ISA RIO DE JANEIRO SECTION TECH MEETING 2025

Rio de Janeiro
Section

O Impacto da Transformação Digital e dos Padrões Abertos de Dados Industriais nos Negócios, Meio Ambiente e Sociedade

11 de dezembro de 2025 - das 8h às 18h

IBMEC – Campus Barra da Tijuca

Av. Armando Lombardi, 940, Rio de Janeiro / RJ

Um *Roadmap* de Processos e Produtos Rumo ao Compliance com a norma ISA/IEC 62443

Palestrante: Rafael Lima – Gerente de Novos Negócios

PORQUE?

Há muito em jogo!

Os sistemas digitais sustentam mais de **90% da produtividade do país**, uma falha massiva nesses sistemas ou uma violação/ciberataque em larga escala representa uma **ameaça de alto risco** para economia nacional.

$10.5 Trilhões

Custo do crime cibernético

$4 Trilhões

Orçamento federal dos EUA

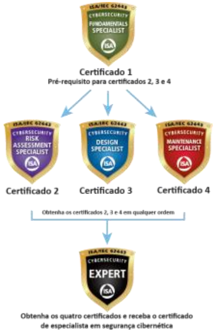
O QUE É

Principal referência global para segurança cibernética industrial, **a norma ISA/IEC 62443** é um conjunto de padrões e relatórios técnicos que fornecem uma estrutura para proteger sistemas de controle e automação (IACS).

OBJETIVO

Em ambientes industriais cada vez mais conectados com alto fluxo de dados a exposição a riscos cibernéticos representam uma ameaça real e a norma ISA/IEC 62443 serve como um guia para a implementação de medidas de segurança robustas que ajudam a mitigar esses riscos e garantir **segurança** e **disponibilidade**.

FLUXO

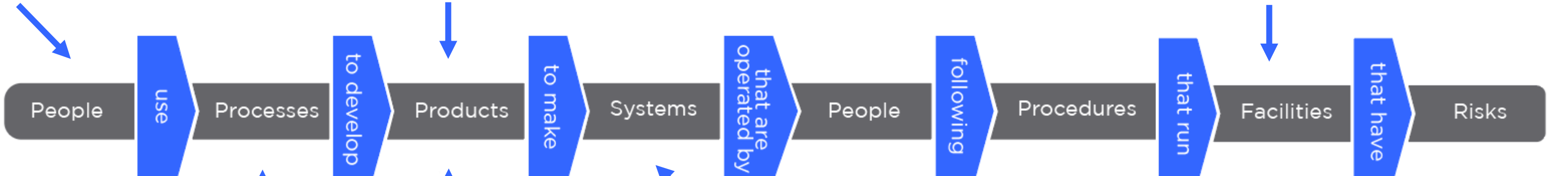


Component Security Assurance (CSA)

IEC 62443-4-2

IACS Security Assurance
OT Site Assessment

IEC 62443-2-1, 2-4, 3-2, 3-3



Security Development Livecycle (SDLA)

IEC 62443-4-1

IIoT Component Security Assurance (ICSA)

IEC 62443-4-2

System Security Assurance (SSA)

IEC 62443-3-3

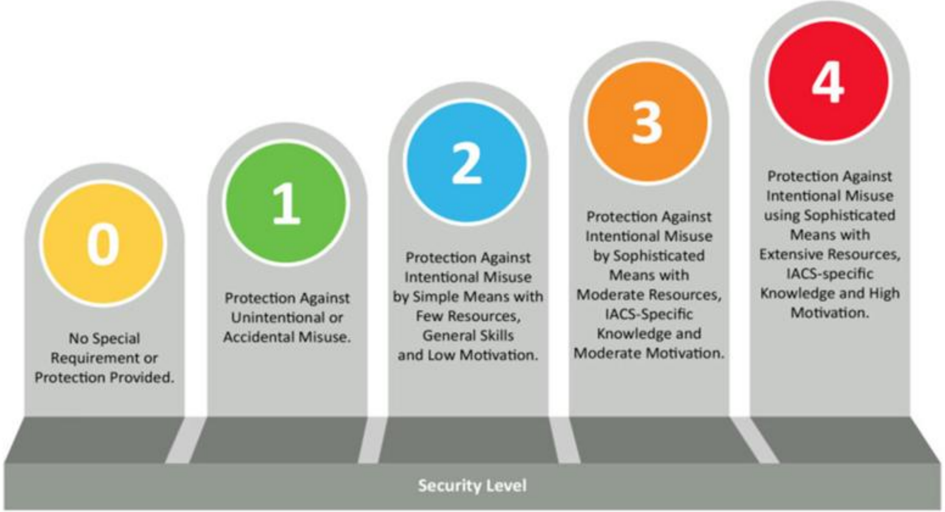
IEC 62443

Na prática

Abordagem de risco por níveis de segurança permitindo que as empresas apliquem controles de segurança de forma mais eficiente focando os maiores esforços nas áreas mais críticas.

- SL-T – *Target Security Level*
- SL-A – *Achieved Security Level*
- SL-C – *Capability Security Level*

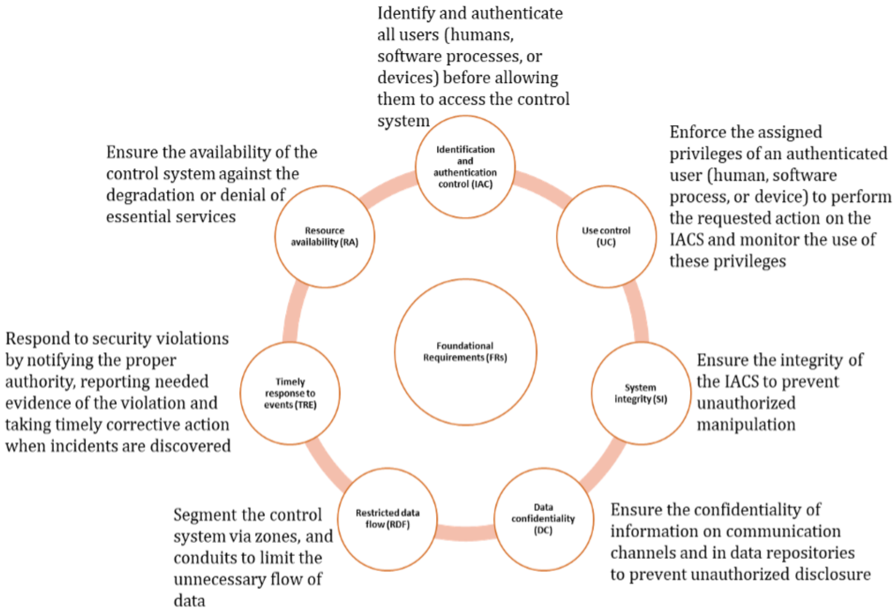
Figure 1. ISA/IEC 62443 Security Levels


0
No Special Requirement or Protection Provided.
1
Protection Against Unintentional or Accidental Misuse.
2
Protection Against Intentional Misuse by Simple Means with Few Resources, General Skills and Low Motivation.
3
Protection Against Intentional Misuse by Sophisticated Means with Moderate Resources, IACS-Specific Knowledge and Moderate Motivation.
4
Protection Against Intentional Misuse using Sophisticated Means with Extensive Resources, IACS-specific Knowledge and High Motivation.
Security Level

IEC 62443

Requisitos Fundamentais

- FR1 – Identificação, autenticação e controle de acesso;
- FR2 – Controle de uso;
- FR3 – Integridade do sistema;
- FR4 – Confidencialidade de dados;
- FR5 – Restrição de fluxo de dados;
- FR6 – Tempo de resposta a eventos;
- FR7 – Disponibilidade de recursos.



Foundational Requirements (FRs)
Identification and authentication control (IAC)
Use control (UC)
System integrity (SI)
Data confidentiality (DC)
Restricted data flow (RDF)
Timely response to events (TRE)
Resource availability (RA)

Identify and authenticate all users (humans, software processes, or devices) before allowing them to access the control system

Enforce the assigned privileges of an authenticated user (human, software process, or device) to perform the requested action on the IACS and monitor the use of these privileges

Ensure the integrity of the IACS to prevent unauthorized manipulation

Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure

Segment the control system via zones, and conduits to limit the unnecessary flow of data

Respond to security violations by notifying the proper authority, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered

Ensure the availability of the control system against the degradation or denial of essential services

Figure 2: IEC 62443 Foundational Requirement Areas & Definitions

ESTRUTURA DA NORMA

- ISA-62443-1-x: fornece uma visão **geral** e conceitual da norma, definindo termos e modelos de segurança;

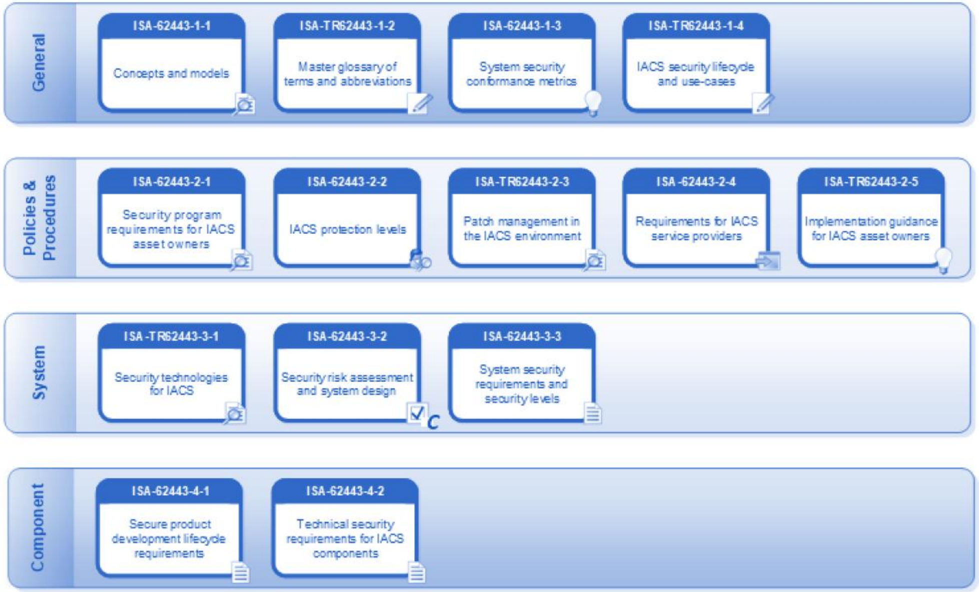
- ISA-62443-2-x: define **políticas e procedimentos** que devem ser seguidos para manter um sistema seguro e eficaz;

- ISA-62443-3-x: **requisitos de sistemas**, especifica os requisitos técnicos de segurança que devem ser incorporados durante a concepção e implementação de um IACS;

- ISA-62443-4-x: **requisitos de componentes**, define os requisitos de segurança para os componentes do sistema, como controladores, softwares e dispositivos de campo.

ESTRUTURA DA NORMA

Dividida em quatro grupos principais, que tratam de diferentes aspectos da segurança cibernética industrial:



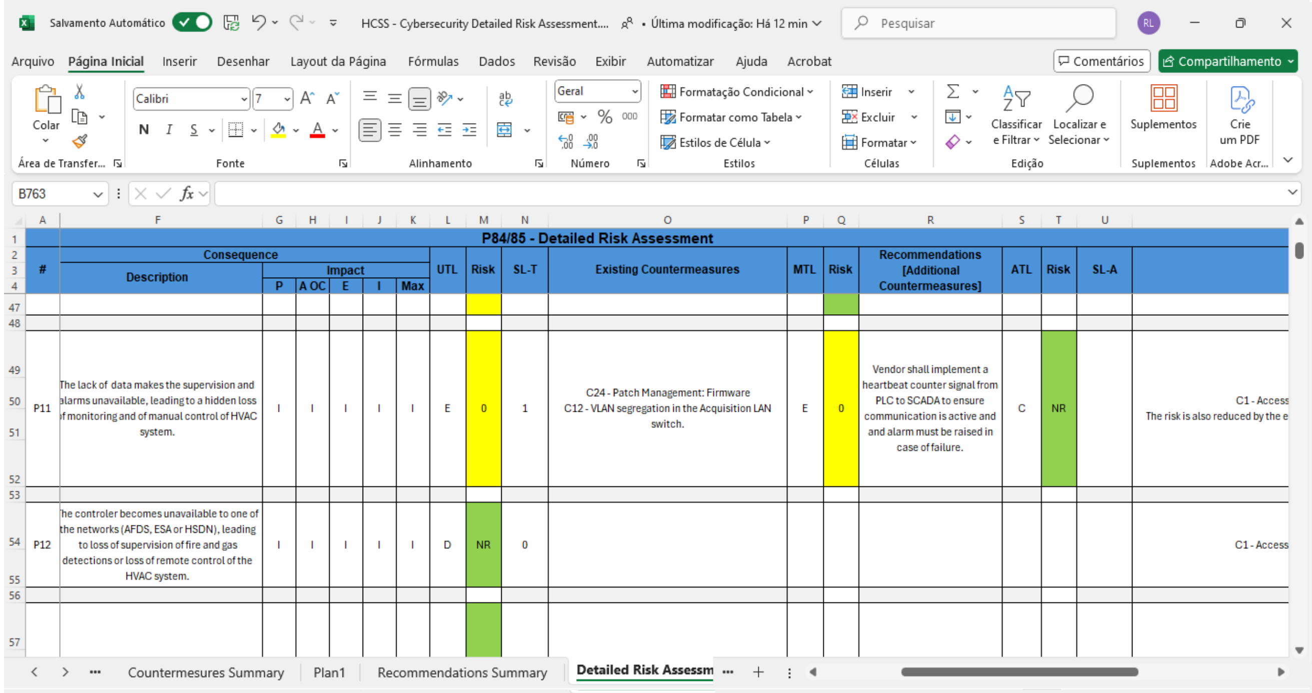
General	ISA-62443-1-1 Concepts and models	ISA-TR62443-1-2 Master glossary of terms and abbreviations	ISA-62443-1-3 System security conformance metrics	ISA-TR62443-1-4 IACS security lifecycle and use-cases	
Policies & Procedures	ISA-62443-2-1 Security program requirements for IACS asset owners	ISA-62443-2-2 IACS protection levels	ISA-TR62443-2-3 Patch management in the IACS environment	ISA-62443-2-4 Requirements for IACS service providers	ISA-TR62443-2-5 Implementation guidance for IACS asset owners
System	ISA-TR62443-3-1 Security technologies for IACS	ISA-62443-3-2 Security risk assessment and system design	ISA-62443-3-3 System security requirements and security levels		
Component	ISA-62443-4-1 Secure product development lifecycle requirements	ISA-62443-4-2 Technical security requirements for IACS components			

CASE

Desenvolvimento de sistemas completos de controle e segurança para FPSOs (Floating Production Storage and Offloading) abrangente a todos os subsistemas essenciais para a operação segura e eficiente das plataformas entregando um sistema robusto, capaz de gerenciar, em tempo real, operações críticas de extração, processamento e armazenamento de petróleo.

METODOLOGIA

ANÁLISE DE RISCOS



P84/85 - Detailed Risk Assessment

#	Consequence						UTL	Risk	SL-T	Existing Countermeasures	MTL	Risk	Recommendations [Additional Countermeasures]	ATL	Risk	SL-A	
	Description	Impact															
		P	A OC	E	I	Max											
P11	The lack of data makes the supervision and alarms unavailable, leading to a hidden loss of monitoring and of manual control of HVAC system.	I	I	I	I	I	E	0	1	C24 - Patch Management: Firmware C12 - VLAN segregation in the Acquisition LAN switch.	E	0	Vendor shall implement a heartbeat counter signal from PLC to SCADA to ensure communication is active and and alarm must be raised in case of failure.	C	NR		C1 - Access The risk is also reduced by the e
P12	The controler becomes unavailable to one of the networks (AFDS, ESA or HSDN), leading to loss of supervision of fire and gas detections or loss of remote control of the HVAC system.	I	I	I	I	I	D	NR	0								C1 - Access

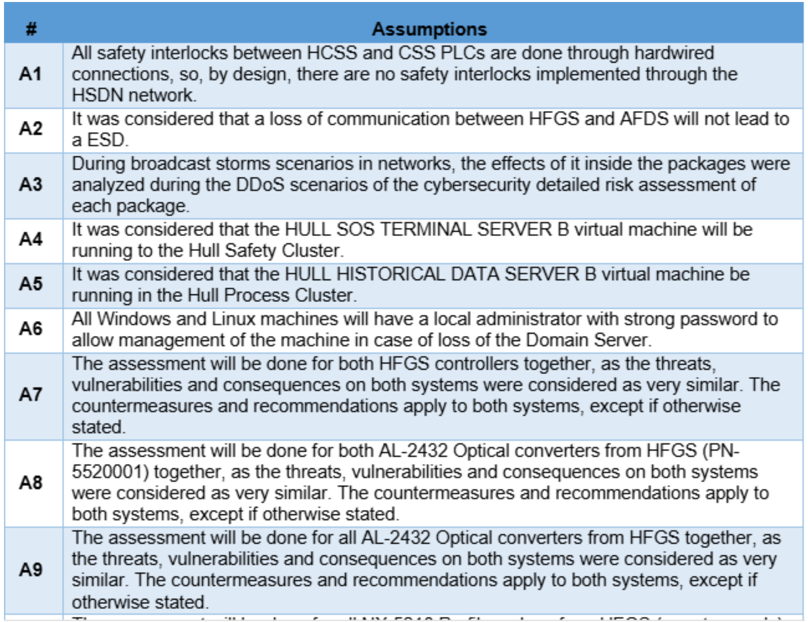
AÇÕES IMPLEMENTADAS

Na Altus

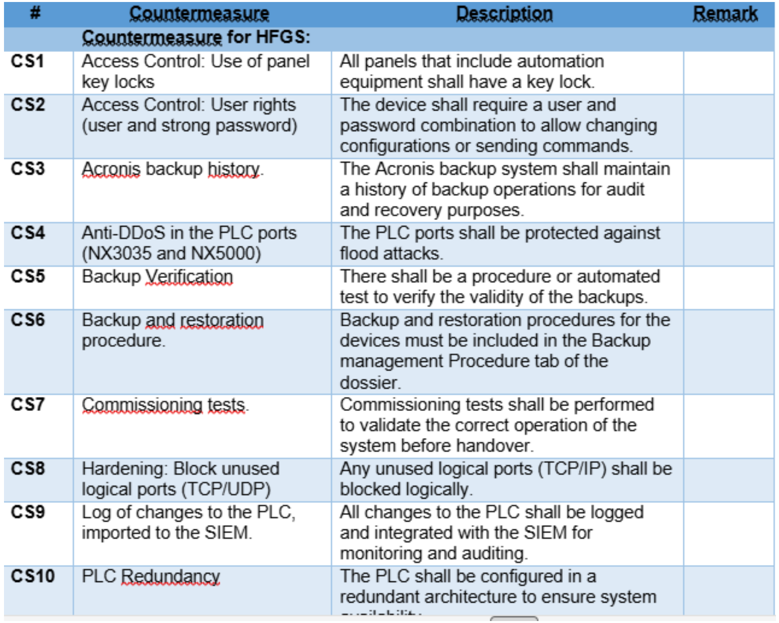
- Análise completa dos requisitos, identificando os que já foram alcançados e as oportunidades de melhoria;
- Plano de ação com planejamento Planejamento estratégico de ações priorizadas;
- Políticas mais avançadas de PKI (Public Key Infrastructure), buscando garantir que os componentes realizem verificações mais robustas de certificados digitais, incluindo o uso de criptografia para validar a autenticidade e integridade dos certificados, aumentando a proteção contra ataques;
- Mapeamento e adoção dos controles mínimos de rotina operacional de segurança cibernética necessários de acordo com o Manual de Procedimentos da Operação 5.13.

METODOLOGIA ALTUS

Exemplo de avaliação de riscos



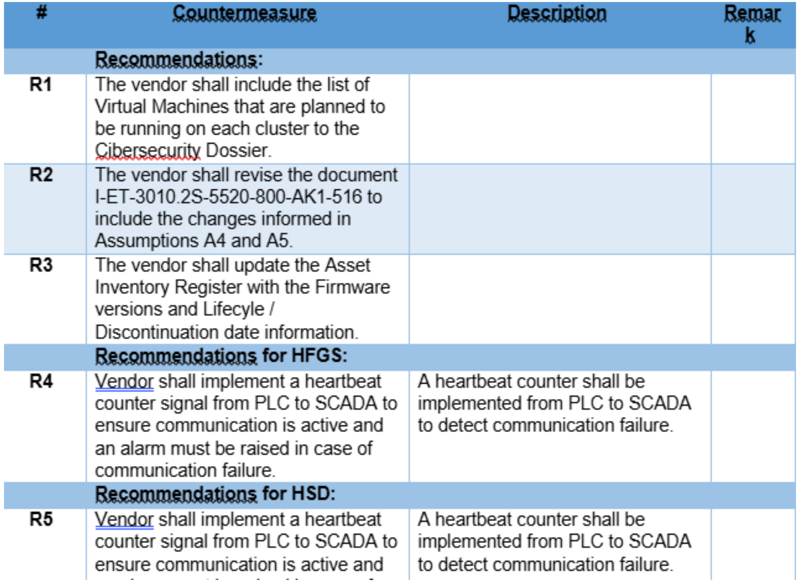
#	Assumptions
A1	All safety interlocks between HCSS and CSS PLCs are done through hardwired connections, so, by design, there are no safety interlocks implemented through the HSDN network.
A2	It was considered that a loss of communication between HFGS and AFDS will not lead to a ESD.
A3	During broadcast storms scenarios in networks, the effects of it inside the packages were analyzed during the DDoS scenarios of the cybersecurity detailed risk assessment of each package.
A4	It was considered that the HULL SOS TERMINAL SERVER B virtual machine will be running to the Hull Safety Cluster.
A5	It was considered that the HULL HISTORICAL DATA SERVER B virtual machine be running in the Hull Process Cluster.
A6	All Windows and Linux machines will have a local administrator with strong password to allow management of the machine in case of loss of the Domain Server.
A7	The assessment will be done for both HFGS controllers together, as the threats, vulnerabilities and consequences on both systems were considered as very similar. The countermeasures and recommendations apply to both systems, except if otherwise stated.
A8	The assessment will be done for both AL-2432 Optical converters from HFGS (PN-5520001) together, as the threats, vulnerabilities and consequences on both systems were considered as very similar. The countermeasures and recommendations apply to both systems, except if otherwise stated.
A9	The assessment will be done for all AL-2432 Optical converters from HFGS together, as the threats, vulnerabilities and consequences on both systems were considered as very similar. The countermeasures and recommendations apply to both systems, except if otherwise stated.



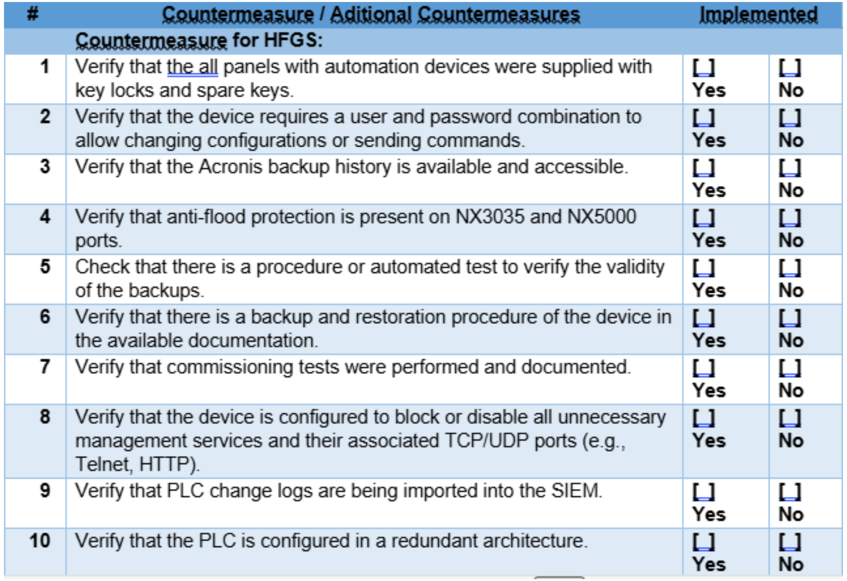
#	Countermeasure	Description	Remark
	Countermeasure for HFGS:		
CS1	Access Control: Use of panel key locks	All panels that include automation equipment shall have a key lock.	
CS2	Access Control: User rights (user and strong password)	The device shall require a user and password combination to allow changing configurations or sending commands.	
CS3	Acronis backup history.	The Acronis backup system shall maintain a history of backup operations for audit and recovery purposes.	
CS4	Anti-DDoS in the PLC ports (NX3035 and NX5000)	The PLC ports shall be protected against flood attacks.	
CS5	Backup Verification	There shall be a procedure or automated test to verify the validity of the backups.	
CS6	Backup and restoration procedure.	Backup and restoration procedures for the devices must be included in the Backup management Procedure tab of the dossier.	
CS7	Commissioning tests.	Commissioning tests shall be performed to validate the correct operation of the system before handover.	
CS8	Hardening: Block unused logical ports (TCP/UDP)	Any unused logical ports (TCP/IP) shall be blocked logically.	
CS9	Log of changes to the PLC, imported to the SIEM.	All changes to the PLC shall be logged and integrated with the SIEM for monitoring and auditing.	
CS10	PLC Redundancy	The PLC shall be configured in a redundant architecture to ensure system availability.	

METODOLOGIA ALTUS

Exemplo de avaliação de riscos



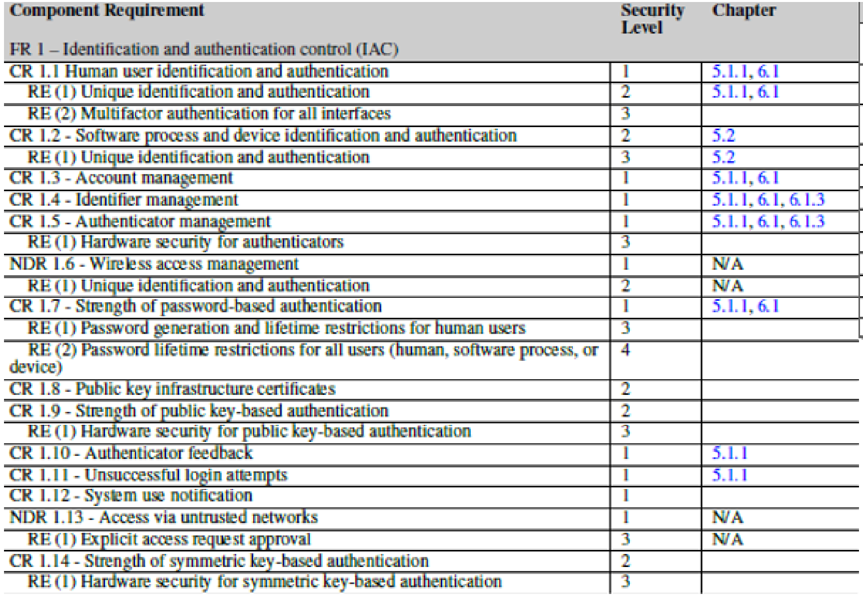
#	Countermeasure	Description	Remark
	Recommendations:		
R1	The vendor shall include the list of Virtual Machines that are planned to be running on each cluster to the Cibersecurity Dossier.		
R2	The vendor shall revise the document I-ET-3010.2S-5520-800-AK1-516 to include the changes informed in Assumptions A4 and A5.		
R3	The vendor shall update the Asset Inventory Register with the Firmware versions and Lifecycle / Discontinuation date information.		
	Recommendations for HFGS:		
R4	Vendor shall implement a heartbeat counter signal from PLC to SCADA to ensure communication is active and an alarm must be raised in case of communication failure.	A heartbeat counter shall be implemented from PLC to SCADA to detect communication failure.	
	Recommendations for HSD:		
R5	Vendor shall implement a heartbeat counter signal from PLC to SCADA to ensure communication is active and	A heartbeat counter shall be implemented from PLC to SCADA to detect communication failure.	



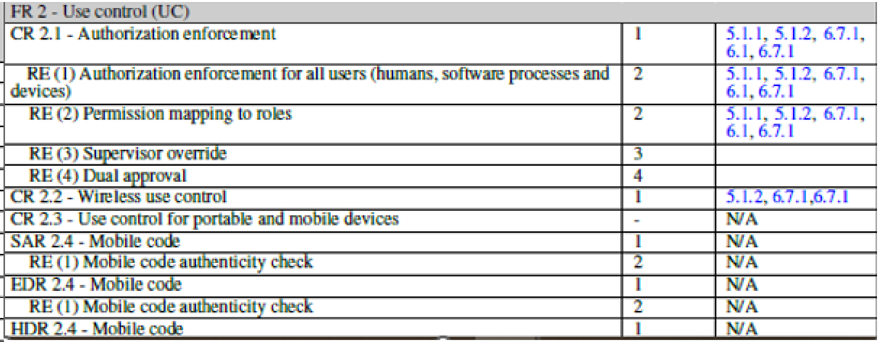
#	Countermeasure / Aditional Countermeasures	Implemented	
	Countermeasure for HFGS:		
1	Verify that the all panels with automation devices were supplied with key locks and spare keys.	[ ] Yes	[ ] No
2	Verify that the device requires a user and password combination to allow changing configurations or sending commands.	[ ] Yes	[ ] No
3	Verify that the Acronis backup history is available and accessible.	[ ] Yes	[ ] No
4	Verify that anti-flood protection is present on NX3035 and NX5000 ports.	[ ] Yes	[ ] No
5	Check that there is a procedure or automated test to verify the validity of the backups.	[ ] Yes	[ ] No
6	Verify that there is a backup and restoration procedure of the device in the available documentation.	[ ] Yes	[ ] No
7	Verify that commissioning tests were performed and documented.	[ ] Yes	[ ] No
8	Verify that the device is configured to block or disable all unnecessary management services and their associated TCP/UDP ports (e.g., Telnet, HTTP).	[ ] Yes	[ ] No
9	Verify that PLC change logs are being imported into the SIEM.	[ ] Yes	[ ] No
10	Verify that the PLC is configured in a redundant architecture.	[ ] Yes	[ ] No

METODOLOGIA ALTUS

Exemplo de requisitos de componentes



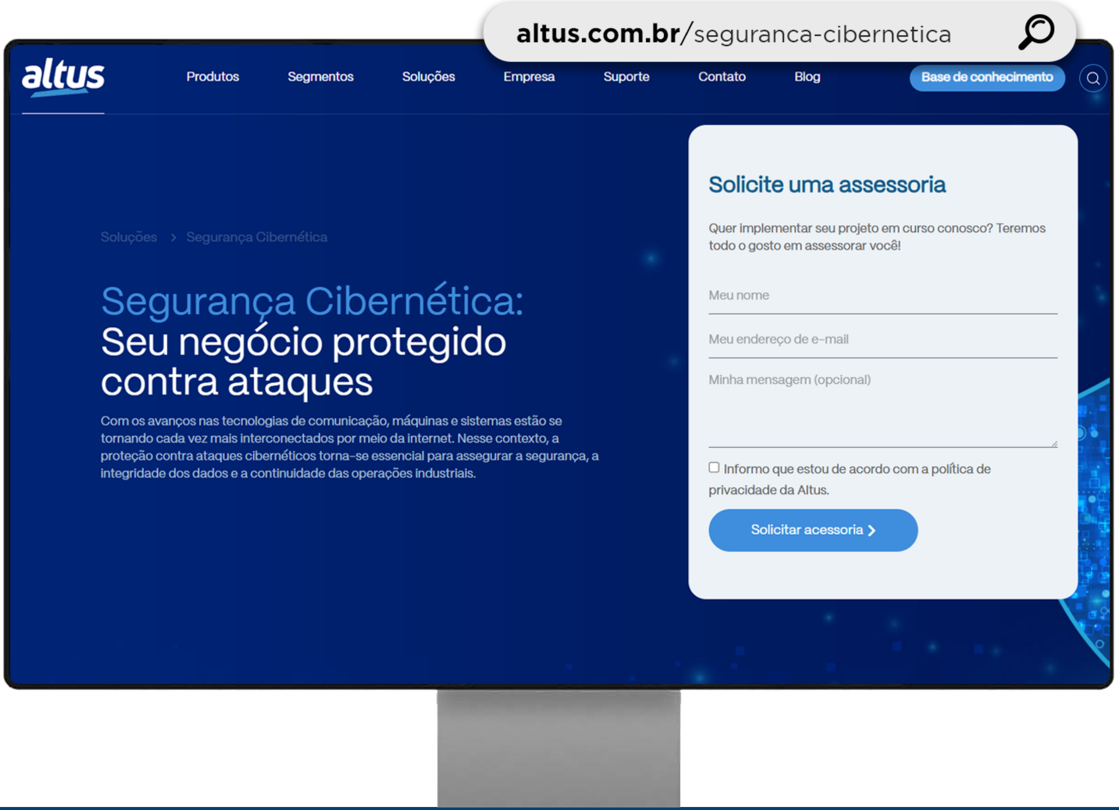
Component Requirement FR 1 – Identification and authentication control (IAC)	Security Level	Chapter
CR 1.1 Human user identification and authentication	1	5.1.1, 6.1
RE (1) Unique identification and authentication	2	5.1.1, 6.1
RE (2) Multifactor authentication for all interfaces	3	
CR 1.2 - Software process and device identification and authentication	2	5.2
RE (1) Unique identification and authentication	3	5.2
CR 1.3 - Account management	1	5.1.1, 6.1
CR 1.4 - Identifier management	1	5.1.1, 6.1, 6.1.3
CR 1.5 - Authenticator management	1	5.1.1, 6.1, 6.1.3
RE (1) Hardware security for authenticators	3	
NDR 1.6 - Wireless access management	1	N/A
RE (1) Unique identification and authentication	2	N/A
CR 1.7 - Strength of password-based authentication	1	5.1.1, 6.1
RE (1) Password generation and lifetime restrictions for human users	3	
RE (2) Password lifetime restrictions for all users (human, software process, or device)	4	
CR 1.8 - Public key infrastructure certificates	2	
CR 1.9 - Strength of public key-based authentication	2	
RE (1) Hardware security for public key-based authentication	3	
CR 1.10 - Authenticator feedback	1	5.1.1
CR 1.11 - Unsuccessful login attempts	1	5.1.1
CR 1.12 - System use notification	1	
NDR 1.13 - Access via untrusted networks	1	N/A
RE (1) Explicit access request approval	3	N/A
CR 1.14 - Strength of symmetric key-based authentication	2	
RE (1) Hardware security for symmetric key-based authentication	3	



FR 2 - Use control (UC)		
CR 2.1 - Authorization enforcement	1	5.1.1, 5.1.2, 6.7.1, 6.1, 6.7.1
RE (1) Authorization enforcement for all users (humans, software processes and devices)	2	5.1.1, 5.1.2, 6.7.1, 6.1, 6.7.1
RE (2) Permission mapping to roles	2	5.1.1, 5.1.2, 6.7.1, 6.1, 6.7.1
RE (3) Supervisor override	3	
RE (4) Dual approval	4	
CR 2.2 - Wireless use control	1	5.1.2, 6.7.1,6.7.1
CR 2.3 - Use control for portable and mobile devices	-	N/A
SAR 2.4 - Mobile code	1	N/A
RE (1) Mobile code authenticity check	2	N/A
EDR 2.4 - Mobile code	1	N/A
RE (1) Mobile code authenticity check	2	N/A
HDR 2.4 - Mobile code	1	N/A

Página de Segurança no site da Altus:

Disponível no menu *Soluções,* uma página dedicada de forma exclusiva a informar e atualizar nossos parceiros sobre segurança cibernética.



altus.com.br/seguranca-cibernetica

Segurança Cibernética:
Seu negócio protegido contra ataques

Com os avanços nas tecnologias de comunicação, máquinas e sistemas estão se tornando cada vez mais interconectados por meio da internet. Nesse contexto, a proteção contra ataques cibernéticos torna-se essencial para assegurar a segurança, a integridade dos dados e a continuidade das operações industriais.

Solicite uma assessoria

Quer implementar seu projeto em curso conosco? Teremos todo o gosto em assessorar você!

Meu nome

Meu endereço de e-mail

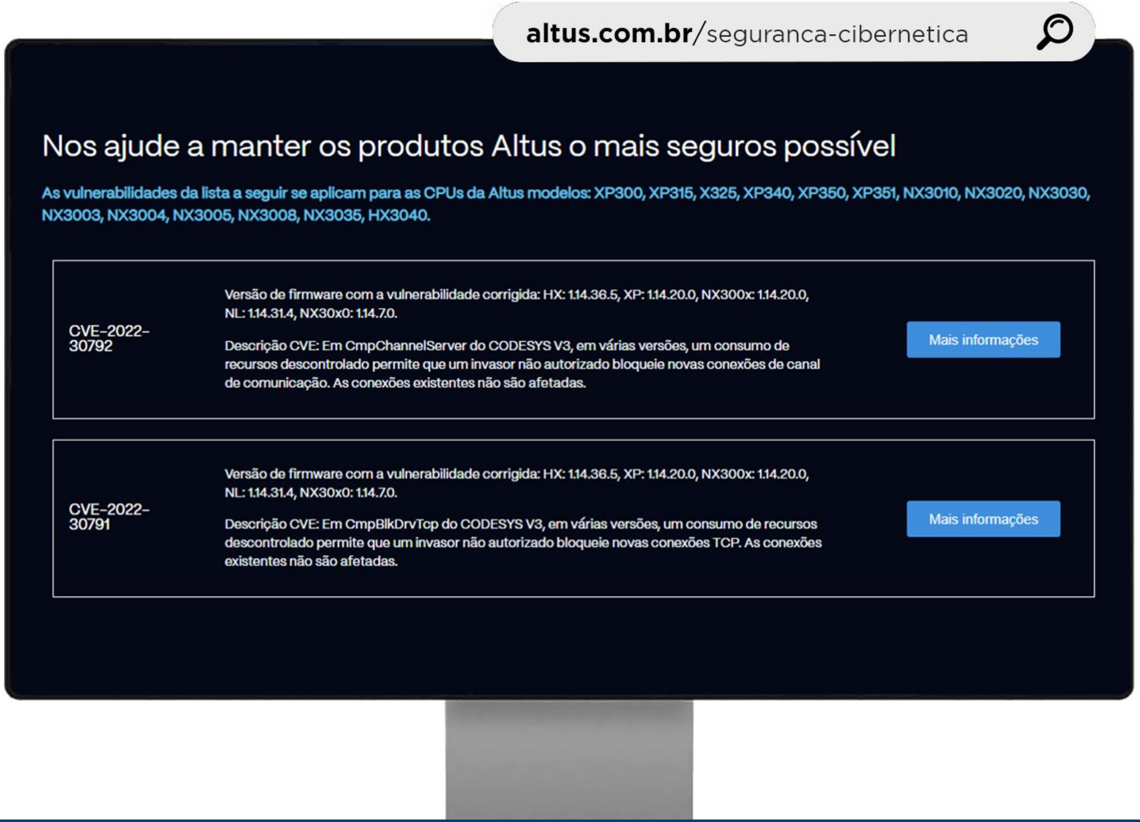
Minha mensagem (opcional)

□ Informo que estou de acordo com a política de privacidade da Altus.

Solicitar acessoria ›

Lista de Vulnerabilidades Conhecidas:

Na página de Segurança Cibernética, disponibilizamos um mapa atualizado das vulnerabilidades conhecidas, orientações para mitigá-las, além de comunicados e atualizações recentes sobre o tema.



Nos ajude a manter os produtos Altus o mais seguros possível

As vulnerabilidades da lista a seguir se aplicam para as CPUs da Altus modelos: XP300, XP315, X325, XP340, XP350, XP351, NX3010, NX3020, NX3030, NX3003, NX3004, NX3005, NX3008, NX3035, HX3040.

CVE-2022-30792

Versão de firmware com a vulnerabilidade corrigida: HX: 1.14.36.5, XP: 1.14.20.0, NX300x: 1.14.20.0, NL: 1.14.31.4, NX30x0: 1.14.7.0.

Descrição CVE: Em CmpChannelServer do CODESYS V3, em várias versões, um consumo de recursos descontrolado permite que um invasor não autorizado bloqueie novas conexões de canal de comunicação. As conexões existentes não são afetadas.

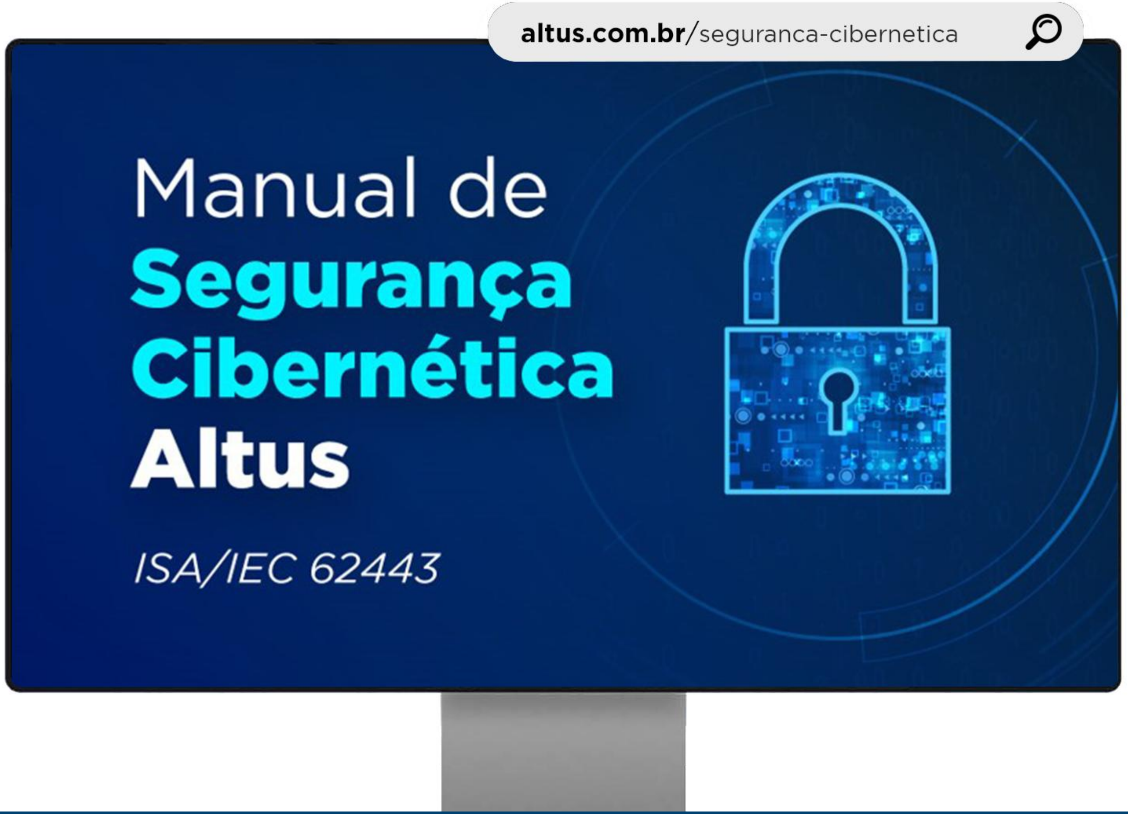
CVE-2022-30791

Versão de firmware com a vulnerabilidade corrigida: HX: 1.14.36.5, XP: 1.14.20.0, NX300x: 1.14.20.0, NL: 1.14.31.4, NX30x0: 1.14.7.0.

Descrição CVE: Em CmpBlkDrvTcp do CODESYS V3, em várias versões, um consumo de recursos descontrolado permite que um invasor não autorizado bloqueie novas conexões TCP. As conexões existentes não são afetadas.

Manual de segurança cibernética:

Disponível para download no site da Altus o manual oferece informações importantes sobre segurança com os produtos Altus.



Qual o **valor** de garantir a **disponibilidade** das suas operações?

Obrigado!

Rafael Lima

Gerente de Novos Negócios

Técnico em Eletrônica, graduado em Física e Pós-Graduado Gestão de Empresas de Base tecnológica. Com mais de 20 anos de experiência e atualmente responsável por projetos de AI, Gerenciamento de Ativos e pelo Roadmap de Cibersegurança dos Produtos e Serviços da Altus.

altus

✉ rafael.lima@altus.com.br

☎ (51) 3589-9500