

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

Segurança Cibernética em Tecnologia Operacional de Infraestruturas Críticas

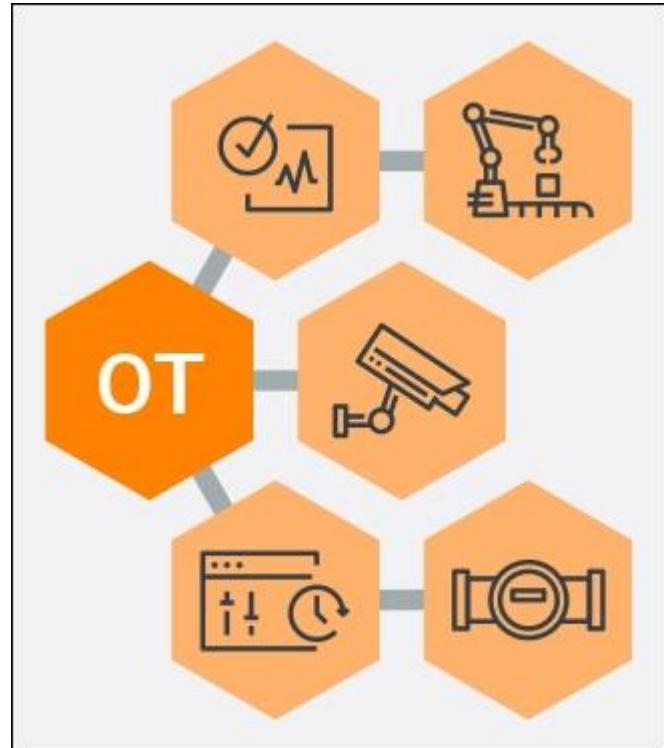
*“Só iremos nos prevenir daquilo que
compreendemos como risco!”*

CONTEXTUALIZAÇÃO

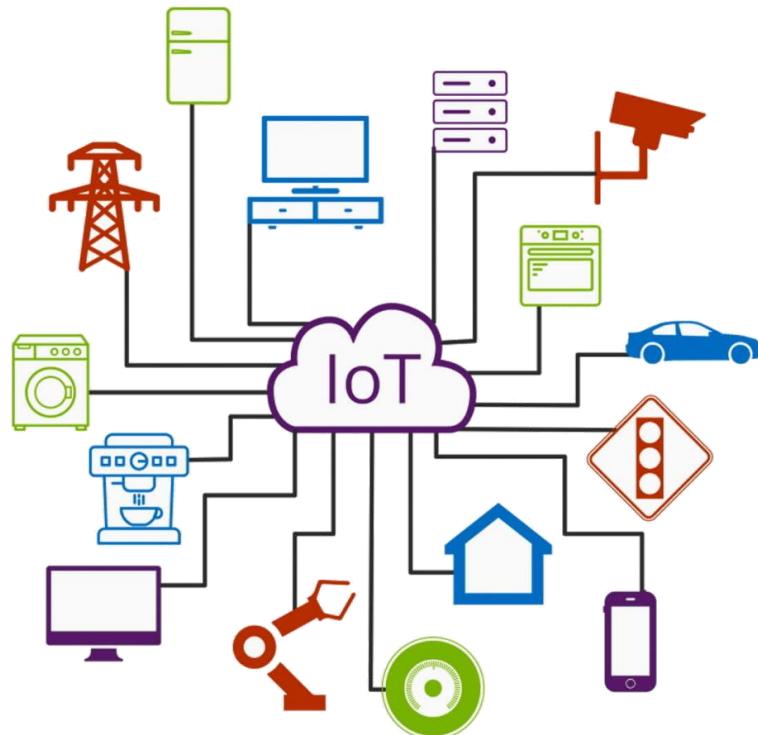
Estrutura de IT e OT



Hardwares
Softwares
Protocolos de Comunicação



Internet das Coisas (IoT)



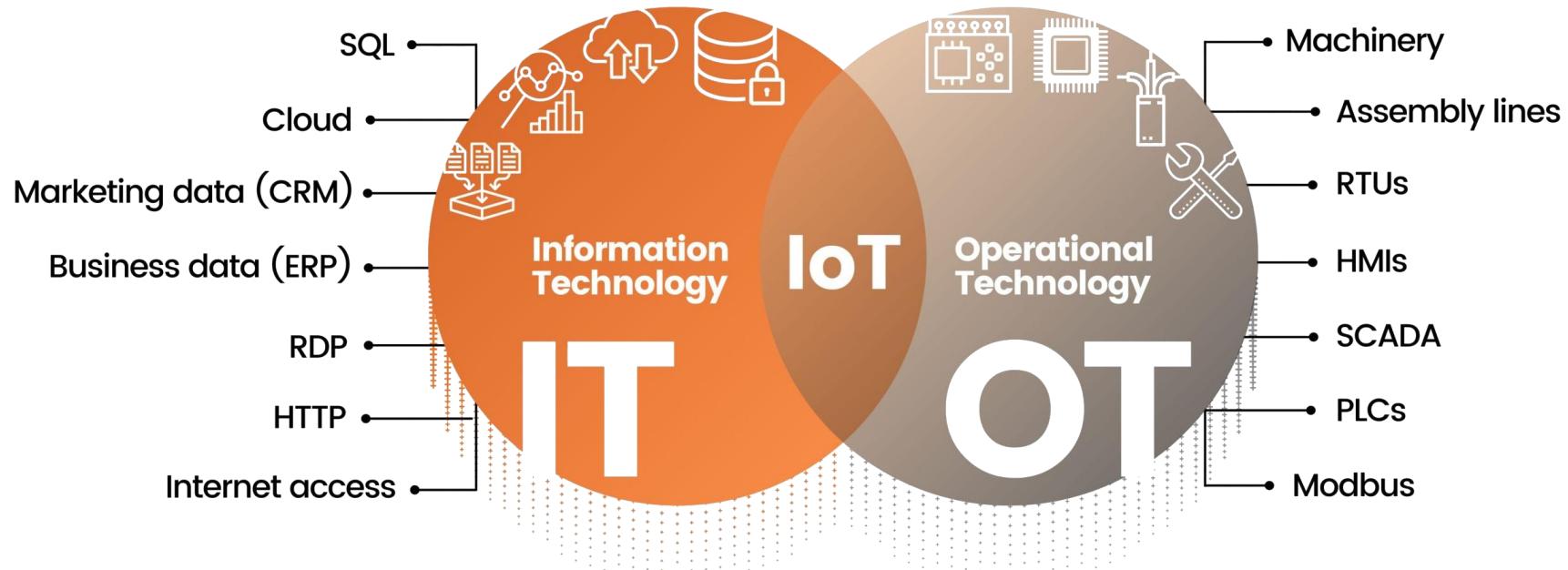
IoT e a 4^a Revolução Industrial



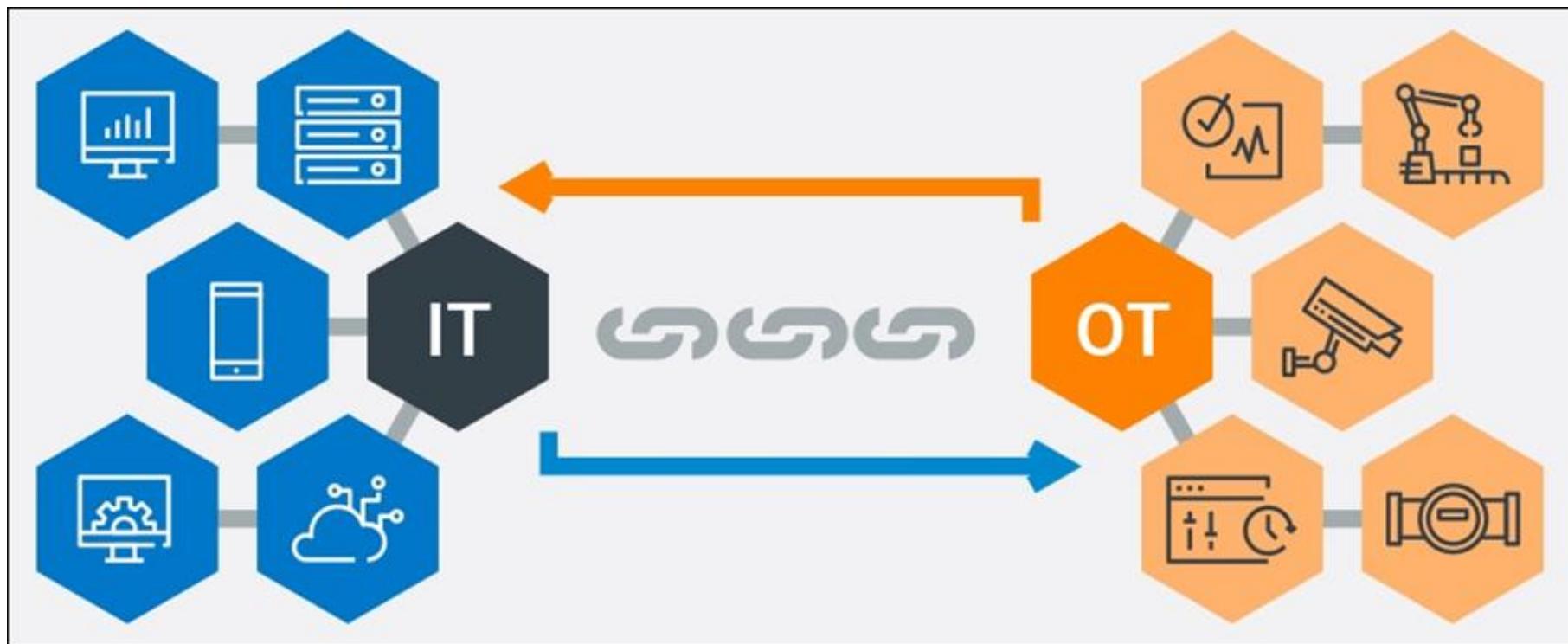
Nova Tecnologia Operacional



Integração OT e IT através de IoT

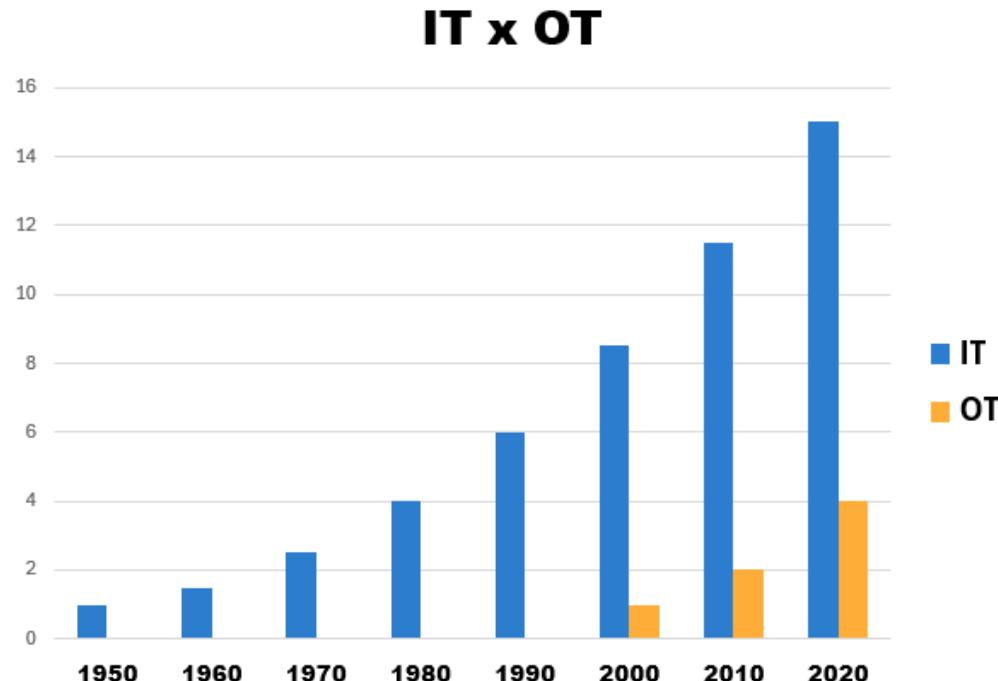


Tecnologias Diferentes e Integradas

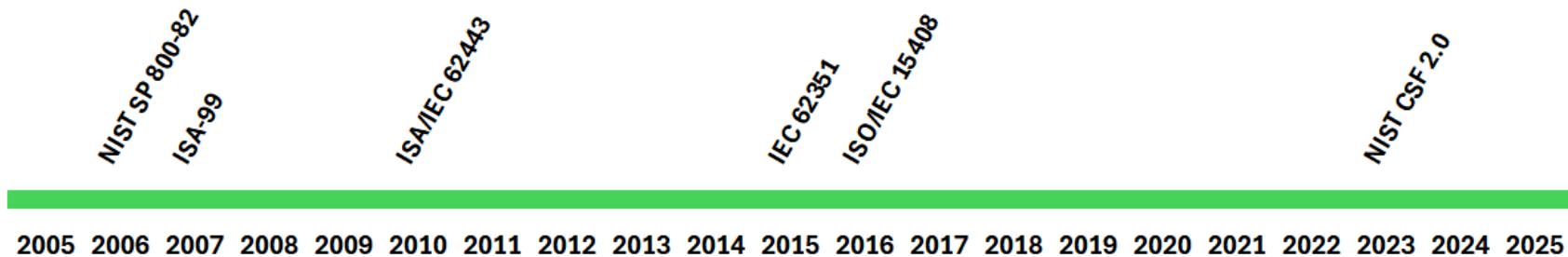


E A SEGURANÇA CIBERNÉTICA ?

Evolução da Segurança Cibernética



Evolução da Segurança Cibernética



International Society of Automation
Setting the Standard for Automation™



International
Electrotechnical
Commission



International
Organization for
Standardization



POR QUE ENVOLVER SEGURANÇA CIBERNÉTICA?

Ciberataques à Infraestrutura Crítica

Junho/2022

Ciberataque paralisa companhia siderúrgica no Irã

Grupo responsável pelo ataque é o mesmo que já havia paralisado algumas infraestruturas críticas como ferrovias, radiodifusão e postos de gasolina iranianos no ano passado



Fevereiro/2024

Gigante siderúrgica ThyssenKrupp sofre ciberataque e paralisa divisão automotiva

Uma das maiores produtoras de aço do mundo sofreu grande impacto devido a ataque ao seu sistema de TI



Ciberataques à Infraestrutura Crítica



As you can see in the video, this cyberattack has been carried out carefully so to protect innocent individuals

Ciberataques à Infraestrutura Crítica

Maio/2024

Rockwell pede desconexão de Internet para redes IoT

Fabricante de equipamentos industriais Rockwell pediu a seus clientes que desconectassem os dispositivos ICS da Internet devido ao aumento da atividade cibernética maliciosa. A empresa citou o aumento no número de atores de ameaças que visam infraestruturas críticas



Ciberataques à Infraestrutura Crítica

Agosto/2025

Ataque cibernético à Jaguar Land Rover gera prejuízo estimado de US\$ 2,5 bilhões no Reino Unido

Paralisação afetou mais de 5 mil empresas e levou o governo britânico a oferecer US\$ 2 bilhões em garantias de crédito à montadora



Ciberataques à Infraestrutura Crítica



CASOS DE ALTO IMPACTO NO SANEAMENTO

Ciberataques ao Saneamento

Novembro/2023

Instalação de água da Pensilvânia atingida por hackers ligados ao Irã

Um grupo hacker anti-Israel com ligações ao Irã forçou uma estação de tratamento de água na Pensilvânia a entrar em operação manual



Fevereiro/2024

Hacker invade e altera tratamento de água na Flórida

Invasão ao sistema ocorreu através do software de acesso remoto que os operadores usavam para manutenção e alterou o nível de hidróxido de sódio de 100 para 11.100 partes por milhão



Ciberataques ao Saneamento



Ciberataques ao Saneamento

Fevereiro/2024

Infraestrutura crítica está em risco real e imediato

A Agência de Segurança Cibernética e de Infraestruturas (CISA), a Agência de Segurança Nacional (NSA) e o Departamento Federal de Investigação (FBI), em conjunto com as principais agências internacionais e governamentais do EUA, como a Agência de Proteção Ambiental (EPA), publicaram um Aviso Conjunto de Segurança Cibernética em 7 de fevereiro sobre atividades maliciosas de um grupo de ataque conhecido como Volt Typhoon que é patrocinado pela China



Ciberataques ao Saneamento



Ciberataques ao Saneamento

Julho/2024

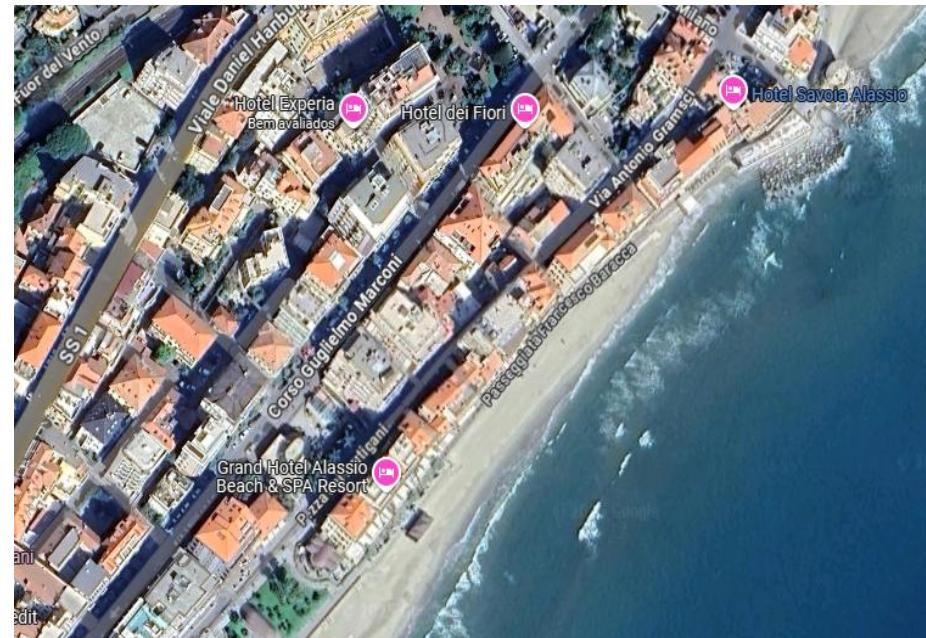
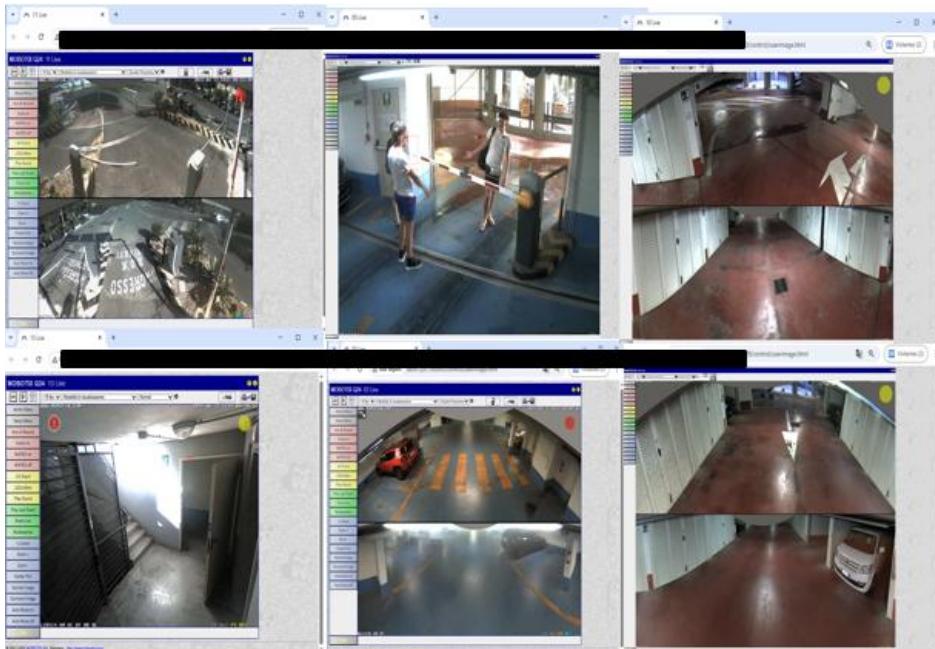
Prioridade Máxima: EUA declaram guerra total aos ciberataques chineses

*A China tem sido acusada de realizar inúmeros ataques cibernéticos contra infraestruturas críticas dos EUA, com um foco particular em endpoints expostos à Internet em instalações de água. Estes ataques não só comprometem a segurança de sistemas, mas também **colocam em risco a saúde pública e a segurança nacional***



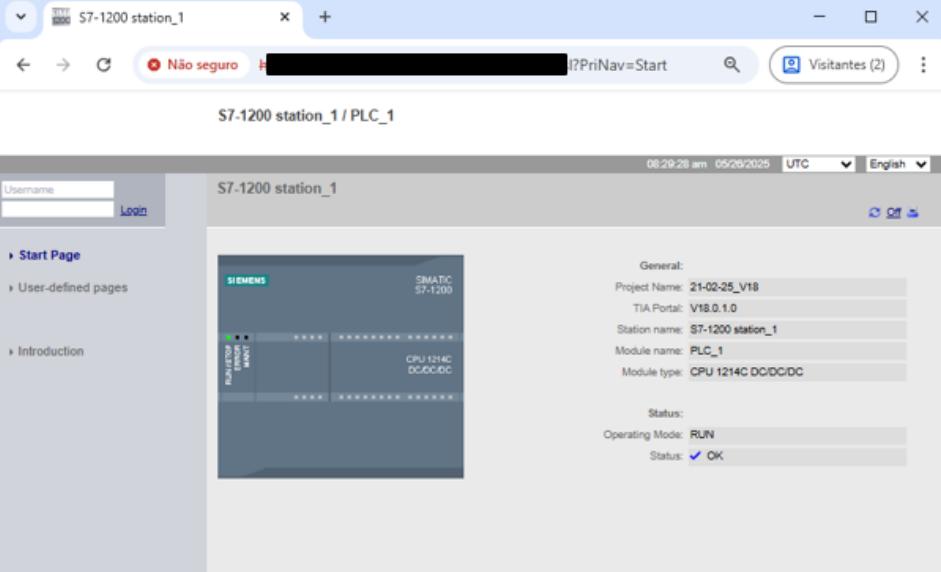
Ativos Expostos na Internet

Sistema de videomonitoramento em hotel na Itália



Ativos Expostos na Internet

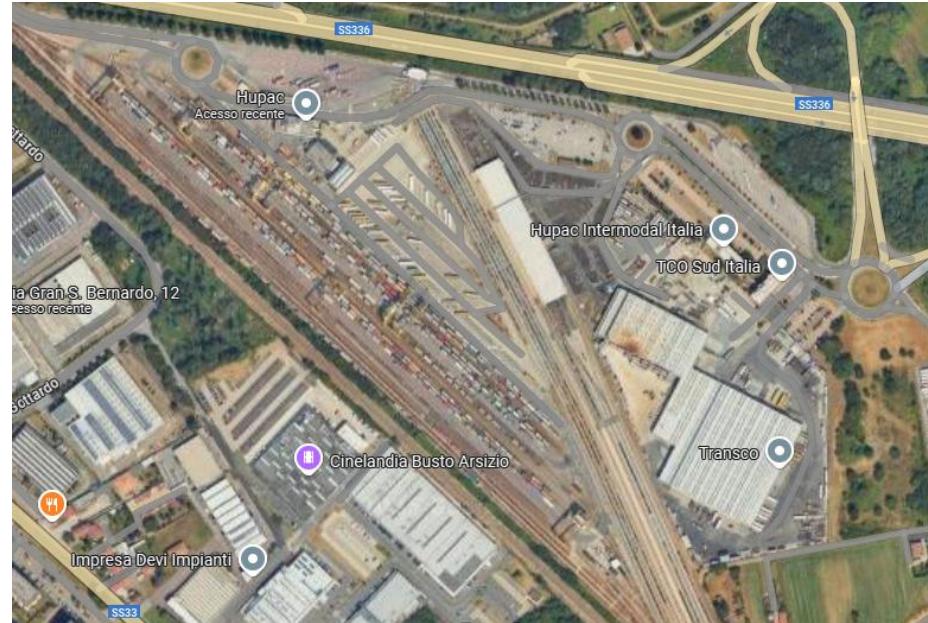
PLC de empresa ferroviária na Itália



The screenshot shows a web-based interface for a Siemens SIMATIC Manager. The title bar reads "S7-1200 station_1". The main content area displays a "Start Page" for "S7-1200 station_1". On the left, there is a navigation sidebar with links for "Start Page", "User-defined pages", and "Introduction". The main content area includes a "General" section with the following details:

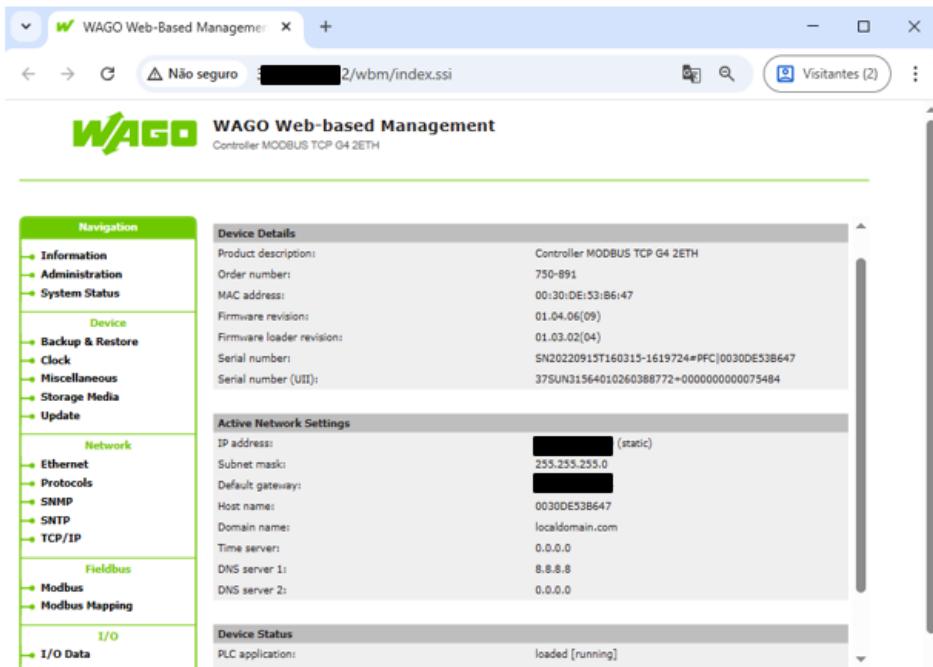
Project Name:	21-02-25_V18
TIA Portal:	V18.0.1.0
Station name:	S7-1200 station_1
Module name:	PLC_1
Module type:	CPU 1214C DC/DC/DC

Below this is a "Status" section showing "Operating Mode: RUN" and "Status: ✓ OK". To the left of the status section is a small thumbnail image of the PLC hardware, labeled "SIEMENS" and "SIMATIC S7-1200".



Ativos Expostos na Internet

Controlador Modbus em empresa de saneamento na Suíça

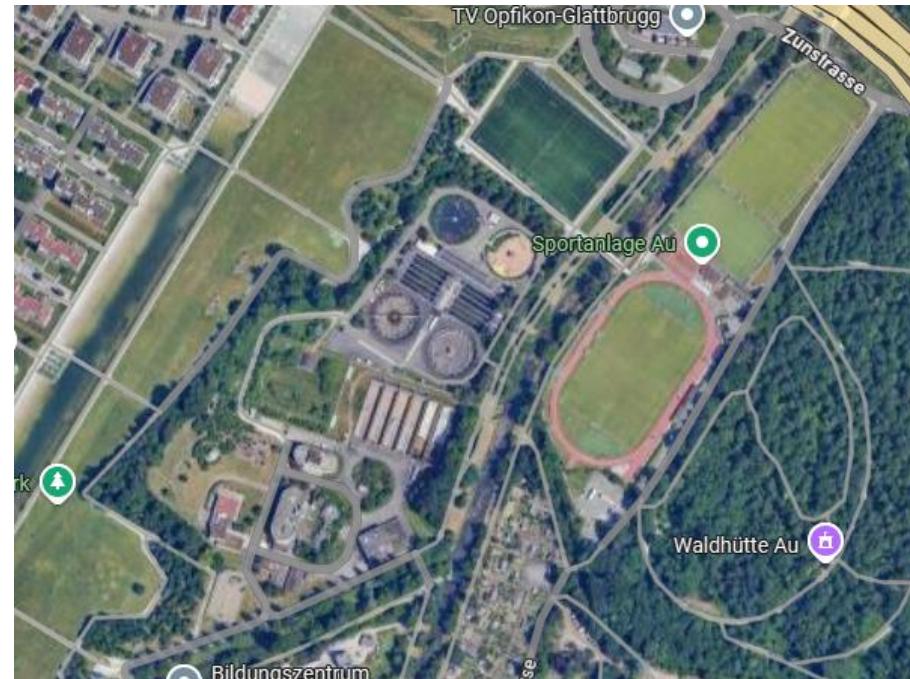


The screenshot shows the WAGO Web-based Management interface for a Controller MODBUS TCP G4 2ETH. The navigation menu on the left includes sections for Information, Administration, System Status, Backup & Restore, Clock, Miscellaneous, Storage Media, Update, Network (Ethernet, Protocols, SNMP, SNTP, TCP/IP), Fieldbus (Modbus, Modbus Mapping), and I/O. The main content area displays the following information:

Device Details	
Product description:	Controller MODBUS TCP G4 2ETH
Order number:	750-891
MAC address:	00:30:DE:53:B6:47
Firmware revision:	01.04.06(09)
Firmware loader revision:	01.03.02(04)
Serial number:	SN20220915T160315-1619724#RFC 0030DE53B647
Serial number (UII):	37SUN31564010260388772+0000000000075484

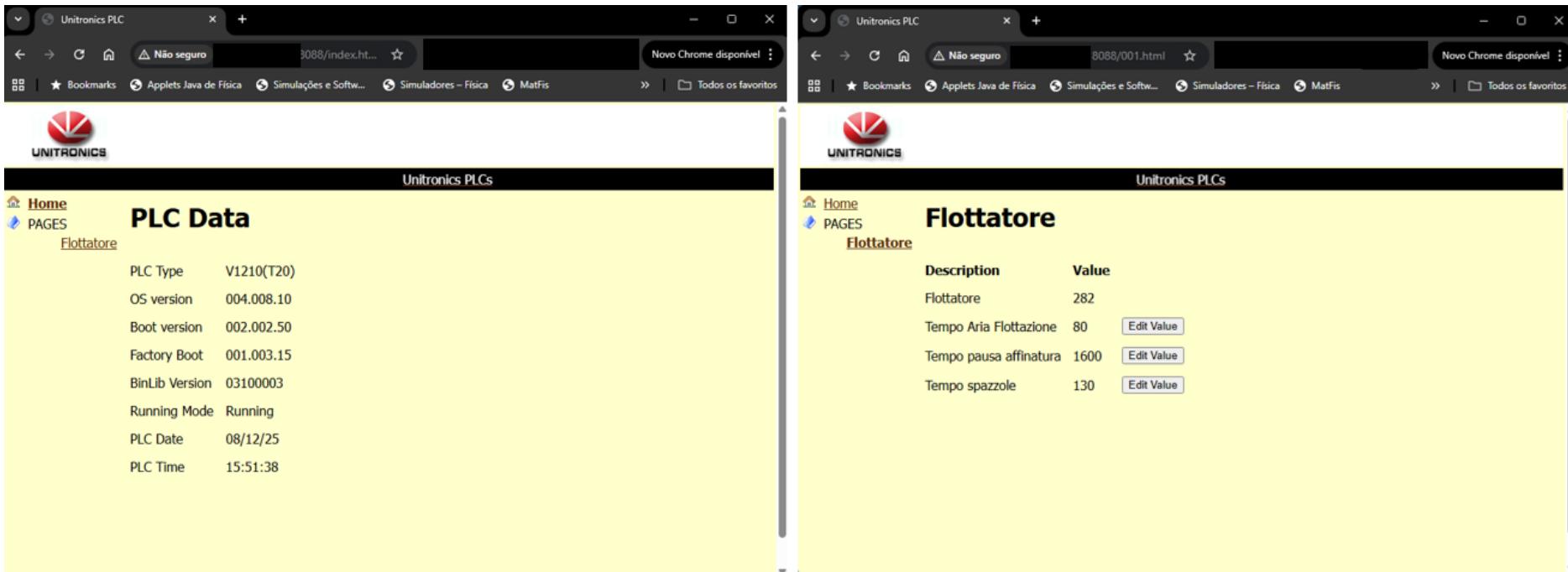
Active Network Settings	
IP address:	[REDACTED] (static)
Subnet mask:	255.255.255.0
Default gateway:	[REDACTED]
Host name:	0030DE53B647
Domain name:	localdomain.com
Time server:	0.0.0.0
DNS server 1:	8.8.8.8
DNS server 2:	0.0.0.0

Device Status	
PLC application:	loaded [running]



Ativos Expostos na Internet

PLC + HMI em empresa de saneamento na Itália



PLC Data

Parameter	Value
PLC Type	V1210(T20)
OS version	004.008.10
Boot version	002.002.50
Factory Boot	001.003.15
BinLib Version	03100003
Running Mode	Running
PLC Date	08/12/25
PLC Time	15:51:38

Flottatore

Description	Value	Action
Flottatore	282	
Tempo Aria Flottazione	80	Edit Value
Tempo pausa affinatura	1600	Edit Value
Tempo spazzole	130	Edit Value

Ativos Expostos na Internet

PLC + HMI em empresa de saneamento na Itália

Left Screenshot: Flottatore Configuration

Description	Value
Flottatore	416
Tempo Aria Flottazione	80
Tempo pausa affinatura	160
Tempo spazzole	130

Valid range: -32768 to 32767

Value:

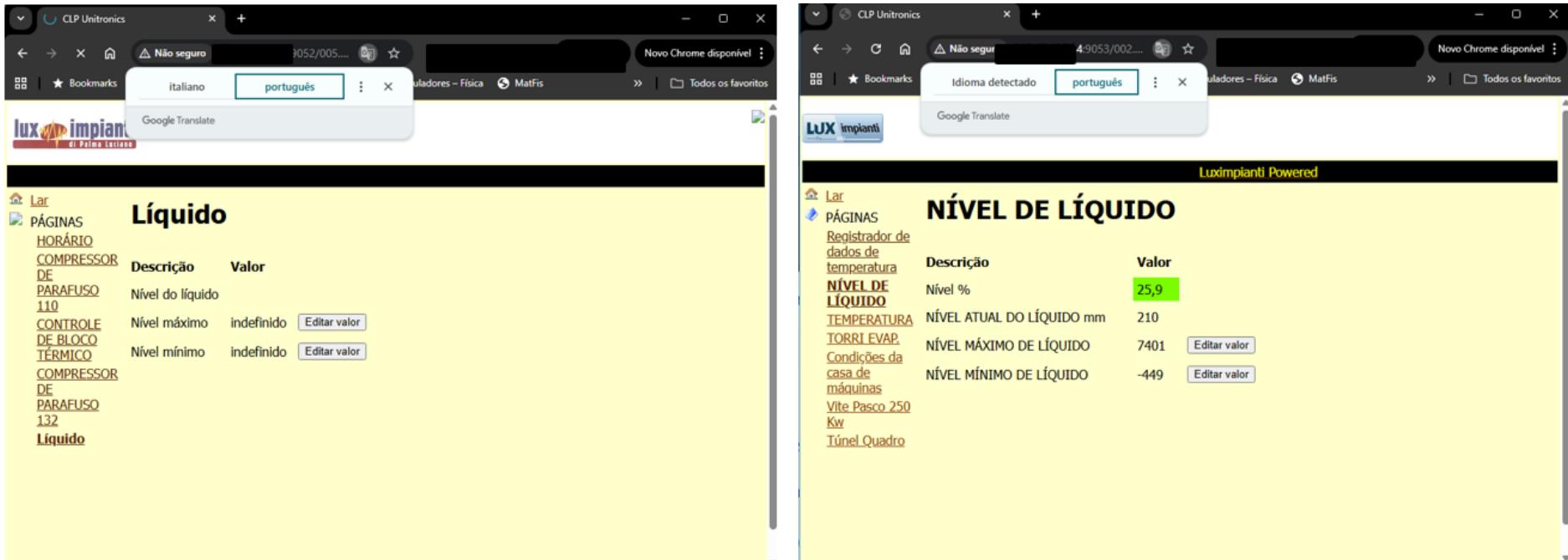
Buttons: OK, Cancel

Right Screenshot: HORÁRIO (Schedule) Configuration

Descrição	Valor
HORA / MINUTOS	1500
DIA / MÊS	812
ANO	2025
HORÁRIO	
COMPRESSOR DE PARAFUSO 110	DIA DA SEMANA
CONTROLE DE BLOCO TÉRMICO	BANDA 1
COMPRESSOR DE PARAFUSO 132	BANDA 2
Líquido	BANDA 3
Soquete	0
falha de rede	931
inversor de desgaste	625
alarmes de inversor	378
Alarme	Regular
Redefinição automática	ativado
Estado do compressor 1	regular
Status do compressor 2	regular
Compressor de 3 estados	regular
Reiniciar	ok

Ativos Expostos na Internet

PLC + HMI em empresa de saneamento na Itália



Líquido

Descrição	Valor
Nível do líquido	Indefinido
Nível máximo	Indefinido
Nível mínimo	Indefinido

NÍVEL DE LÍQUIDO

Descrição	Valor
Nível %	25,9
NÍVEL ATUAL DO LÍQUIDO mm	210
NÍVEL MÁXIMO DE LÍQUIDO	7401
NÍVEL MÍNIMO DE LÍQUIDO	-449

Ativos Expostos na Internet

PLC + HMI em empresa de saneamento na Itália

TEMPERATURA

Descrição	Valor
TEMPERATURA DO TÚNEL 1	-19,3
CONFIGURAR TÚNEL 1	700,0
FRIO	À TEMPERATURA
DESCONGELAMENTO	
TEMPERATURA DO TÚNEL 2	-20,5
CONJUNTO DE TÚNEL 2	-300,1
FRIO	À TEMPERATURA
DESCONGELAMENTO	
TEMPERATURA DA CÉLULA 1	-26,5
CONJUNTO CELLA 1	-2222,1
FRIO	À TEMPERATURA
DESCONGELAMENTO	
TEMPERATURA DA CÉLULA 2	-24,7
CONJUNTO CELLA 2	-22,0
FRIO	À TEMPERATURA
DESCONGELAMENTO	
Solenóide do bloco 1	0
Solenóide do bloco 2	1
Baixo Prx	0,25

TORRI EVAP.

Descrição	Valor	
NÍVEL DE LÍQUIDO	Sistema de alta pressão	10,72
TEMPERATURA	Torre Evap. 1	Acesso
TORRI EVAP.	Velocidade da ventoinha (RPM)	414
Condições da casa de máquinas	Torre Evap 2	Acesso
Vite Pasco 250 Kw	Velocidade do ventilador (RPM)	414
Túnel Quadro	Função anticongelante	Desligado

Ativos Expostos na Internet

PLC + HMI em empresa de saneamento na Itália

TEMPERATURA

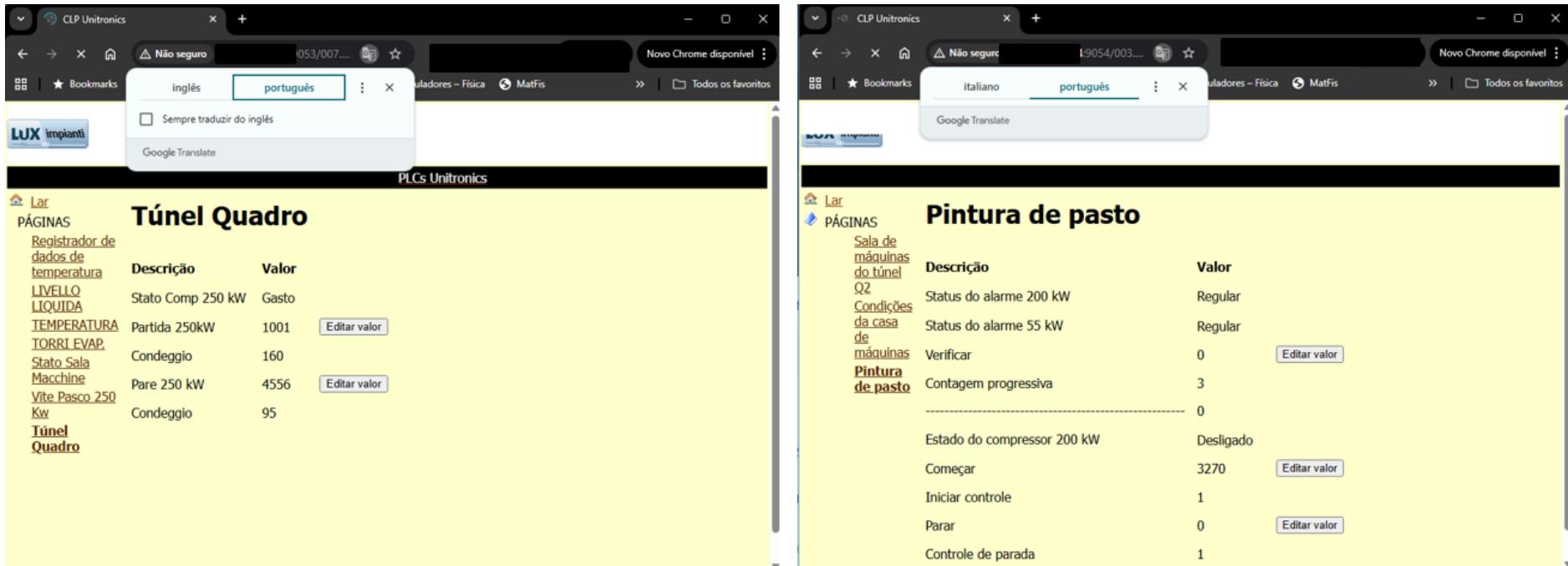
Descrição	Valor
TEMPERATURA DO TÚNEL 1	-19,3
CONFIGURAR TÚNEL 1	700,0
FRIO	À TEMPERATURA
DESCONGELAMENTO	
TEMPERATURA DO TÚNEL 2	-20,5
CONJUNTO DE TÚNEL 2	-300,1
FRIO	À TEMPERATURA
DESCONGELAMENTO	
TEMPERATURA DA CÉLULA 1	-26,5
CONJUNTO CELLA 1	-2222,1
FRIO	À TEMPERATURA
DESCONGELAMENTO	
TEMPERATURA DA CÉLULA 2	-24,7
CONJUNTO CELLA 2	-22,0
FRIO	À TEMPERATURA
DESCONGELAMENTO	
Solenóide do bloco 1	0
Solenóide do bloco 2	1
Baixo Pnx	0,25

TORRI EVAP.

Descrição	Valor
NÍVEL DE LÍQUIDO	Sistema de alta pressão
TEMPERATURA	10,72
TORRI EVAP.	Acesso
Condições da casa de máquinas	
Vite Pasco 250 Kw	414
Túnel Quadro	
FRIO	Torre Evap. 2
DESCONGELAMENTO	
TEMPERATURA DA CÉLULA 2	414
CONJUNTO CELLA 2	
FRIO	Função anticongelante
DESCONGELAMENTO	Desligado

Ativos Expostos na Internet

PLC + HMI em empresa de saneamento na Itália



Túnel Quadro

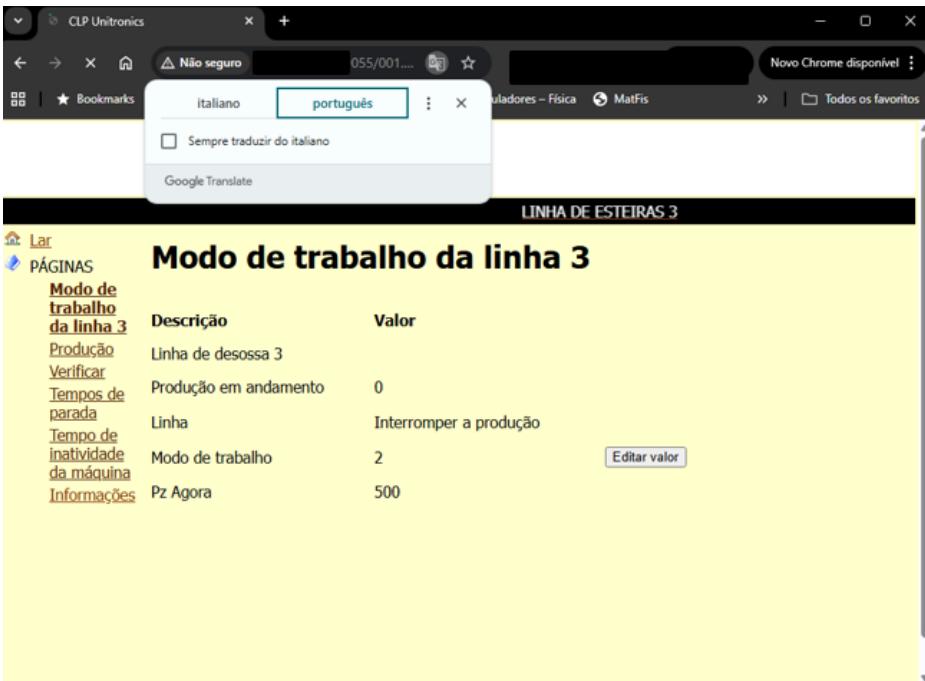
	Descrição	Valor
LIVELLO LIQUIDA	Stato Comp 250 kW	Gasto
TEMPERATURA TORRI EVAP.	Partida 250kW	1001
Stato Sala Macchine	Condeggio	160
Vite Pasco 250 Kw	Pare 250 kW	4556
Túnel Quadro	Condeggio	95

Pintura de pasto

	Descrição	Valor
Sala de máquinas do túnel	Status do alarme 200 kW	Regular
Q2	Status do alarme 55 kW	Regular
Condições da casa de máquinas	Verificar	0
Pintura de pasto	Contagem progressiva	3
		0
	Estado do compressor 200 kW	Desligado
	Começar	3270
	Iniciar controle	1
	Parar	0
	Controle de parada	1

Ativos Expostos na Internet

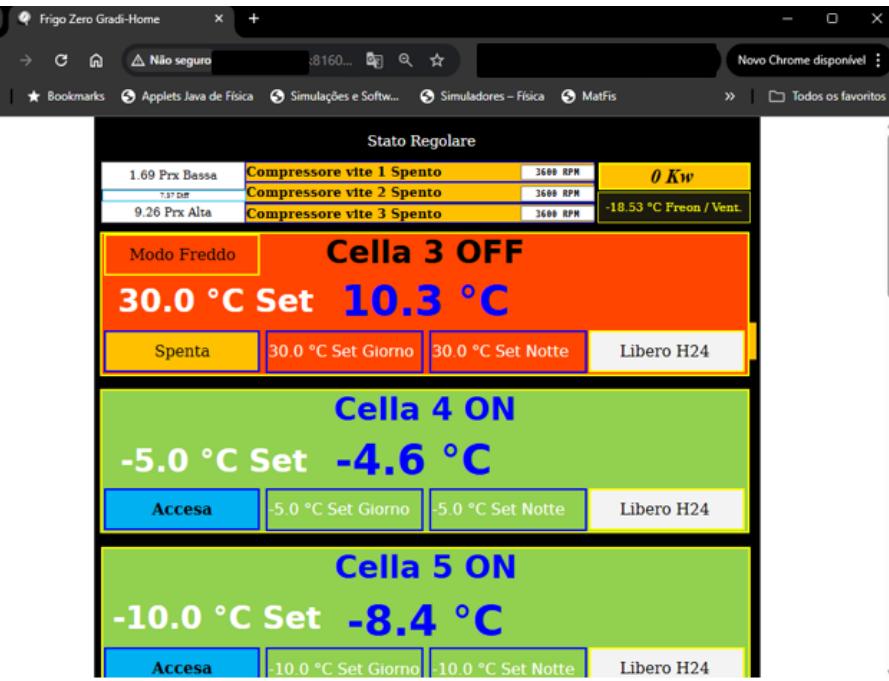
PLC + HMI em empresa de saneamento na Itália



LINHA DE ESTEIRAS 3

Modo de trabalho da linha 3

Descrição	Valor
Linha de desossa 3	0
Produção em andamento	0
Linha	Interromper a produção
Modo de trabalho	2
Pz Agora	500



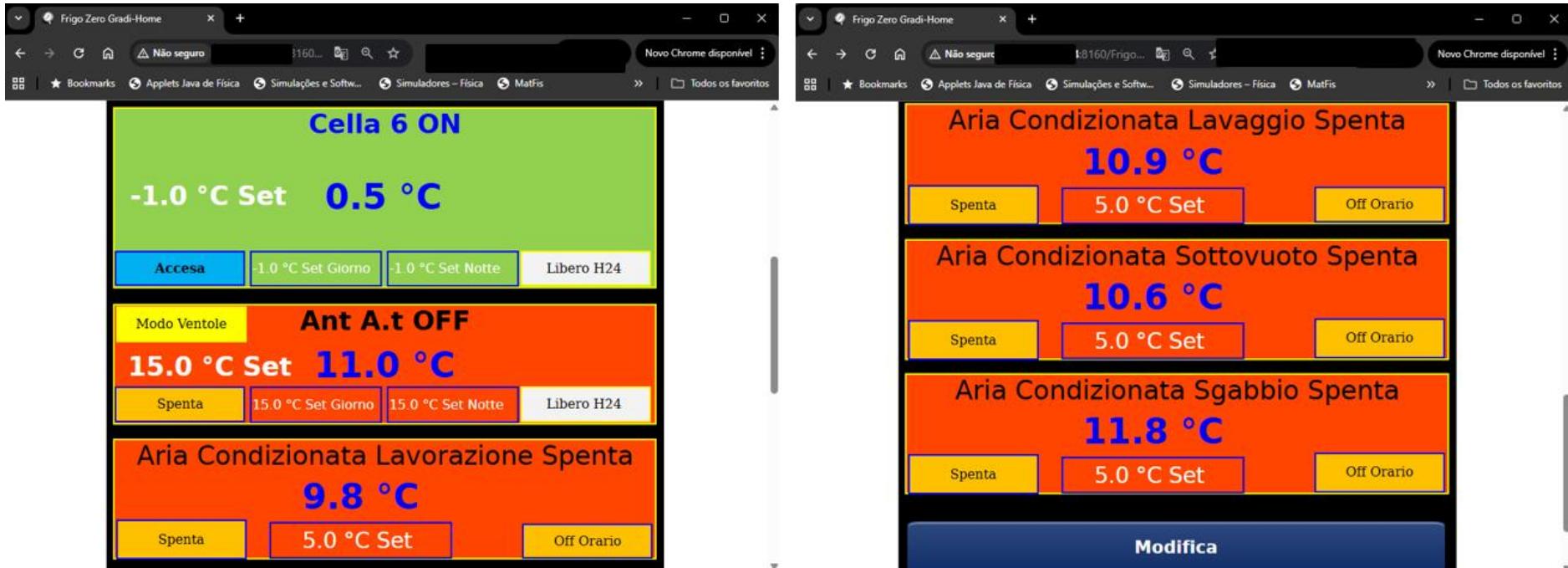
Frigo Zero Gradi-Home

Stato Regolare

1.69 Prx Bassa	Compressore vite 1 Spento	3600 RPM	0 Kw
7.37 Prx	Compressore vite 2 Spento	3600 RPM	
9.26 Prx Alta	Compressore vite 3 Spento	3600 RPM	-18.53 °C Freon / Vent
Modo Freddo	Cella 3 OFF	30.0 °C Set 10.3 °C	
Spenta	30.0 °C Set Giorno	30.0 °C Set Notte	Libero H24
Modo Freddo	Cella 4 ON	-5.0 °C Set -4.6 °C	
Spenta	-5.0 °C Set Giorno	-5.0 °C Set Notte	Libero H24
Modo Freddo	Cella 5 ON	-10.0 °C Set -8.4 °C	
Spenta	-10.0 °C Set Giorno	-10.0 °C Set Notte	Libero H24

Ativos Expostos na Internet

PLC + HMI em empresa de saneamento na Itália



Ativos Expostos na Internet

PLC + HMI em empresa de saneamento na Itália

General Information

Hostnames [REDACTED].it

Domains wadsl.it

Country Italy

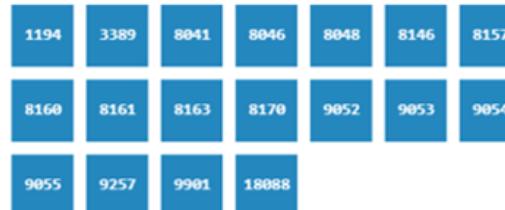
City Teramo

Organization [REDACTED]

ISP [REDACTED]

ASN [REDACTED]

Open Ports



OpenSSH 7.1

SSH-2.0-OpenSSH_7.1
Key type: ssh-rsa
Compression Algorithms:
none

Vulnerabilities

3 11 18 1 8

VNC

RFB 003.008
Authentication disabled

Serbatoio Idrop. Zona Muletti Serbatoio Idrop. Zona Mole

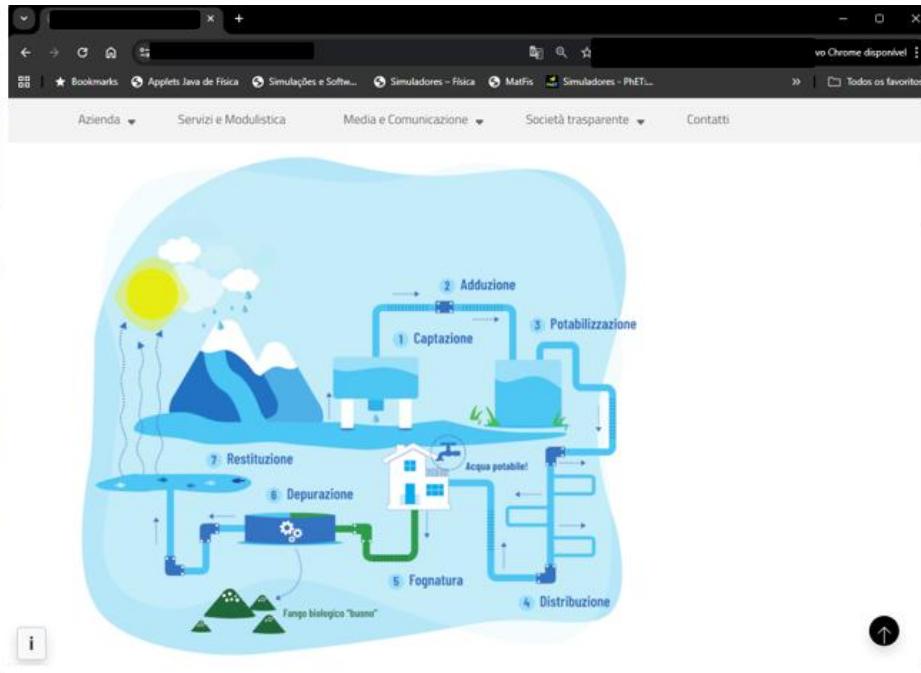
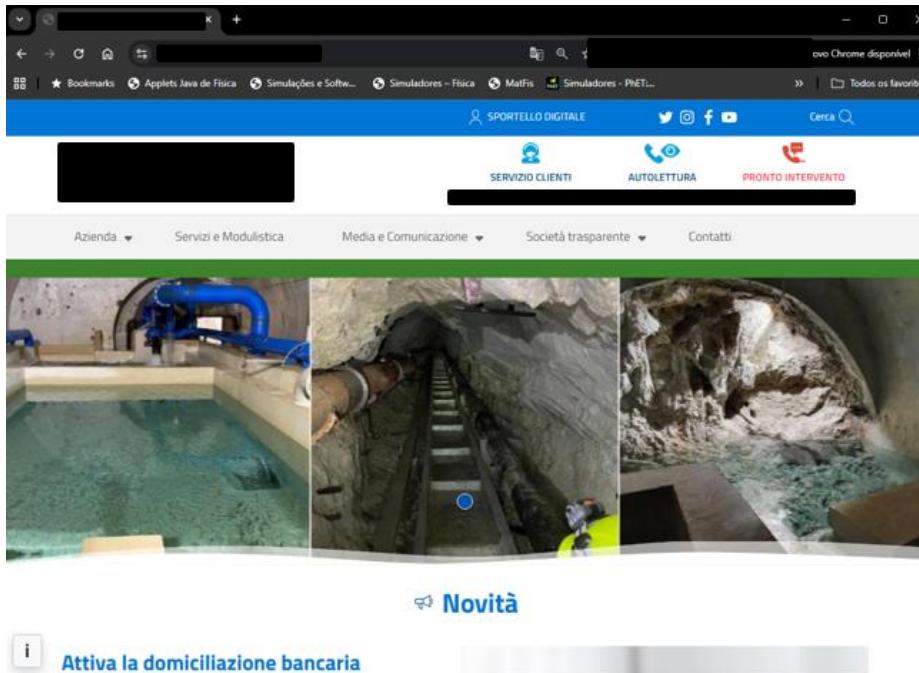


VNC:
Protocol Version: 3.8
Security Types:
1: None
Server Name: Untronics
Geometry: 800x480



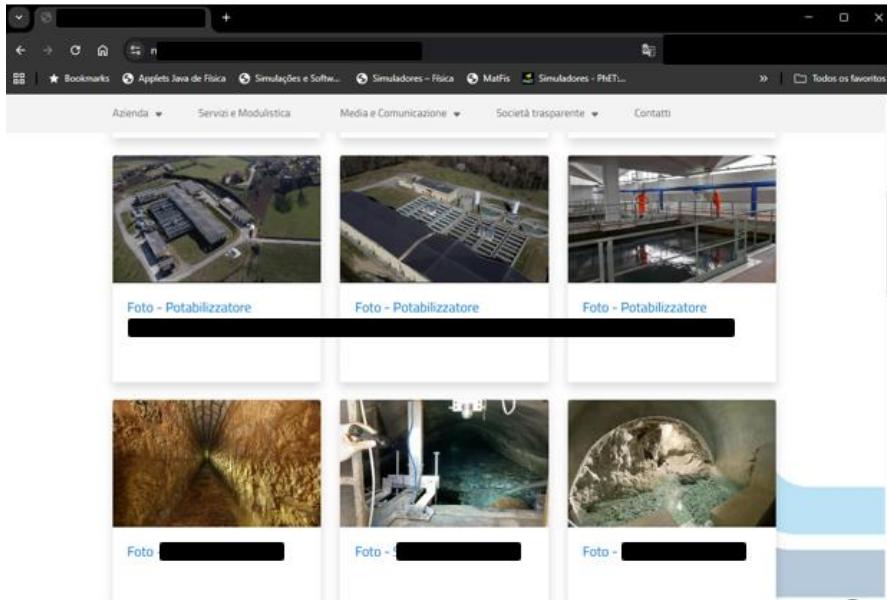
Ativos Expostos na Internet

PLC + HMI em empresa de saneamento na Itália



Ativos Expostos na Internet

PLC + HMI em empresa de saneamento na Itália



E NO BRASIL ?

Ciberataques no Brasil

Março/2024

Grupo Dark Storm anuncia ataques a infraestruturas críticas do Brasil

Ameaça visa backbones de Internet, aeroportos, hospitais, serviços e sites do Governo, como represália a nações que apoiam Israel contra o Hamas



Abril/2024

Infraestrutura crítica brasileira está sob ciberataques

Brasil sofreu 61 ciberataques em infraestruturas críticas em 2023, trazendo impactos em setores diversos, incluindo tecnologia, saúde, agricultura e governo



Ciberataques no Brasil

Abril/2025

Ataque hacker suspende atividades do IPEN, um dos principais produtores de fármacos contra o câncer do Brasil
Ação foi classificada como altamente sofisticada e organizada, segundo a Comissão Nacional de Energia Nuclear (CNEN) e paralisou a linha de produção por vários dias

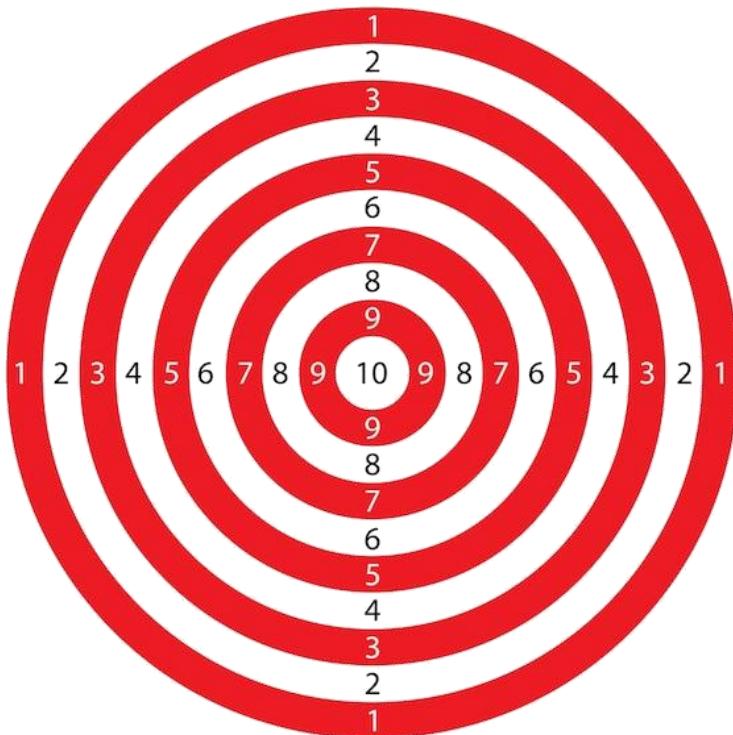


Ciberataques no Brasil



QUAIS SÃO AS MOTIVAÇÕES?

Motivações de Ciberataques



- Motivação Financeira
- Espionagem Industrial
- Hacktivismo Político
- Vingança
- Sabotagem
- Desafio e Notoriedade
- Curiosidade e Pesquisa
- Terrorismo

Componente Geopolítico



COMO INTEGRAR OT, IT E SEGURANÇA CIBERNÉTICA ?

Plano Estratégico - Etapas

Fase 1 - Diagnóstico e Avaliação Inicial <ul style="list-style-type: none">Inventário de ativos OT/ICSMapeamento de topologias físicas e lógicasRisk Assessment em OTAnálise de vulnerabilidades técnicasGap Analysis em relação à ISA/IEC 62443 e NIST SP 800-82	Fase 4 - Capacitação e Conscientização <ul style="list-style-type: none">Treinamento para operadores sobre segurança OTSimulações de resposta a incidentes OT
Fase 2 - Definição de Políticas e Arquitetura Segura <ul style="list-style-type: none">Criação e/ou revisão de política de segurança OTDefinição de zonas e conduites de segurançaDefinição de controles de acesso físico e lógicoRevisão de protocolos industriaisGestão de vulnerabilidades, patches e mudanças	Fase 5 - Monitoramento Contínuo e Resposta a Incidentes <ul style="list-style-type: none">Implantação de SOC OT ou integração com SOC ITConfiguração de SIEM com fontes OTResposta a Incidentes OT com playbooks específicosIntegração Threat Intelligence para ambientes industriais
Fase 3 - Implementação de Controles Técnicos <ul style="list-style-type: none">Segmentação de redes IT/OT com firewalls industriaisControle de acesso a dispositivos OTWhitelisting de aplicações em HMIs e servidoresMonitoramento contínuo de tráfego OTHardening de PLC, switches industriais, estaçõesControle de mídias removíveis e acesso remoto seguro	Fase 6 - Melhoria Contínua <ul style="list-style-type: none">Revisão periódica de riscosAtualização de patches/firmware em ciclo de manutençãoAuditórias técnicas anuais de segurança OTTestes de penetração não-invasivos (PenTest OT)Simulações anuais de crises cibernéticas OT

Plano Estratégico - Fontes

Normas e Frameworks



International Society of Automation
Setting the Standard for Automation™



International
Electrotechnical
Commission



International
Organization for
Standardization



Consultorias



Fornecedores



ISA 99 – ISA/IEC 62443



	IEC 62443-1-1	IEC 62443-1-2	IEC 62443-1-3	IEC 62443-1-4	
Geral	Conceitos e Modelos	Glossário Mestre de Termos e Abreviações	Métricas de conformidade de segurança do sistema	Ciclo de vida de segurança e casos de uso do IACS	
Políticas e Procedimentos	IEC 62443-2-1	IEC 62443-2-2	IEC 62443-2-3	IEC 62443-2-4	IEC 62443-2-5
Sistema	IEC 62443-3-1	IEC 62443-3-2	IEC 62443-3-3		
Componente	IEC 62443-4-1	IEC 62443-4-2			
	Requisitos do ciclo de vida de desenvolvimento de produtos seguros	Requisitos técnicos de segurança para componentes IACS			

Normas Internacionais para Segurança de Sistemas de Automação e Controle Industrial (IACS) e Redes de Tecnologia Operacional (OT)

Integração IT, OT e Cibersegurança



Obrigado!

Paulo Santos

Chefe de Departamento de Infraestrutura e Segurança da Informação - CEDAE

E-mail: psantos@cedae.com.br

Tel.: (21) 2562-6070
(21) 98736-9854