15º Congresso de Inovação, Ciência e Tecnologia do IFSP - 2024

Segurança Cibernética no padrão O-PAS™

MAYARA G. ESTEFANI[1], MÁRCIO R. BUZOLI[2], AFONSO C. TURCATO [3]

[1] Graduando em Engenharia Elétrica, Bolsista, IFSP Campus Sertãozinho, mayara.estefani@aluno.ifsp.edu.br.
[2] Graduado em Engenharia Elétrica, Bolsista, IFSP Campus Sertãozinho, m.buzoli@aluno.ifsp.edu.br.
[3] Doutorado em Engenharia Elétrica, Professor Orientador, IFSP Campus Sertãozinho, afonso.turcato@ifsp.edu.br.

Área de conhecimento (Tabela CNPq): 3.04.05.02-5 Automação Eletrônica de Processos Elétricos e Industriais.

RESUMO: O padrão O-PAS™ vem sendo especificado desde 2016, com o objetivo de levar os Sistemas de Automação de Processos Industriais rumo à chamada Indústria 4.0. Enquanto a versão 1.0 do padrão O-PAS possuía como principal objetivo o suporte a interoperabilidade de componentes, a versão 2.1 (atual) tem como principal objetivo a portabilidade de configuração entre os componentes do sistema. As tecnologias da Indústria 4.0 representam uma oportunidade para as empresas aprimorarem seus processos produtivos, melhorando a eficiência, reduzindo desperdícios e custos. Além disso, a segurança cibernética é uma prioridade, integrada desde o início do processo de desenvolvimento do O-PAS e, tornou-se um requisito essencial tomando como base a série de normas IEC 62443: Segurança para automação industrial e sistemas de controle. Neste contexto, este trabalho possui, como objetivo principal, a apresentação dos requisitos fundamentais de segurança cibernética estabelecidos no O-PAS e o levantamento de suas respectivas correspondências na série de normas IEC 62443, mais especificamente da Parte 4 relacionada aos requisitos técnicos de segurança para componentes de um IACS (*Industrial Automation Control System*). Os resultados obtidos mostram que os principais objetivos de segurança do O-PAS estão fortemente correlacionados aos requisitos fundamentais de segurança da norma IEC 62443.

PALAVRAS-CHAVE: Sistemas de Automação de Processos Industriais, O-PAS™, Segurança Cibernética, *Cybersecurity*, IEC 62443.

Cybersecurity on the O-PAS™ standard

ABSTRACT: *The O-PAS™ standard has been specified since 2016, with the aim of taking Industrial Process Automation Systems towards the so-called Industry 4.0. While version 1.0 of the O-PAS standard had as its main objective the support of component interoperability, version 2.1 (current) has as its main objective the portability of configuration between system components. Industry 4.0 technologies represent an opportunity for companies to improve their production processes, improving efficiency, reducing waste and costs. In addition, cybersecurity is a priority, integrated from the beginning of the O-PAS development process and has become an essential requirement based on the IEC 62443 series of standards: Security for industrial automation and control systems. In this context, this work has, as its main objective, the presentation of the fundamental cybersecurity requirements established in O-PAS and the survey of their respective correspondences in the IEC 62443 series of standards, more specifically in Part 4 related to the technical security requirements for components of an IACS (Industrial Automation Control System). The results obtained show that the main security objectives of O-PAS are strongly correlated with the fundamental security requirements of the IEC 62443 standard.*

KEYWORDS: IACS, O-PAS™, Cyber Security, Cybersecurity, IEC 62443.

INTRODUÇÃO

A quarta revolução industrial, ou Indústria 4.0, está transformando a produção e operação das empresas através de novas tecnologias que impulsionam a automação e a eficiência, além de impactar a economia e a sociedade. Essa revolução é composta por tecnologias como sistemas ciberfísicos, Big Data, inteligência artificial, computação em nuvem e Internet das Coisas.

O padrão O-PAS™ para Sistemas de Automação Industrial está em desenvolvimento desde 2016 e tem como objetivo levar os Sistemas de Automação de Processos Industriais rumo à chamada Indústria 4.0, pois define uma arquitetura aberta, segura e interoperável (Qamsane et al., 2022).

O padrão define 11 (onze) objetivos principais: *Identification; Authentication; Non-repudiation; Authorization; Integrity; Anomaly Detection; Confidentiality; Segmentation; Auditability/Accountability; Availability; Incident Response*.

Apesar de promissor, o padrão ainda possui lacunas em sua especificação que inviabilizam sua implementação prática no contexto deste trabalho, como observado nas partes 6.2 (The Open Group, 2023a) e 6.6 (The Open Group, 2023b) da norma O-PAS™.

Neste sentido, o problema técnico-científico contempla o desafio transpor as especificações da norma O-PAS, ainda em desenvolvimento e com lacunas, em uma lista de requisitos técnicos de segurança a serem cumpridos no desenvolvimento dos Componentes e dos Sistemas IACS pela empresa financiadora deste projeto. A resolução desse problema exige a aplicação de conhecimento técnico-científico para traduzir as normas, lidar com um grande volume de informações e garantir compatibilidade com tecnologias legadas e futuras. Além disso, este trabalho é inédito, pois a própria implementação do padrão O-PAS é inédita e nunca foi experimentado.

Desta forma, o objetivo geral do projeto foi realizar um levantamento e verificação dos requisitos de segurança cibernética estabelecidos no O-PAS que estão contidos no padrão atual de referência em segurança cibernética para plantas industriais, descrito na série de normas IEC 62443, mais especificamente na Parte 4 relacionada aos requisitos para componentes.

MATERIAL E MÉTODOS

A metodologia deste trabalho é detalhada com o alinhamento aos objetivos específicos estabelecidos, que visam a elaboração de uma lista dos requisitos técnicos de segurança, agrupados em sete objetivos principais, que estão listados na família de normas IEC 62443, e que possuam correspondência com os onze objetivos macros de segurança cibernética do padrão O-PAS.

Os cinco objetivos específicos estabelecidos foram:

1. Capacitação da equipe em relação ao conceito de Segurança Cibernética na Indústria por meio de cursos e pesquisa bibliográfica sobre o tema. Inicialmente, a pesquisa foi conduzida na base de dados IEEE *Xplore* e, posteriormente, ampliada para as demais bases de dados e sistemas de busca da Internet;
2. Criação de Fluxogramas e mapas mentais sobre os principais aspectos das normas. Esse objetivo consistia em descrever, por meio de mapas-mentais e/ou fluxogramas, as interligações entre os conceitos e determinações de segurança do padrão O-PAS com a série de normas IEC 62443 dos componentes de um IACS;
3. Criação de formulários, tipo ‘checklist’, para a verificação dos principais tópicos tratados nas normas;
4. Confecção de relatório no formato de guia/tutorial contendo os resultados obtidos;
5. Realização de seminário/treinamento para apresentação dos resultados e capacitação da equipe técnica da empresa financiadora do projeto.

Com a realização de levantamento prévio realizado, já foi possível estabelecer um mapeamento macro que relaciona os objetivos principais de segurança do O-PAS com os objetivos fundamentais de segurança descritos na série de normas IEC 62443.

Há uma forte correspondência entre os Objetivos 1 e 2 (totalmente) e o 3 (parcialmente) do O-PAS com o Requisito Fundamental 1 da série IEC-62443. Assim como, o Requisito Fundamental 2 da IEC possui forte correspondência com o Objetivo 3 (parcialmente) e com o Objetivo 4 (totalmente) e assim por diante. Esse mapeamento completo está apresentado na Figura 1.

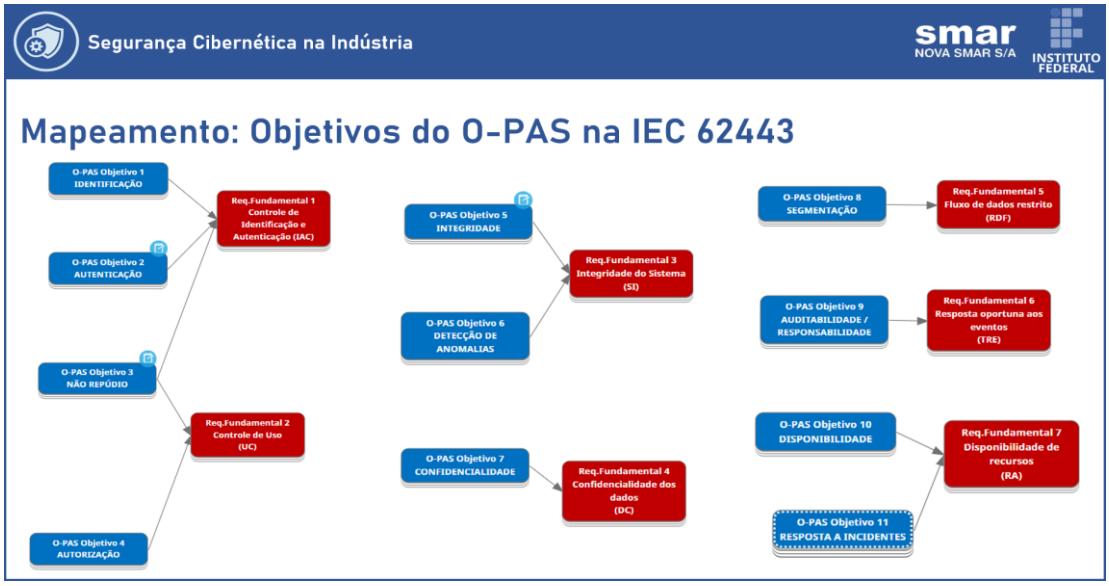

Figura 1. Mapeamento dos onze objetivos principais de segurança do O-PAS (em azul) com os sete requisitos fundamentais de segurança da IEC 62443 (em vermelho).

RESULTADOS E DISCUSSÃO

Os resultados consistem em uma coletânea de certificados, fluxogramas, mapas-mentais, formulários tipo *checklist* que compuseram um relatório final completo.

Tabela 1 – lista do material obtido durante o projeto.

Livro - *Industrial Automation and Control System Security Principles - Ronald L. Krutz*
Livro - *Industrial Cybersecurity: Case Studies and Best Practices - Steve Mustard*
Livro - *Industrial Cybersecurity: Efficiently monitor the cybersecurity - Pascal Ackerman*
Livro - Segurança Cibernética Industrial - Thiago Branquinho e Marcelo Branquinho
Livro - O Quinto Domínio - Richard A. Clarke e Robert K. Knake
Norma - IEC-62443-1-1 (2007) – *Terminology, Concepts and Models*
Norma - IEC-62443-3-1 (2009) – *Security technologies for industrial automation and control systems*
Norma - IEC-62443-3-3 (2013) – *System security requirements and security levels*
Norma - IEC-62443-4-1 (2018) – *Secure product development lifecycle requirements*
Norma - IEC-62443-4-2 (2019) – *Technical security requirements for IACS components*
Curso - Introdução e Conceitos de Segurança Cibernética em ambientes OT (ISA São Paulo)
Curso - *Cybersecurity Practices for Industrial Control Systems (CISA - Cybersecurity Practices for Industrial Control Systems)*
Curso - Visão geral da ISA/IEC 62443 para fornecedores de produtos IC46M – *ISA International*
Relatórios – *Data Breach Investigations Reports (Verizon)*
E-book – Segurança Cibernética Industrial: Monitoramento e Detecção de Anomalias (Cisco)
Whitepaper - Differentiation of the IT security standard series ISO 27000 and IEC 62443 (ABB)
Whitepaper – 7 Steps to ICS and SCADA Security (Exida)
Whitepaper – Introdução ao Framework de Segurança Cibernética do NIST (NIST)
Whitepaper – Industrial Control Systems: Engineering Foundations and Cyber-Physical Attacks Lifecycle
Guia – *Security of Industrial Automation and Control Systems (ISA)*
Guia – *An Overview of ISASecure Certification (ISASecure)*

Alguns cursos foram realizados pela equipe do projeto como parte de capacitação e nivelamento entres os integrantes.

CERTIFICADO

Certificamos que [redacted] inscrito no CPF sob o nº [redacted], participou do treinamento a distância de **"Introdução e Conceitos de Segurança Cibernética em Ambientes OT"**, com carga horária total de 15 horas, realizado no mês de julho de 2023 pela **ISA - Associação Internacional de Automação - Seção São Paulo**.

São Paulo, 31 de julho de 2023.

Alexandre de Oliveira
Instrutor

Carlos Eduardo Gurgel Paiola
Presidente ISA São Paulo Section

International Society of Automation
São Paulo Section

Figura 2. Certificado de uma das capacitações realizadas pela equipe do projeto.

Certificate of Training

Completion

Presented by the

U.S. Department of Homeland Security

Cybersecurity and Infrastructure Security Agency (CISA)

Awarded To

[redacted]

For completion of the online course:

100W Cybersecurity Practices for Industrial Control Systems

On

8/31/2023

CEUs Awarded: .20

Contact Hours: 2 Hours

Figura 3. Certificado de outra capacitação realizada pela equipe do projeto.

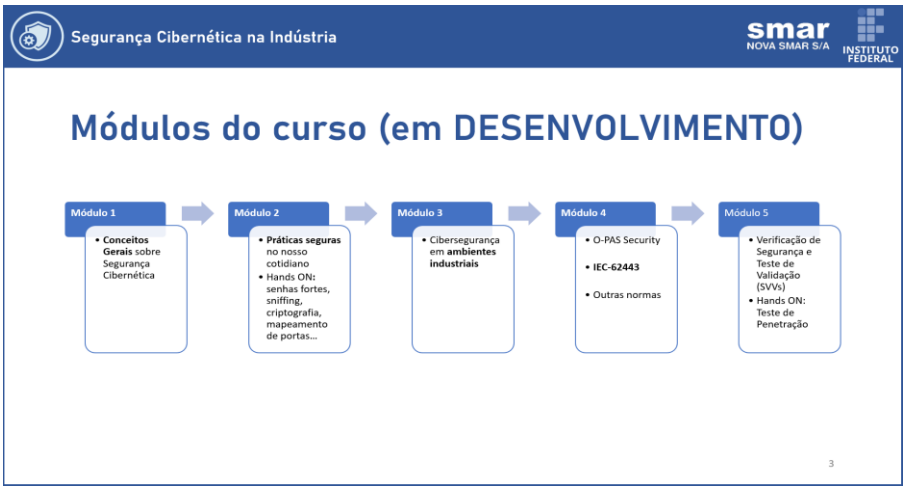

Figura 4. Módulos do treinamento elaborado pela equipe do projeto.

Figura 5. Foto de um dos treinamentos realizados.

Conforme apresentado, todos os objetivos específicos foram plenamente alcançados. É importante destacar a contribuição deste estudo, que visou evidenciar os mecanismos de segurança propostos na especificação O-PAS. Devido ao processo de definição em andamento, a especificação O-PAS, atualmente na versão 2.1, ainda contém várias lacunas a serem preenchidas. A versão 3.0 está prevista para ser publicada até o final de 2024.

CONCLUSÕES

A principal contribuição desse projeto é que todo o levantamento de informações e suas análises foram compilados em um relatório amplo, escrito na forma de guia didático, para que as pessoas envolvidas em projetos de automação, que se baseiam no padrão O-PAS, possam assimilar as informações com uma curva de aprendizagem reduzida. Assim, este projeto de desenvolvimento em conjunto é proposto no sentido de contribuir com a especificação do padrão O-PAS™, uma vez que são solicitadas, pela empresa demandante, o levantamento das principais características no aspecto de segurança cibernética, que por sua vez, é um tema ainda pouco explorado e implementado nos atuais produtos e sistemas da empresa e um dos pilares da Indústria 4.0.

Desta maneira, este projeto contribuiu para que uma empresa brasileira lidere as pesquisas e desenvolvimentos da tecnologia O-PAS, o que traz condições de competir com as empresas líderes no mundo de países europeus e nos EUA nos termos da Lei 10.973/2004 (conhecida como a Lei de Inovação). Adicionalmente, conforme já mencionado, todas as atividades relacionadas com melhorias relacionadas à Segurança Cibernética ajudam a proteger a infraestrutura crítica dos países. Dessa forma, contribuem para o Objetivo 16 de Desenvolvimento Sustentável das Nações Unidas, que promove a busca por sociedades pacíficas e inclusivas.

CONTRIBUIÇÕES DOS AUTORES

AFONSO C. TURCATO contribuiu com a concepção e estudo de viabilidade do projeto. MAYARA G. ESTEFANI confeccionou o material de treinamento e MÁRCIO R. BUZOLI fez os testes e experimentos práticos. Todos os autores contribuíram com a revisão do trabalho e aprovaram a versão submetida.

AGRADECIMENTOS

Os autores agradecem à empresa Nova Smar pela colaboração e apoio no desenvolvimento desse projeto (APPDI - PD&I Nº 07/2023 - IFSP e Nova Smar S.A.).

REFERÊNCIAS

QAMSANE et al. Open process automation- and digital twin-based performance monitoring of a process manufacturing system. IEEE Access, v. 10, p. 60823–60835, 2022.
THE OPEN GROUP. O-PAS™ Standard, Version 2.1: Part 6.2 – Information and Exchange Models: Basic Configuration. Apex Plaza, Forbury Road, Reading, Berkshire, RG1 1AX, Reino Unido, 2023.
THE OPEN GROUP. O-PAS™ Standard, Version 2.1: Part 6.6 – Information and Exchange Models: IEC 61131. Apex Plaza, Forbury Road, Reading, Berkshire, RG1 1AX, Reino Unido, 2023.