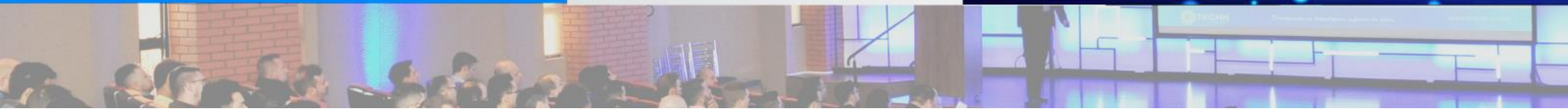
ETECHN evento técnico

INDÚSTRIA EFICIENTE



Segurança Industrial

A nova preocupação da Indústria 4.0

AVISO IMPORTANTE

O conteúdo técnico da palestra é de responsabilidade da empresa palestrante.

Fique à vontade para baixar o arquivo em PDF e se atualizar com as novas tecnologias apresentadas nesta edição.

Qualquer dúvida em relação ao conteúdo apresentado, você pode entrar em contato direto com o palestrante.

1. RockYou2021: The biggest password leak yet – 2021

The largest stolen password collection of all time saw 8.4 billion passwords leaked.

The hacker – whose identity is not disclosed – named the password compilation "RockYou2021", referencing the 2009 RockYou data breach, in which more than 32 million users had their passwords harvested.

The password hacker posted a 100GB txt file containing 8.4 billion password entries, alongside previous data leaks.

The hacker declared that the list contained 82 billion passwords. However, the exact number is around ten times smaller. Security experts also say that businesses and consumers are at risk.

Cybersecurity expert Troy Hunt explained on Twitter that RockYou2021 is not actually a list of 8.4 billion passwords. In fact, the 100GB seems to be a compilation of old password leaks, possible and frequently-used passwords, and a wordlist. This still makes it the biggest leak yet, because of the actual number and weight of data.

Decentralized Finance Platform Hacks

As the cryptocurrency ecosystem has evolved, tools and utilities for storing, converting, and otherwise managing it have developed at breakneck speed. Such rapid expansion has come with its share of oversights and missteps, though. And cybercriminals have been eager to capitalize on these mistakes, frequently stealing vast troves of cryptocurrency worth tens or hundreds of millions of dollars. At the end of March, for example, North Korea's Lazarus Group memorably stole what at the time was $540 million worth of Ethereum and USDC stablecoin from the popular Ronin blockchain "bridge." Meanwhile, in February, attackers exploited a flaw in the Wormhole bridge to grab what was then about $321 million worth of Wormhole's Ethereum variant. And in April, attackers targeted the stablecoin protocol Beanstalk, granting themselves a "flash loan" to steal about $182 million worth of cryptocurrency at the time.

DEFI

Euler Finance: Hacker steals around $197M in 2023's largest hack

Published 36 mins ago on March 13, 2023
By Suzuki Shillsalot

Notícias > Antivírus e Segurança

Ransomware WannaCry já infectou 200 mil computadores em 150 países

Um registro de domínio interrompeu acidentalmente uma (e apenas uma) das variantes do malware

Data Theft From Health Care Providers

Health care providers and hospitals have long been a favorite target of ransomware actors, who look to create maximum urgency to entice victims to pay up in the hopes of restoring their digital systems. But health care data breaches have also continued in 2022 as criminals pool data they can monetize through identity theft and other types of financial fraud. In June, the Massachusetts-based service provider Shields Health Care Group disclosed that it suffered a data breach throughout much of March impacting roughly 2 million people in the United States. The stolen data included names, Social Security numbers, birth dates, addresses, and billing information, as well as medical information like diagnoses and medical record indicators. In Texas, patients of Baptist Health System and Resolute Health Hospital announced a similar breach in June that exposed similar data, including Social Security numbers and sensitive patient medical information. Both Kaiser Permanente and Yuma Regional Medical Center in Arizona also disclosed data breaches in June.


BUT THAT'S NONE OF MY BUSINESS

Last Upd

Updates

Iranian Oil Terminal offline after malware attack

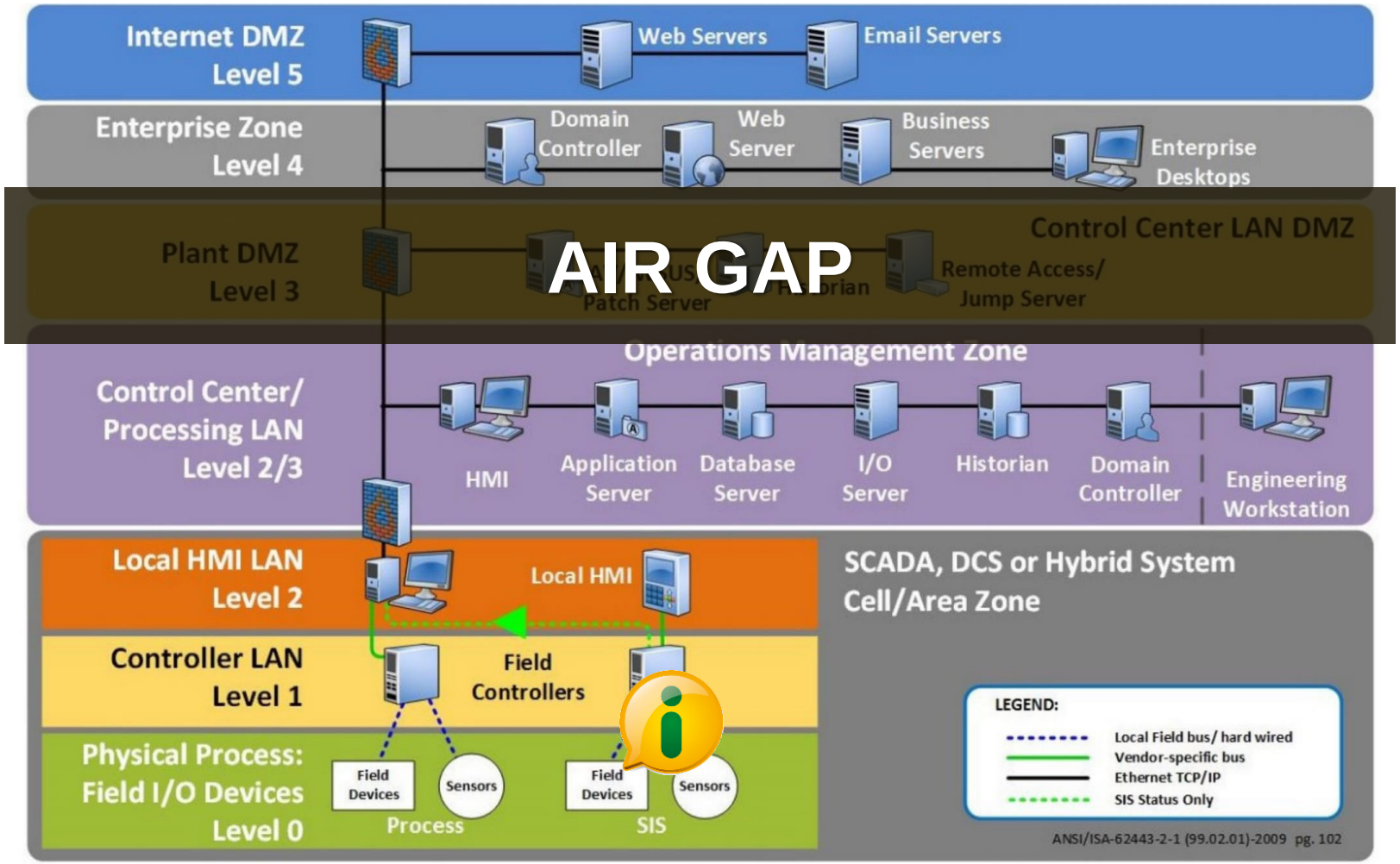
Event Year:	2012	**Reliability:**	Confirmed
Country:	Iran		
Industry Type:	Petroleum		
Description:	Iran has been forced to disconnect key oil facilities after suffering a malware attack. The computer virus is believed to have hit the internal computer systems at Iran's oil ministry and its national oil company. Equipment on the Kharg Island and at other Iranian oil plants has been disconnected from the net as a precaution.		
Impact:	Equipment on the Kharg Island and at other Iranian oil plants has been disconnected from the net as a precaution after suffering a malware attack.		

Title	Year	Industry	Country	Brief
Page 1 of 9				
Baku-Tbili			urkey	
Iranian Oil			an	
German Si			ermany	
Russian-Ba			nited States	
U-2 spy pl			nited States	
After 'God			nited States	
Public utili			nited States	
Broadcast			anada	
PLC Passv			anada	
Duplicate			anada	
Whitehat T			anada	
Hackers Ta			nited States	
Electronic Sabotage of Venezuela Oil Operations	2002	Petroleum	Venezuela	
Nimda Impact on Manufacturing System	2001	Food & Beverage	United States	
CIA Trojan Causes Siberian Gas Pipeline Explosion	1982	Petroleum	Russian Federation	
Hacker Takes Over Russian Gas System	1999	Petroleum	Russian Federation	
Iranian Hackers Attempt to Disrupt Israel Power System	2003	Power and Utilities	Israel	

"O custo anual global de crimes cibernéticos foi estimado em **€5.5 Tn em 2021**"

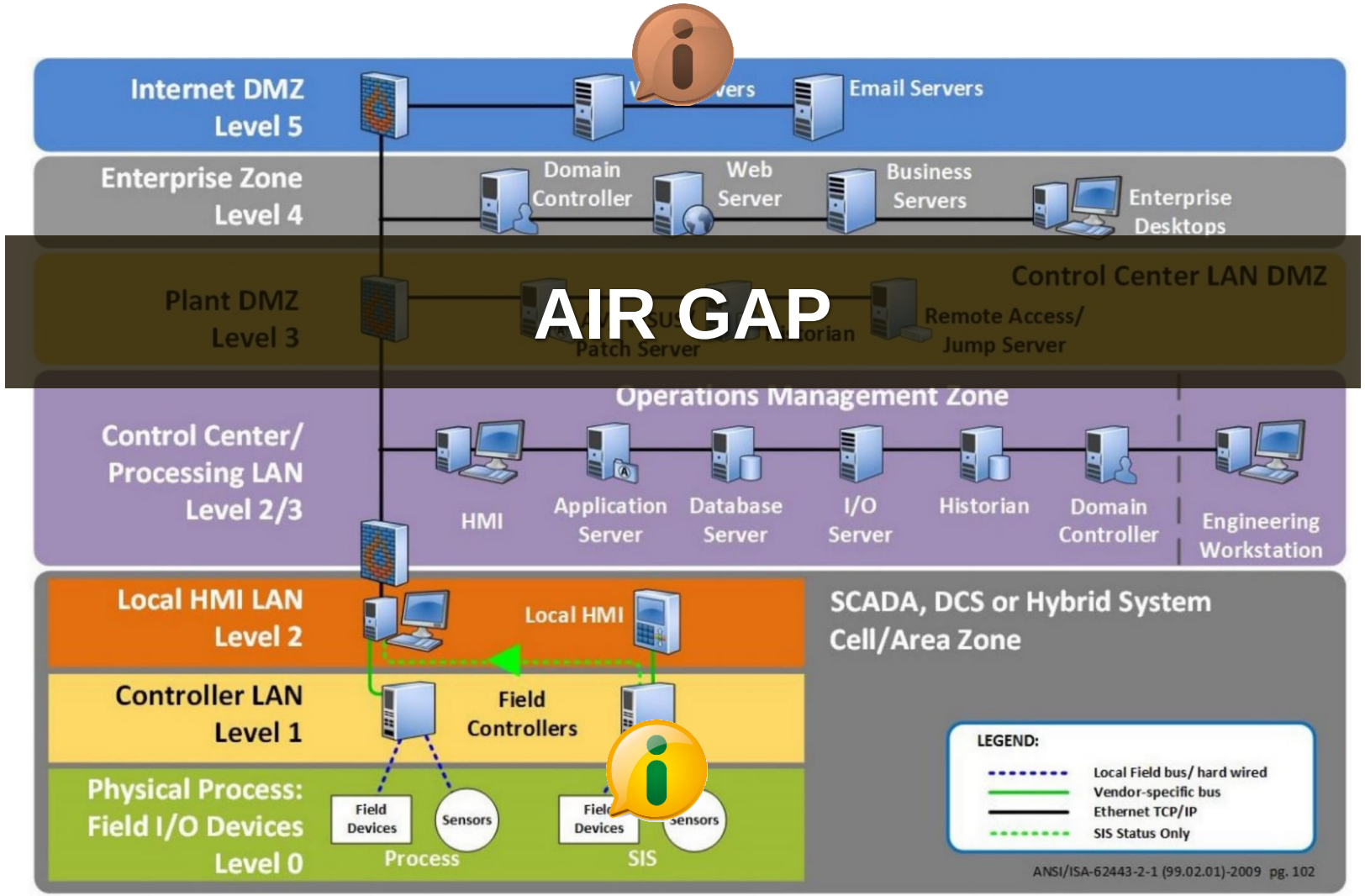
Source: ***Cyber Resilience Act - Factsheet | Shaping Europe's digital future (europa.eu)***

“Por que devo me preocupar com isso?”



A Industria 4.0

“Cuidar da Segurança Industrial será um requisito legal”



Status quo

Legislações da União Européia (UE):

Requisitos aplicáveis às empresas e entidades

- ✓ **NIS - DIRECTIVE (EU) 2016/1148 medidas para estabelecer um nível comum de Segurança Cibernética em toda EU**

- ➢ requisitos para os operadores de **Serviços Essenciais** e para os prestadores de serviços digitais (por exemplo, infraestruturas críticas)
- ➢ ex., EULYNX - Especificação para o setor ferroviário

Requisitos aplicáveis à Máquinas

- ✓ **MD – Machinery Directive 2006/42/EC**

- ➢ Não há requisitos específicos para a Segurança Cibernética

Legislações fora da União Européia (UE):

USA:
- ✓ Cyber Incident Reporting Act
- ✓ The State and Local Government Cybersecurity Act
- ✓ Federal Rotational Cyber Workforce Program Act
- ✓ Strengthening American Cybersecurity Act

China:
- ✓ Data Security Law

India:
- ✓ IT Act

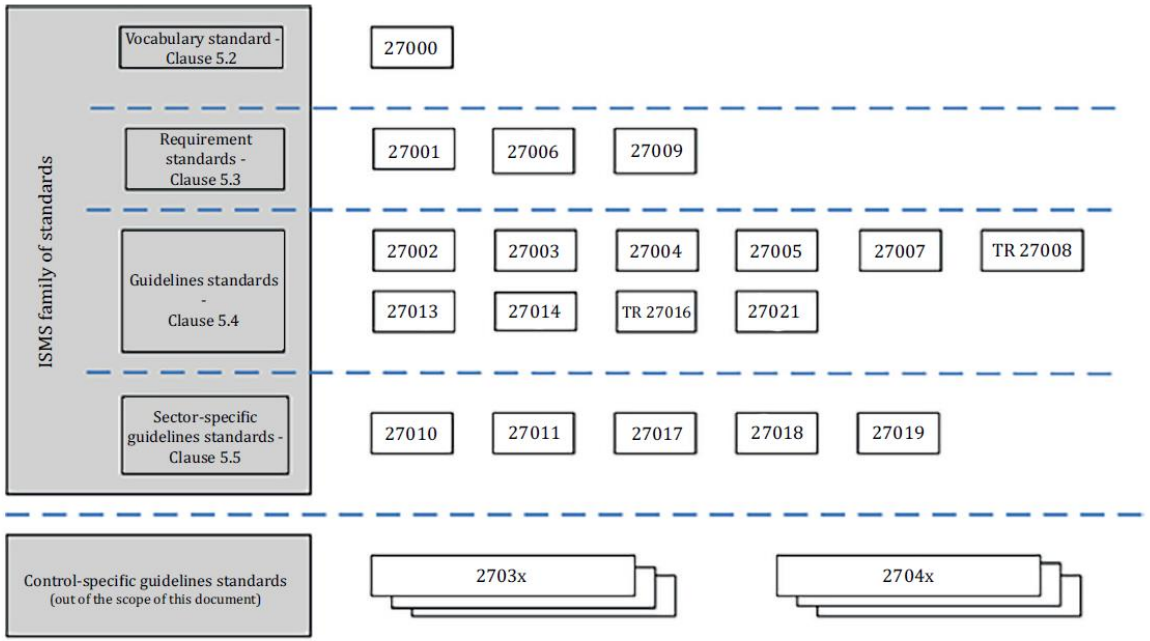
Australia:
- ✓ Security of Critical Infrastructure Act 2018

...

As duas principais Normas

ISO27000

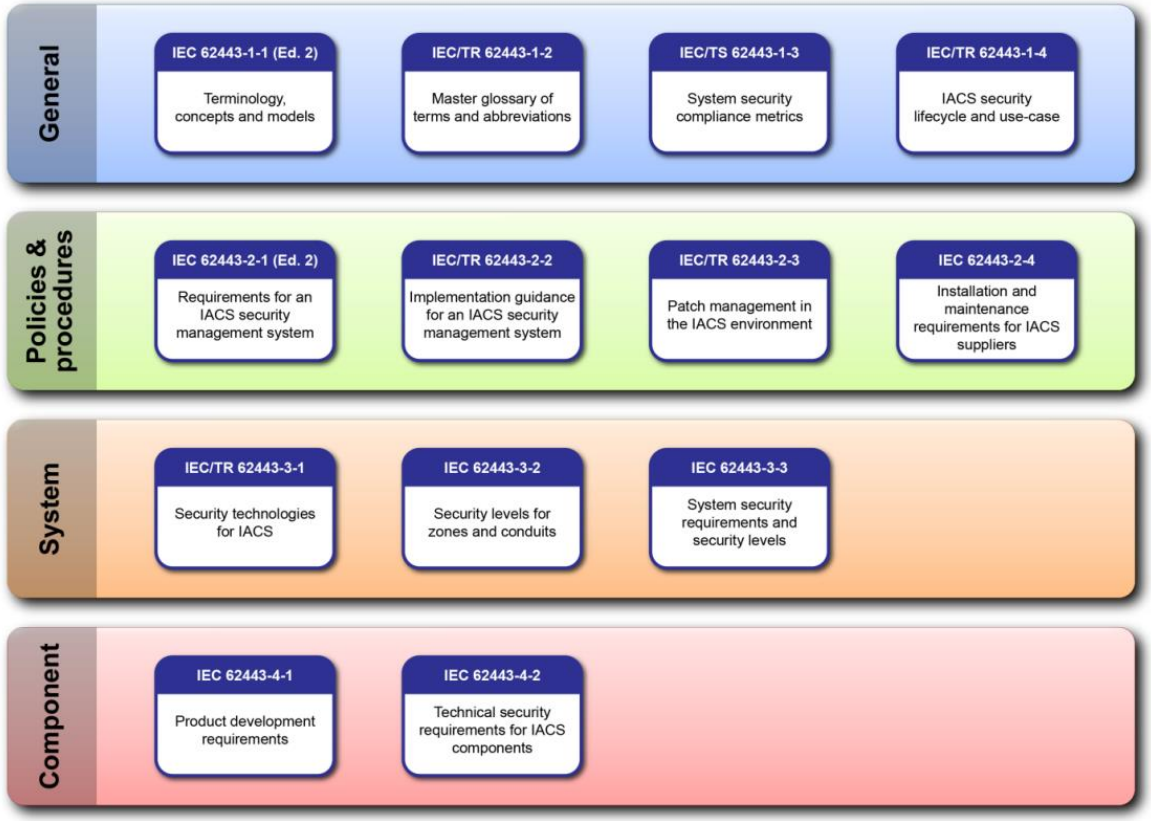
Information Security Management Systems (ISMS)



Source: IEC/ISO 27000:2018

IEC 62443

Security for Industrial Automation & Control System (IACS)



UE

OCT 2024

Network and Information Systems 2
NIS 2

Requisitos aplicáveis às **Empresas**

- Treinamentos Específicos
- Medidas para gerir e mitigar os riscos
- Obrigações de comunicações de riscos
- Requisitos de segurança para Serviços Essenciais e Importantes, i.e:, energia elétrica, ferrovias, **fabricação de máquinas e equipamentos**

MAY 2023

Machinery Regulation

Requisitos aplicáveis à **Máquinas**

- Proteção contra a intrusão (**foco nas funções de segurança de máquinas**)
- **MAQUINAS NOVAS E EXISTENTES**
- A segurança cibernética será parte da ISO 12100

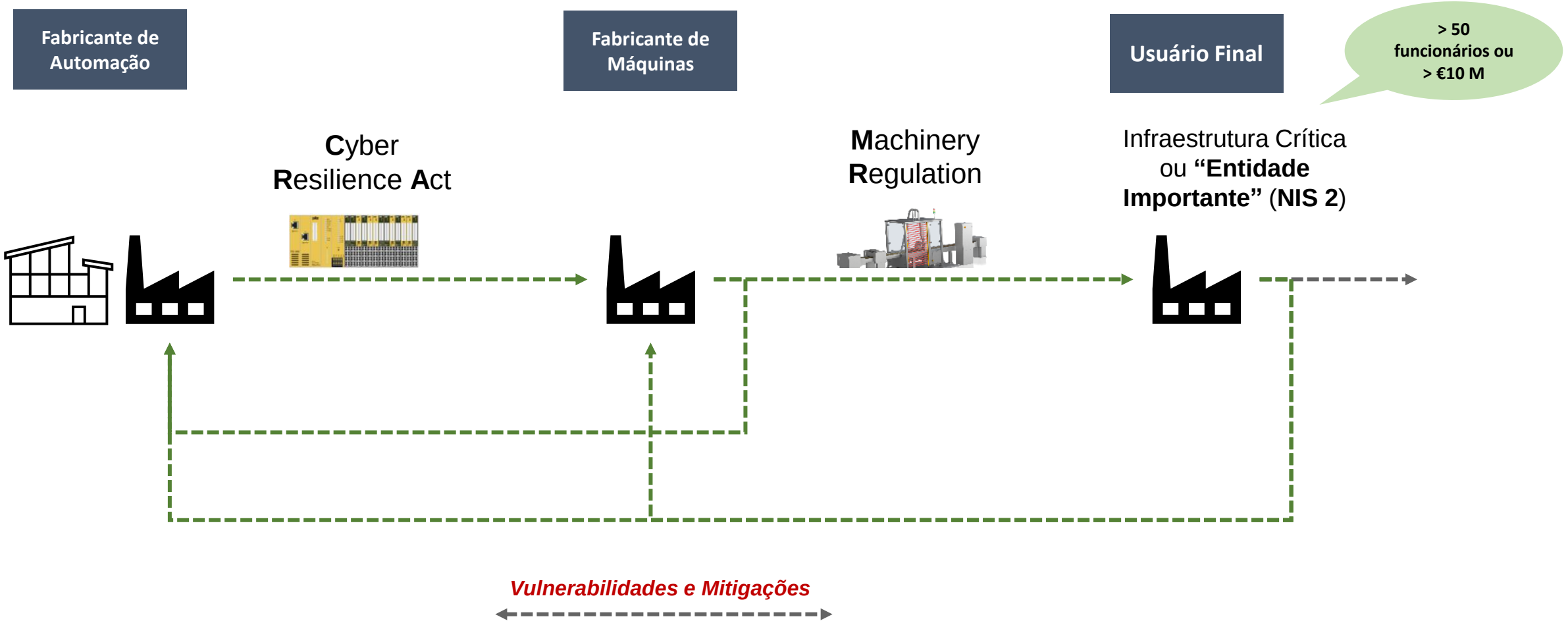
OCT 2024

Cyber Resilience Act

Requisitos aplicáveis a **Produtos com Elementos Digitais**

- Processos de desenvolvimento
- Os produtos com elementos digitais devem ser fornecidos sem quaisquer vulnerabilidades conhecidas.

As vulnerabilidades de segurança devem ser mitigadas em todo o processo produtivo



Machinery and Equipment Manufacturers Association
- Working Group Industrial Security

German Electro and Digital Industry Association
- Working Group Industrial Security

Is the first IT security platform in Germany for small and medium-sized enterprises (SMEs) in the field of automation. CERT@VDE helps to react appropriately to digital threats and to communicate security gaps.
https://cert.vde.com/

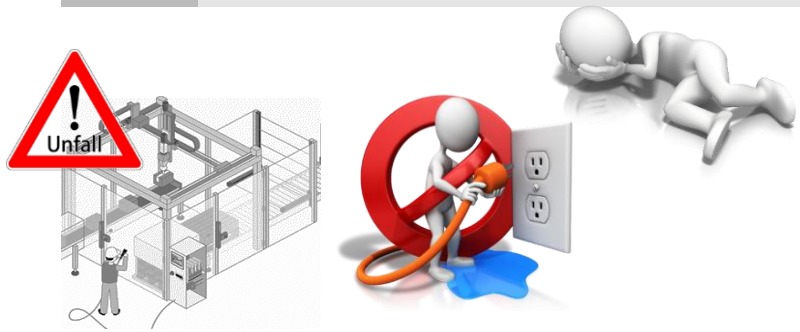
TC44/WG 15 – IEC TS 63074 – Safety of machinery – Security aspects related to functional safety of safety-related control systems

Guest in DKE/AK 931.1.2 German mirror to IEC 62443

Technical Committee 3.22 “IT-Security” – VDI/VDE-GMA

A Segurança de Máquinas precisa estar alinhada com a Segurança Industrial

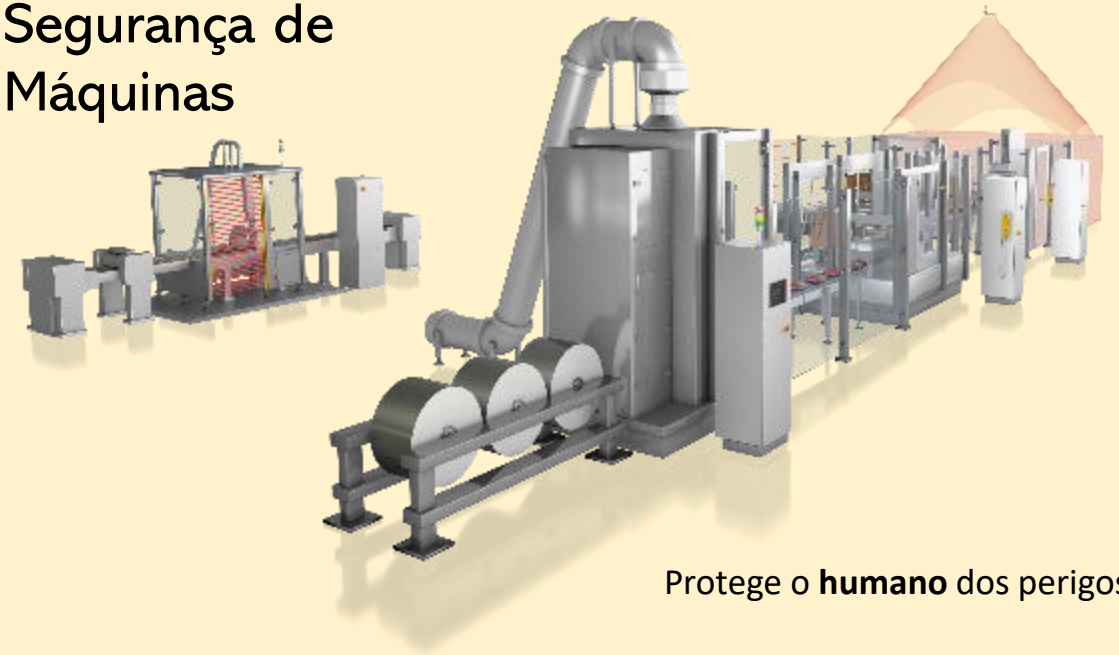
Colegas sofrem ferimentos graves!



Principais Legislações de segurança aplicadas no Brasil:

- NR 6 – Equipamento de Proteção Individual (EPI);
- NR 9 – Programa para Prevenção de Riscos Ambientais (PPRA);
- NR 10 – Segurança em Instalações e Serviços em Eletricidade;
- NR 12 – Segurança no Trabalho em Máquinas e Equipamentos;
- NR 13 – Caldeiras e Vasos de Pressão;
- NR 15 – Atividades e Operações Insalubres;
- NR 17 – Ergonomia;
- NR 26 – Sinalização de Segurança.

Segurança de Máquinas



Protege o **humano** dos perigos na máquina

Ex: proteção contra riscos devido a peças móveis em máquinas.

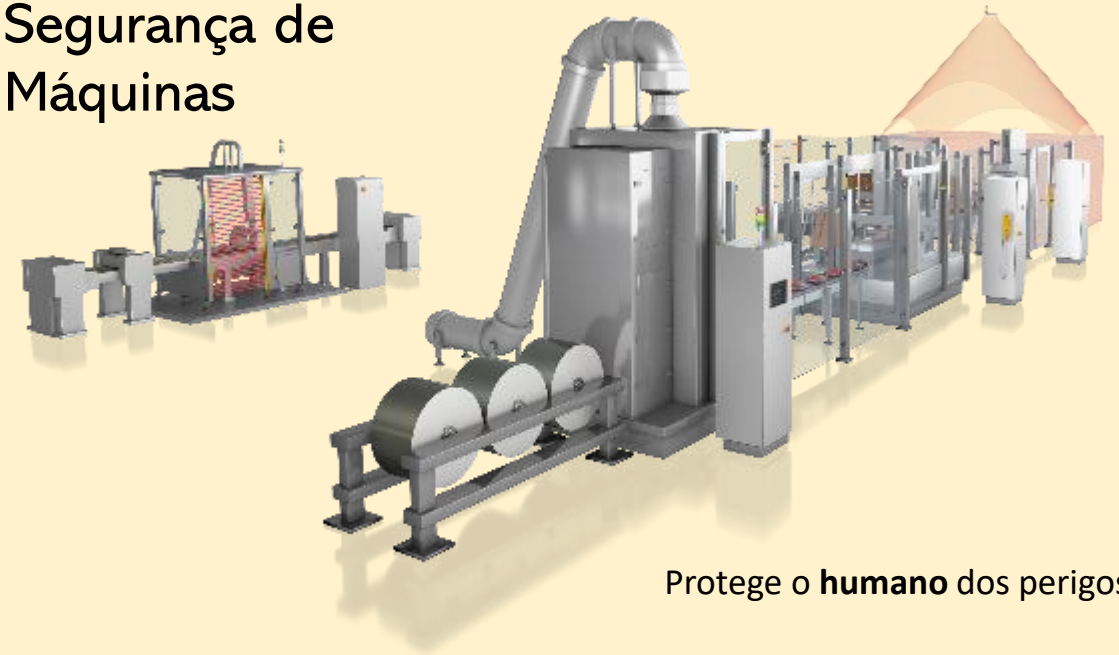
A Segurança de Máquinas precisa estar alinhada com a Segurança Industrial

Segurança Industrial

Protege sua **máquina** e seus **dados** contra manipulação e acesso não autorizado.

"Segurança Cibernética!!!"

Segurança de Máquinas

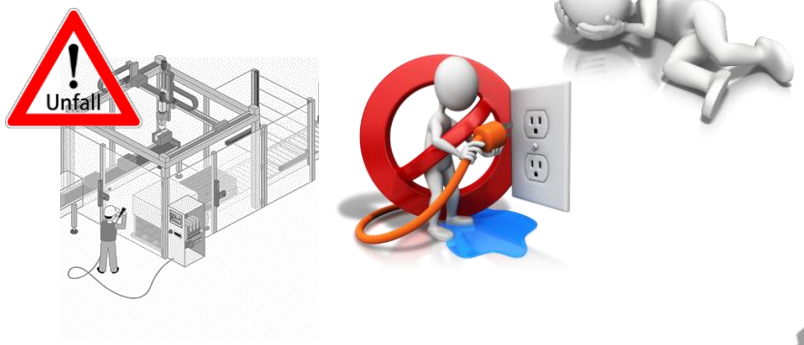


Protege o **humano** dos perigos na máquina

Ex: proteção contra riscos devido a peças móveis em máquinas.

Desafios diários na Operação Industrial

SEGURANÇA
Colegas sofrem ferimentos graves!
do Operador



Proteção de DADOS
Perda de dados e roubo de arquivos!

Responsabilidade
Os gerentes serão responsabilizados!
CIVIL

Riscos de
Paradas de Máquinas Custam!
PRODUÇÃO

EMPLOYEE PROTECTION

LI
PRO

Gerente de Automação / Manutenção

PRODUCTIVITY PROTECTION

PROTEÇÃO DE DADOS

Segurança Industrial

Segurança Operacional

SISTEMA DE CONTROLE DA MÁQUINA

Painel de Controle com SW de Segurança

Possibilidade

Acesso Fisico ao Componente sem Autorização

Consequencia

Risco Cibernético ao Componente da Malha (SRP/CS)

Impacto

SISTEMA DE SEGURANÇA DA MÁQUINA

Perda da Função de Segurança

- Malware instalado em um PLC de Segurança

Pode gerar

Aumento do Risco Operacional

- Função de Segurança Desabilitada

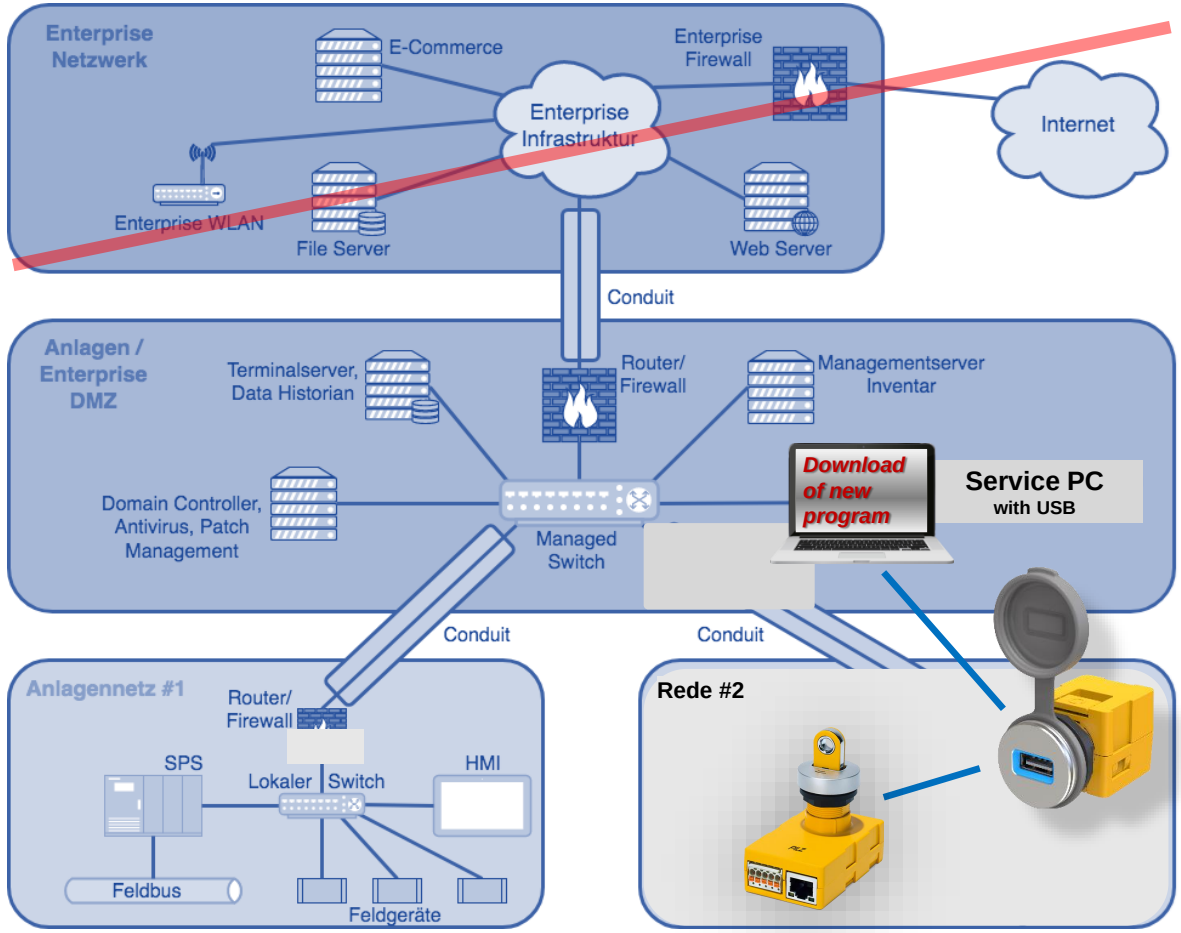
Pode resultar

Acidente de Trabalho

Contra-medidas de Segurança Industrial

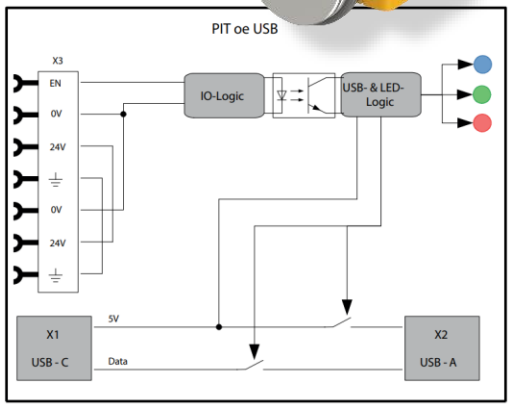
Requisito Básico de Segurança	Descrição
Controle de **Identificação e Autenticação**	**Identificar e autenticar todos os usuários** (pessoas, processos de software e dispositivos) antes de permitir que eles acessem o sistema de controle

Controle de Identificação e Autenticação



→ *Contra-medidas*

Portas USB Protegidas com Função de Segurança



- Identificação do operador e suas permissões
- Log de banco de dados de todos os acessos
- Comunicação Modbus/TCP e opção OPC UA
- Prevenção de infecção por Malware

Transponder para Controle de Acesso Seguro

Contra-medidas de Segurança Industrial

Requisito Básico de Segurança	Descrição
Controle de **Identificação e Autenticação**	**Identificar e autenticar todos os usuários** (pessoas, processos de software e dispositivos) antes de permitir que eles acessem o sistema de controle
Controle de Usuário	Impor os **privilégios** atribuídos para um **usuário autenticado** executar a ação solicitada no sistema de controle e monitorar esses privilégios

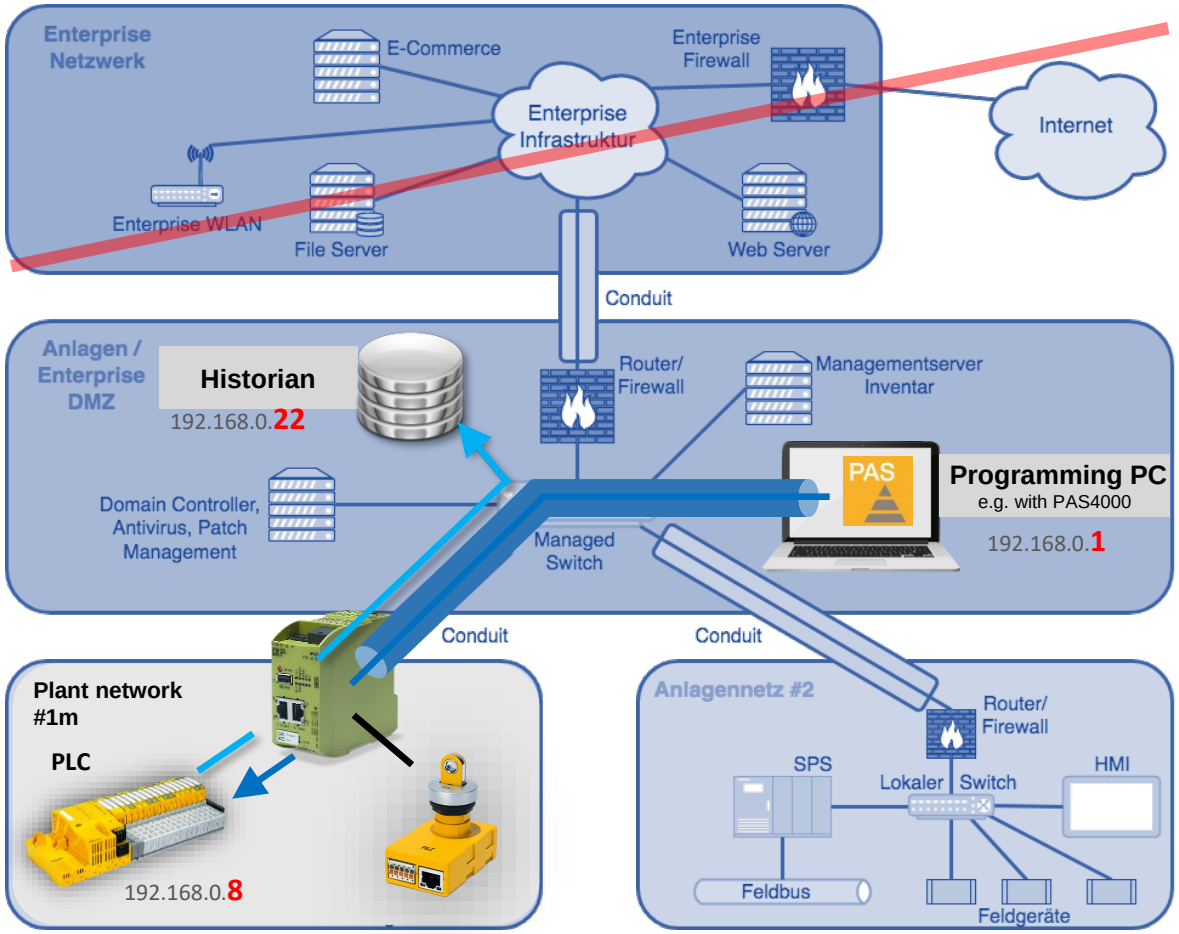
Controle de Usuários

Transponder para Controle de Acesso Seguro

Contra-medidas de Segurança Industrial

Requisito Básico de Segurança	Descrição
Controle de **Identificação e Autenticação**	**Identificar e autenticar todos os usuários** (pessoas, processos de software e dispositivos) antes de permitir que eles acessem o sistema de controle
Controle de Usuário	Impor os **privilégios** atribuídos para um **usuário autenticado** executar a ação solicitada no sistema de controle e monitorar esses privilégios
Restrição do Fluxo de Dados	**Segmentar o sistema de controle por meio de zonas** e canais para limitar os dados de fluxo desnecessários

Restrição do Fluxo de Dados

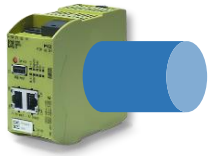


→ *Contra-medidas*

1. Firewall com regras.

Initiator	via Protocol / Port	to
192.168.0.**1**	**RTFN**	192.168.0.**8**
192.168.0.**8**	**OPC UA**	192.168.0.**22**

2. VPN Encriptada.



3. Transponder para Controle de Acesso Seguro

SEGURANÇA DO OPERADOR

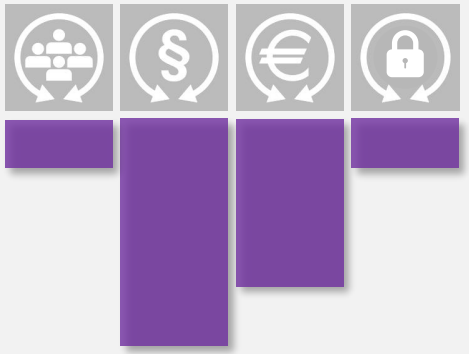
Tecnologia de Controle de Acesso permite definir Modos de Operações e Permissões de Acesso

Controle de Acesso Seguro

Controle de Acesso Integrado

- ✓ A Empresa deve garantir que **apenas pessoal qualificado e treinado possa trabalhar** em tal modo de operação.
- ✓ **Chaves Individuais com Transponder** definem os modos de operação como automático, configuração, serviço, ...
- ✓ Modos de operação e as funções relevantes dos funcionários gerenciados remotamente com **Sistema de Gestão de Controle de Acesso**

Gerente de Planta

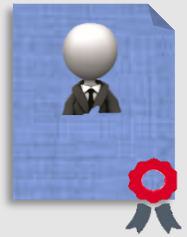


RESPONSABILIDADE CIVIL

DATA
PROETECTION

PRODUCTIVITY
PROTECTION

A Gerência é responsável civilmente por não instruir ou adotar medidas de segurança



Culpabilidade Organizacional / Operacional pode ser dada de 3 maneiras

Culpabilidade por Seleção

Deveres e responsabilidades delegadas a **funcionários inadequados ou não qualificados.**

- ✓ **Contra-medidas**
- ✓ Cada funcionário recebe seu próprio transponder pessoal
- ✓ As permissões no transponder dependem das qualificações do funcionário
- ✓ Transponders e funcionários são gerenciados remotamente

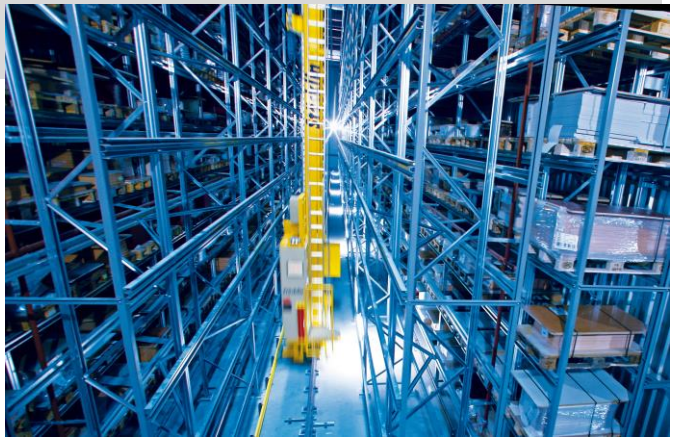
Culpabilidade por Instrução

Não há **Instruções de Trabalho**, ou estão incorretas / incompletas…

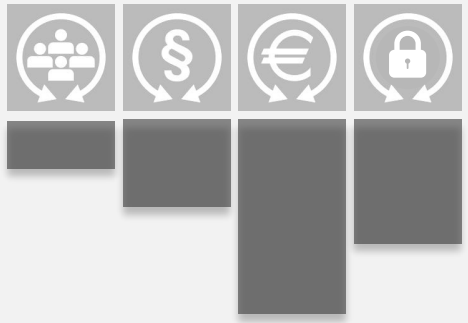
Culpabilidade por Supervisão

As **checagens são realizadas apenas esporadicamente** ou não são realizadas

- ✓ **Contra-medidas**
- ✓ Limite de tempo para permissões do transponder
- ✓ Validade de uma permissão

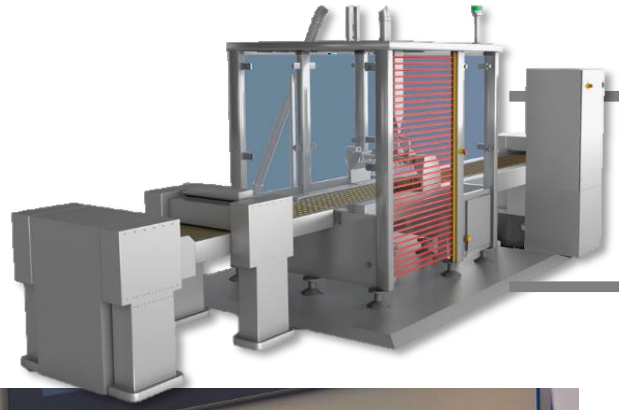


Gerente de Produção

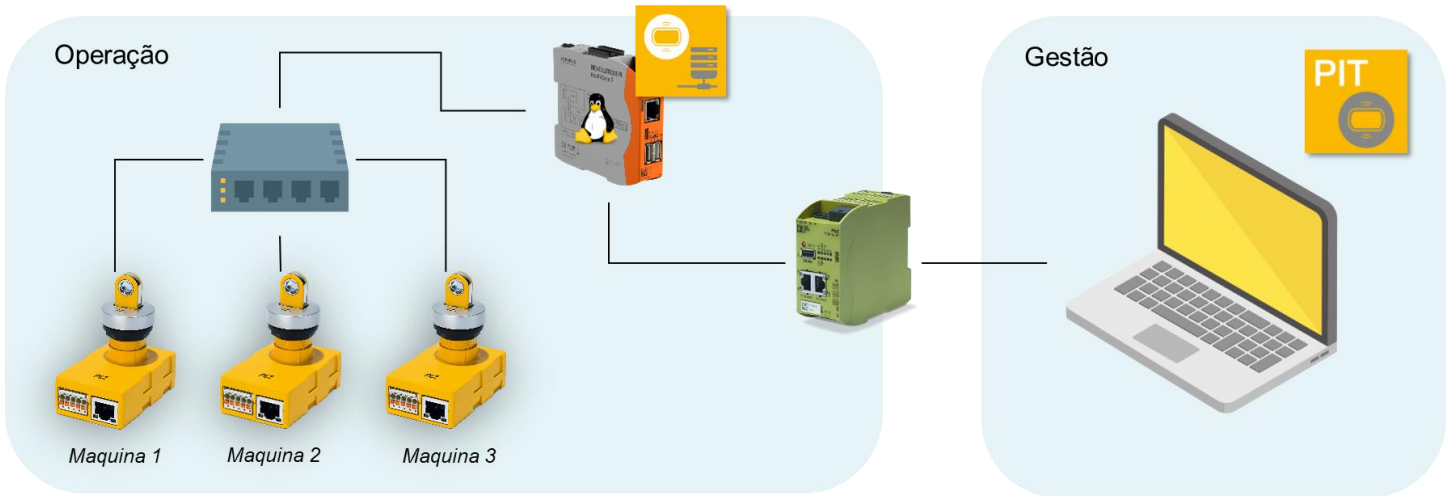


PROTEÇÃO DA PRODUTIVIDADE

Parâmetros são alterados de forma incorreta ocasionando perdas na produção



Manipulação Intencional ou Inadvertida	**Contra-medidas** ✓ **Controle de Permissões** ✓ Níveis de usuário claros, especialmente em máquinas complexas aumentam a proteção de acesso e dados
Operações Complexas	Os funcionários **não entendem os processos ou ficam sobrecarregados com funções e opções** de configuração. **Contra-medidas: As ações podem ser claramente atribuídas aos usuários capacitados**
Controle e Identificação	Entradas não personalizadas e não monitoradas, oportunidades de acesso desprotegidas. **As senhas são inseguras, não personalizadas e geralmente conhecidas** **Contra-medidas** ✓ **Individualiação de Usuários Assegura Transparência e Auditoria**



Cuidar da Segurança Industrial/Cibernética não é mais um "nice to have", é uma necessidade e requisito legal

"O custo anual global de crimes cibernéticos foi estimado em **€5.5 Tn em 2021**"

Source: ***Cyber Resilience Act - Factsheet | Shaping Europe's digital future (europa.eu)***

PILZ

THE SPIRIT OF SAFETY

FRANZ ZANOW

Consultor Comercial Pilz do Brasil

f.zanow@pilz.com.br

(41) 99222-3515

www.pilz.com.br