Mapping: Implementing IEC-62443 with WALLIX PAM4OT

I. Introduction

Navigating the challenging landscape of securing Industrial Automation and Control Systems (IACS) is more critical than ever in our interconnected era. This task is compounded by the integration of numerous components, diverse communication protocols, and a variety of security vulnerabilities, including issues like outdated software and inadequate access controls. The complexity is further accentuated by the escalating frequency of cyber-attacks, underscoring the immediate need for comprehensive and protective measures. As these attacks become more prevalent, safeguarding the resilience of systems in vital industries such as Manufacturing, Energy, and Transportation becomes paramount. Indeed, these sectors essentially form the backbone of our infrastructure, and the substantial risks involved emphasize the critical importance of robust security measures.

In response to this formidable challenge, industry standards like IEC-62443 have emerged as vital frameworks. They play a pivotal role in fortifying the security of these systems that rely on operational technology (OT). This strategic approach aims to address the unique challenges posed by industrial environments and provides a structured framework to enhance cybersecurity in the face of evolving threats.

The IEC-62443 series stands as a comprehensive guide, offering a wealth of concepts, methods, and measures tailored to identify and eliminate potential vulnerabilities within industrial networks and systems. Additionally, the standard encourages a consistent level of security across diverse industrial control systems, fostering trust among all stakeholders, including clients, business partners, and regulatory agencies, each with their unique perspectives and requirements. While the standard comprises four tiers (see Table 1), this document centers around the third section, labeled "System", with a specific focus on part 3-3, “System Security Requirements and Security Levels”. This segment outlines crucial aspects, including System Requirements (SR) and Requirement Enhancements (RE), essential for constructing an IACS aligned with the Target Security Level (SL-T).

Acknowledging the complexity of translating these standards into actionable steps, WALLIX takes a proactive stance, dedicated to facilitating the transition from theory to implementation. This document illustrates WALLIX's potential as a strategic partner, contributing to the development of industrial infrastructures that not only stand resilient against cyber threats but also adeptly navigate unforeseen events, ensuring the soundness of critical systems.

Table 1

Tier	Description
General	Lays the groundwork by introducing fundamental concepts, models, and terms that permeate the entire series
Policies and Procedures	Dives into an effective security program's human and procedural aspects, with a keen focus on plant operations.
System	Delineates the system security requirements and Security Capability Levels (SC-L) imperative for constructing an IACS harmonized with the Target Security Level (SL-T)
Component	Zeroes in on specific security-related requisites for products and components. It spans the technical intricacies of these products and the processes integral to managing them throughout their lifecycle.

II. Bridging Standards and Solutions: WALLIX PAM4OT

Following the critical need for enhanced cybersecurity measures within IACS outlined in the introduction, the need for practical solutions that can turn these high-level standards into actionable, effective security practices becomes clear.

WALLIX PAM4OT, under the OT.Security brand, delivers comprehensive cybersecurity for Operational Technology (OT) environments, safeguarding critical systems and users, both remote and on-site, from cyber threats. This suite enhances security through:

1. **Remote Access**: It integrates Multi-Factor Authentication (MFA) to verify user identities, applies access controls for third-party equipment, and maintains detailed activity logs for adequate monitoring. It also includes secure password and SSH key management to ensure robust protection.

Building upon this foundation, WALLIX's broader suite, encompassing **Privileged Access Management (PAM), Identity as a Service (IDaaS), and Privileged Elevation and Delegation Management (PEDM)**, offers a unified security strategy aligned with the IEC-62443-3-3 standards on access control, incident management, and system integrity:

- **PAM/PASM**: Manages and monitors privileged access, restricts user rights, and facilitates rapid response to incidents, securing industrial systems effectively.

- **IDaaS**: Boosts access security with MFA, Single Sign-On (SSO), and dynamic access policies, while automating user rights management for compliance.
- **PEDM**: Implements granular access control, dynamic privilege elevation, and comprehensive audit trails, adhering to the least privilege principle and enhancing real-time security monitoring.

Additionally, WALLIX PAM4OT's seamless integration into the OT network, as depicted through the Purdue reference architecture (See Figure 1), illustrates its compatibility with Industrial Demilitarized Zones (DMZs), bridging IT and OT levels.

III. Deep Diving into IEC-62443-3-3 System Requirements

In meeting the stringent standards of IEC 62443-3-3, PASM, IDaaS, and PEDM play pivotal roles in fortifying industrial control systems (ICS). Each solution serves a unique purpose, yet it is their combined integration within a security strategy that establishes a comprehensive and layered defense.

Now we'll dive into the specific System Requirements (SRs) outlined in IEC-62443-3-3 for each Foundational Requirement (FR), assessing the WALLIX portfolio's potential contribution to compliance. As per the standard's scope, these requirements extend across all components essential for constructing and operating an Industrial Automation and Control System (IACS). Moreover, WALLIX can assist asset owners in fulfilling these requirements, particularly addressing security components such as Supervision Systems (e.g., SCADA), SAFETY Systems (e.g., Safety PLCs), and Process-related Systems (e.g., RTUs and PLCs) within the PURDUE Model Layers 3, 2, and 1 (See Figure 1), aligning with the desired security levels.

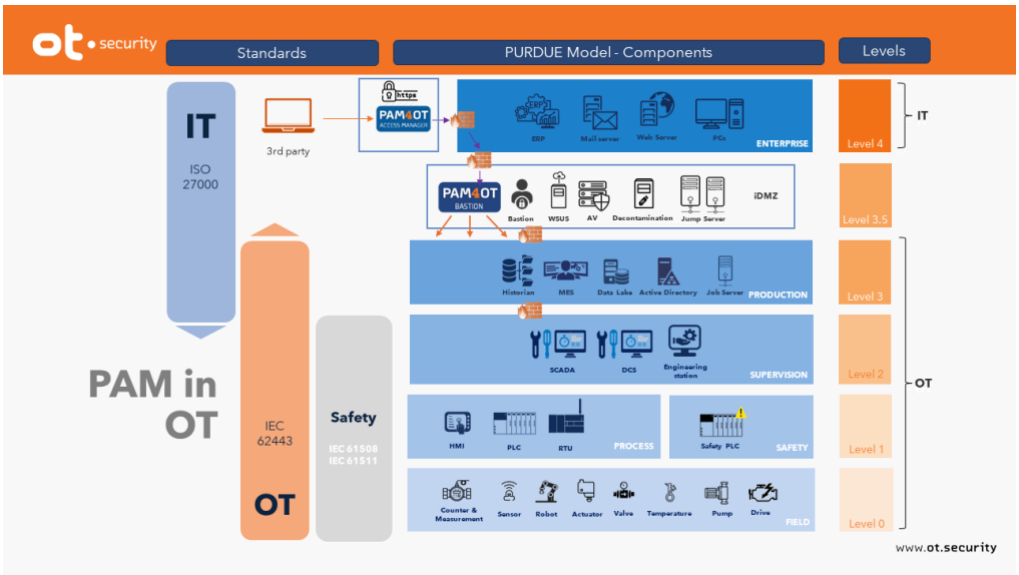

Figure 1

SRs and REs (Number)	Reference	SL1	SL2	SL3	SL4	Match WALLIX yes/no/partial
FR 1						
SR 1.1	5.3	x	x	x	x	yes
SR 1.1 RE 1	5.3.3.1		x	x	x	yes
SR 1.1 RE 2	5.3.3.2			x	x	yes
SR 1.1 RE 3	5.3.3.3				x	yes
SR 1.2	5.4		x	x	x	yes
SR 1.2 RE 1	5.4.3.1			x	x	yes
SR 1.3	5.5	x	x	x	x	yes
SR 1.3 RE 1	5.5.3.1			x	x	yes
SR 1.4	5.6	x	x	x	x	yes
SR 1.5	5.7	x	x	x	x	yes
SR 1.5 RE 1	5.7.3.1			x	x	yes
SR 1.6	5.8	x	x	x	x	yes
SR 1.6 RE 1	5.8.3.1		x	x	x	yes
SR 1.7	5.9	x	x	x	x	yes
SR 1.7 RE 1	5.9.3.1			x	x	partial
SR 1.7 RE 2	5.9.3.2				x	no
SR 1.8	5.10		x	x	x	no
SR 1.9	5.11		x	x	x	no
SR 1.9 RE 1	5.11.3.1			x	x	no
SR 1.10	5.12	x	x	x	x	yes
SR 1.11	5.13	x	x	x	x	yes
SR 1.12	5.14	x	x	x	x	yes
SR 1.13	5.15	x	x	x	x	yes
SR 1.13 RE 1	5.15.3.1		x	x	x	yes
FR 2						
SR 2.1	6.3	x	x	x	x	yes
SR 2.1 RE 1	6.3.3.1		x	x	x	yes

SR 2.1 RE 2	6.3.3.2		x	x	x	yes
SR 2.1 RE 3	6.3.3.3			x	x	yes
SR 2.1 RE 4	6.3.3.4				x	yes
SR 2.2	6.4	x	x	x	x	no
SR 2.2 RE 1	6.4.3.1			x	x	no
SR 2.3	6.5	x	x	x	x	no
SR 2.3 RE 1	6.5.3.1			x	x	no
SR 2.4	6.6	x	x	x	x	no
SR 2.4 RE 1	6.6.3.1			x	x	no
SR 2.5	6.7	x	x	x	x	yes
SR 2.6	6.8		x	x	x	yes
SR 2.7	6.9			x	x	yes
SR 2.8	6.10	x	x	x	x	yes
SR 2.8 RE 1	6.10.3.1			x	x	yes
SR 2.9	6.11	x	x	x	x	yes
SR 2.9 RE 1	6.11.3.1			x	x	no
SR 2.10	6.12	x	x	x	x	partial
SR 2.11	6.13		x	x	x	yes
SR 2.11 RE 1	6.13.3.1			x	x	yes
SR 2.11 RE 2	6.13.3.2				x	no
SR 2.12	6.14			x	x	no
SR 2.12 RE 1	6.14.3.1				x	no
FR 3						
SR 3.1	7.3	x	x	x	x	yes
SR 3.1 RE 1	7.3.3.1			x	x	yes
SR 3.2	7.4	x	x	x	x	yes
SR 3.2 RE 1	7.4.3.1		x	x	x	yes
SR 3.2 RE 2	7.4.3.2			x	x	no
SR 3.3	7.5	x	x	x	x	no
SR 3.3 RE 1	7.5.3.1			x	x	no

SR 3.3 RE 2	7.5.3.2				x	no
SR 3.4	7.6		x	x	x	yes
SR 3.4 RE 1	7.6.3.1			x	x	yes
SR 3.5	7.7	x	x	x	x	yes
SR 3.6	7.8	x	x	x	x	no
SR 3.7	7.9		x	x	x	no
SR 3.8	7.10		x	x	x	yes
SR 3.8 RE 1	7.10.3.1			x	x	yes
SR 3.8 RE 2	7.10.3.2			x	x	yes
SR 3.8 RE 3	7.10.3.3				x	yes
SR 3.9	7.11		x	x	x	yes
SR 3.9 RE 1	7.11.3.1				x	no
FR 4						
SR 4.1	8.3	x	x	x	x	yes
SR 4.1 RE 1	8.3.3.1		x	x	x	yes
SR 4.1 RE 2	8.3.3.2				x	yes
SR 4.2	8.4		x	x	x	yes
SR 4.2 RE 1	8.4.3.1			x	x	yes
SR 4.3	8.5	x	x	x	x	yes
FR 5						
SR 5.1	9.3	x	x	x	x	partial
SR 5.1 RE 1	9.3.3.1		x	x	x	no
SR 5.1 RE 2	9.3.3.2			x	x	yes
SR 5.1 RE 3	9.3.3.3				x	partial
SR 5.2	9.4	x	x	x	x	no
SR 5.2 RE 1	9.4.3.1		x	x	x	no
SR 5.2 RE 2	9.4.3.2			x	x	no
SR 5.2 RE 3	9.4.3.3			x	x	no
SR 5.3	9.5	x	x	x	x	no
SR 5.3 RE 1	9.5.3.1			x	x	no

SR 5.4	9.6	x	x	x	x	no
FR 6						
SR 6.1	10.3	x	x	x	x	yes
SR 6.1 RE 1	10.3.3.1			x	x	yes
SR 6.2	10.4		x	x	x	yes
FR 7						
SR 7.1	11.3	x	x	x	x	yes
SR 7.1 RE 1	11.3.3.1		x	x	x	yes
SR 7.1 RE 2	11.3.3.2			x	x	yes
SR 7.2	11.4	x	x	x	x	yes
SR 7.3	11.5	x	x	x	x	no
SR 7.3 RE 1	11.5.3.1		x	x	x	no
SR 7.3 RE 2	11.5.3.2			x	x	no
SR 7.4	11.6	x	x	x	x	no
SR 7.5	11.7	x	x	x	x	no
SR 7.6	11.8	x	x	x	x	no
SR 7.6 RE 1	11.8.3.1			x	x	no
SR 7.7	11.9	x	x	x	x	no
SR 7.8	11.10		x	x	x	no

IV. Conclusion

WALLIX PAM4OT stands out as a comprehensive solution for securing Industrial Automation and Control Systems (IACS) against cyber threats, demonstrating its effectiveness through its alignment with the IEC-62443 standards. Specifically, WALLIX **covers 62% of all 100 defined controls in the IEC-62443-3-3 standards.** Notably, when focusing on **the core 70 security controls**, excluding areas like backup and restoration, physical network segmentation, PKI management, and wireless management, **WALLIX alignment jumps to nearly 90%**. This highlights the WALLIX portfolio's coverage of nearly all essential security aspects mandated by the standard, thereby ensuring the protection and reliability of critical industrial systems.