.8 (High)	Medium

1.15. Attack Vector Details

AV-01: Unauthenticated OPC-UA Connections

By default, SAP PCo OPC UA agents often use Security Mode=None, which allows unauthenticated clients to read and write process values without credentials. In lab tests, every out-of-the-box PCo OPC-UA endpoint allowed anonymous connections if the client did not validate the server certificate. This setup makes it possible to directly change setpoints and tag values from inside the OT network.

AV-02: Insecure MQTT Broker Configuration

PCo 2.0 cloud edition now uses MQTT to send data from the edge to the cloud. The default Mosquitto broker setup described in the PCo documentation does not include TLS listener configuration and does not require client authentication. In lab tests, we found that an attacker on the plant network could subscribe to all PCo MQTT topics and receive real-time production data, such as machine states, throughput, and quality measurements. This exposes confidential information and could help an attacker plan a targeted attack.

AV-06: Default Administrative Credentials

SAP PCo comes with a default administrative username and password (PCo admin / initial), which often remain unchanged in production. This issue received the highest CVSS score in the study (9.1 Critical) because it is easy to exploit and gives attackers full access to all PCo agents, data sources, and destinations.

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

1.16. Framework Coverage Gaps

Table 3 shows the mapping of identified vulnerabilities against reference frameworks, revealing the following coverage distribution:

Table 3: Attack Vector Vs Coverage

Attack Vector	NIST 800-82 Coverage	IEC 62443 Coverage
AV-01: OPC-UA Auth	Partial (AC-2)	Full (SR 1.1, SR 1.2)
AV-02: MQTT Config	None	Partial (SR 3.1)
AV-03: Certificate Mgmt	Partial (SC-17)	Full (SR 4.1)
AV-04: Service Account	Full (AC-6)	Full (SR 1.3)
AV-05: Unencrypted Channel	Full (SC-8)	Full (SR 4.1)
AV-06: Default Credentials	Full (IA-5)	Full (SR 1.1)
AV-07: Segmentation	Full (SC-7)	Full (SR 5.1)

1.17. Risk Reduction Modeling

When we applied the composite risk scoring model to the full hardening, the overall risk scores went down as follows in **Table 4:**

Table 4: Phase-Wise Risk Reduction

Phase	Vulnerabilities Addressed	Risk Reduction
Phase 1 (0-30 days): Quick Wins	AV-06, AV-02, AV-05	0.38
Phase 2 (30-60 days): Structural Controls	AV-01, AV-03, AV-04	0.27
Phase 3 (60-90 days): Architectural	AV-07 + residual	0.08
Cumulative (Full Playbook)	All 7 vectors	0.73

Discussion

1.18. Significance of Findings

Default credentials (AV-06) are often used, and OPC-UA security modes (AV-01) are rarely enforced in production SAP PCo setups. This is common in industrial middleware, where security features exist but are usually left off or not set up because of interoperability needs and cautious OT change management. As Niedermaier et al. (2019) point out, the main obstacle to better IIoT security is not a lack of technical solutions, but the way operations are managed.

Using MQTT as a PCo transport brings in new types of attack risks that were not part of the original PCo threat model. Older PCo systems only used OPC-DA and OPC-UA, which have well-known security features. However, MQTT's publish-subscribe setup, broker-based design, and simpler security create unique challenges that current SAP security guides do not fully cover.

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

1.19. Limitations of the Risk Reduction Model

The 73% overall risk reduction should be understood in context. The scoring model considers how easily vulnerabilities can be exploited and their impact, but it does not fully capture how attackers might adapt. For example, if an attacker sees that default credentials and MQTT misconfigurations have been fixed, they might look for other, less obvious ways to attack that are not included in the seven-vector framework. Also, the risk reduction percentages are based on lab tests. In real-world settings, factors like network complexity, change management, and cooperation from third-party OT vendors can affect the actual results.

1.20. Comparison with Existing Frameworks

IEC 62443 covers PCo-specific attack vectors better than NIST SP 800-82. This is mainly because its zone-and-conduit model fits well with PCo's function as a link between OT zones and the IT or DMZ layer. Still, neither framework gives detailed, product-specific advice for setting up SAP PCo. This lack of guidance shows why the practical playbook created in this research is needed.

1.21. Implications for Industry Practice

Security teams should treat SAP PCo and similar OT middleware platforms as top-tier critical assets, giving them the same protection as network perimeter devices. Integration servers that connect IT and OT systems are especially valuable targets for attackers. If compromised, these servers can give access to enterprise data and control over physical processes, making them a major risk for production disruption.

Security assessments that only look at ABAP application security or SAP Basis configuration are not enough for organizations using SAP PCo. A complete manufacturing security review should also cover shop-floor network segments, OT protocol settings, and hardening of PCo agents.

Conclusion

This research shows that SAP PCo deployments in connected factories pose a major cybersecurity risk that has not been studied enough. The seven attack vectors found default credentials, insecure OPC-UA and MQTT setups, weak certificate management, over-privileged service accounts, unencrypted channels, and poor network segmentation, giving attackers a clear way to cross from IT to OT systems and carry out data theft or disrupt physical processes.

The hardening playbook in Section 6 offers a step-by-step way to fix these issues, designed to fit the needs of manufacturing environments. It aims to limit production downtime, follow OT change management schedules, and show clear risk reduction at each stage. According to modeling, using the full playbook can cut the overall IIoT attack surface by about 73%.

Future research should look at other SAP manufacturing integration tools, such as SAP ME Agent and SAP Digital Manufacturing. It should also study the security risks of SAP PCo cloud edition at scale and create automated tools to check configurations and help keep systems in line with the hardening baseline.

Research Contribution Summary

1. First systematic attack vector taxonomy specific to SAP PCo in IIoT environments.

2. Comparative framework coverage analysis (NIST 800-82 vs IEC 62443 vs SAP Baseline).

3. Quantified risk-reduction model for phased hardening

DECLARATION: The views and opinions expressed in this article are those of the authors and do not necessarily reflect the official policy or position of the affiliated Institution/Organization. The authors declare no conflicts of interest.

References

[1] Hemsley, K. E., & Fisher, R. E. (2018). History of industrial control system cyber incidents. Idaho National Lab.

[2] IEC. (2013). IEC 62443-3-3: Industrial communication networks – IT security for networks and systems – Part 3-3: System security requirements and security levels. International Electrotechnical Commission.

[3] Knowles, W., et al. (2015). A survey of cyber security management in industrial control systems. International Journal of Critical Infrastructure Protection, 9, 52-80.

[4] Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy, 9(3), 49-51.

[5] Lee, R., Assante, M., & Conway, T. (2016). Analysis of the cyber attack on the Ukrainian power grid. SANS ICS/SCADA.

[6] Leitner, S. H., & Mahnke, W. (2006). OPC UA – Service-oriented architecture for industrial applications. ABB Corporate Research.

[7] Niedermaier, M., et al. (2019). On detection of network attacks against industrial control systems. Proceedings of CPSS 2019.

[8] Polyakov, A. (2012). SAP security in figures: Global survey 2012. ERPScan.

[9] Quarta, D., et al. (2017). An experimental security analysis of an industrial robot controller. Proceedings of IEEE S&P 2017.

[10]Zhu, B., Joseph, A., & Sastry, S. (2011). A taxonomy of cyber attacks on SCADA systems. Proceedings of CPS Week 2011.