Setting the Standard for Automation™

ISA Rio de Janeiro Section
Palestra Técnica

Renata Valente de Araújo

24 de maio de 2018

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Apresentação

2007	• Graduação em Engenharia Elétrica na UFBA
2007 a 2013	• Chemtech – Siemens – Atuação na área de projetos industriais nas áreas de automação, instrumentação, elétrica, telecomunicações e segurança cibernética
2013 a 2016	• Coelba – Atuação no setor comercial – departamento de recuperação de crédito • Coelba – Atuação na área de regulação da distribuição
2016	• Mestre em Engenharia Elétrica pela UFBA
2016	• Atualmente responsável por segurança da informação industrial da Braskem

Braskem

ISA

7 BRASKEM EM NÚMEROS

8.000
INTEGRANTES EM TODO O MUNDO

ATUAÇÃO EM **70** PAÍSES

EBITDA DE R$ **11,5** BI
EM 2016

RECEITA BRUTA R$ **55** BILHÕES

LUCRO LIQUIDO CONSOLIDADO DE R$ **768** MI

R$ **2,9** BI DE INVESTIMENTOS REALIZADOS

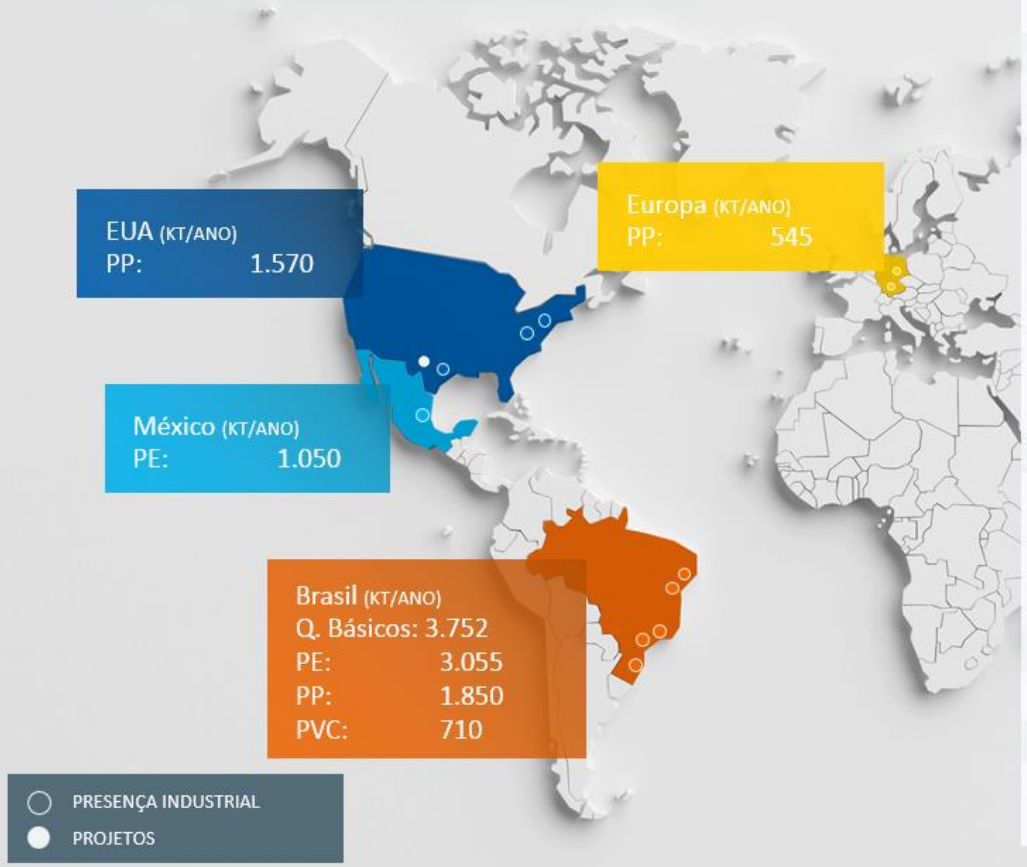
PRODUÇÃO DE MAIS DE **20** MI TONELADAS/ANO DE RESINAS TERMOPLÁSTICAS E OUTROS PRODUTOS QUÍMICOS

DISPÊNDIO EM INOVAÇÃO **79** US$ MI

41 UNIDADES INDUSTRIAIS

4 FOOTPRINT INDUSTRIAL

41 UNIDADES INDUSTRAIS PELO MUNDO



ESTADOS UNIDOS

Pensilvânia	1 PP
West Virginia	1 PP
Texas	3 PP | 1 UTEC

MÉXICO

Veracruz	1 CRACKER | 3 PE

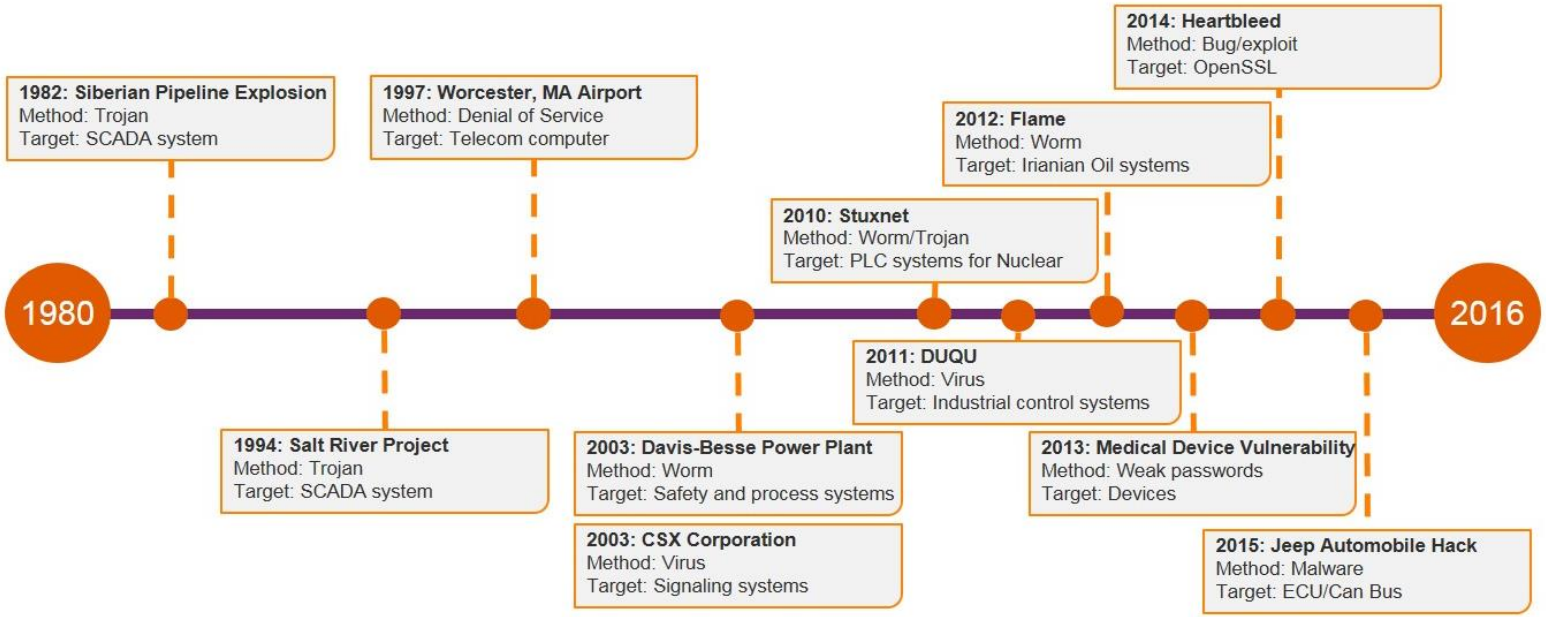
ALEMANHA

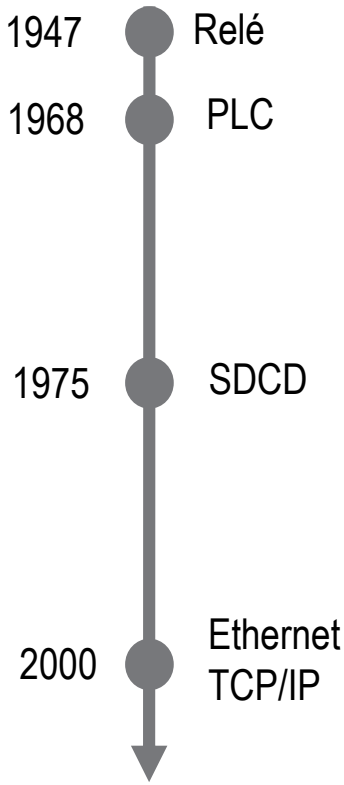
North Rhine	1 PP
Saxony-Anhalt	1 PP

BRASIL

Bahia	1 CRACKER | 4 PE | 1 PP | 1 PVC | CLORO SODA
Alagoas	2 PVC | 1 CLORO SODA
São Paulo	2 PE | 2PP | 1 CRACKER | 1 ESPECIALIDADES
Rio de Janeiro	1 CRACKER | 1 PE | 1 PP
Rio Grande do Sul	2 CRACKER | 5 PE | 2PP

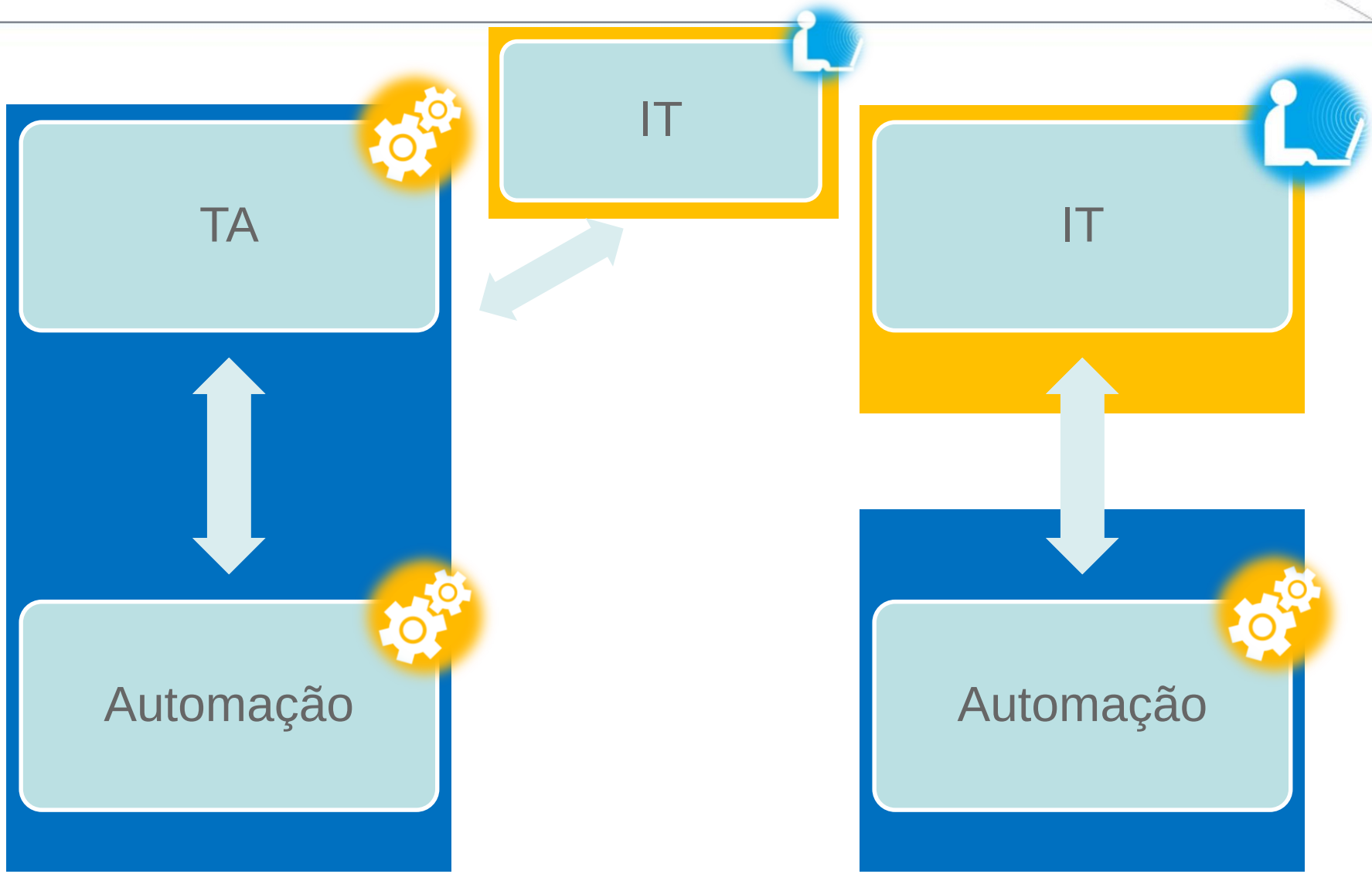
Dados Históricos





Fonte: Gemalto – Breaches of Industrial Control Systems: 1980 – 2016
https://blog.gemalto.com/security/2016/04/07/utilities-under-siege-debunking-smart-grid-cyber-security-myths/

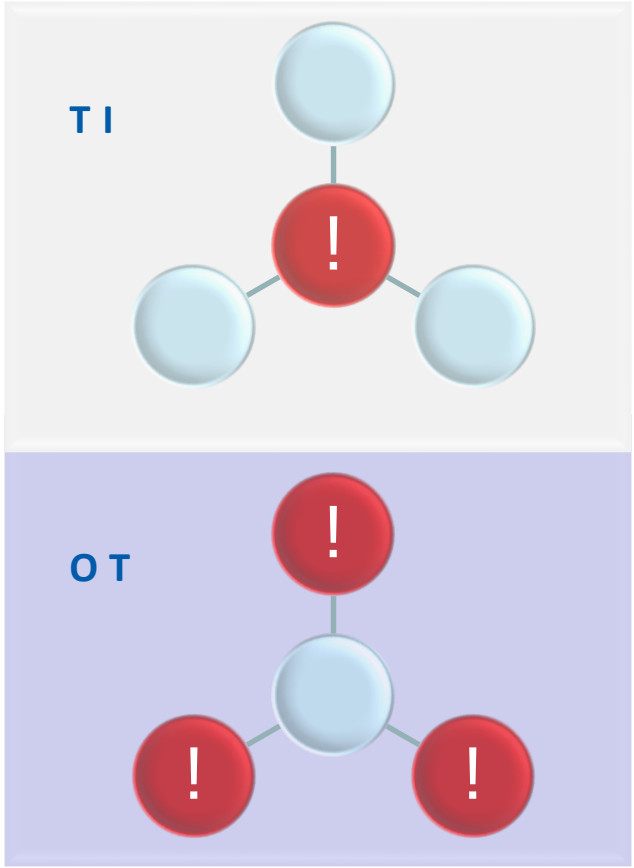
OT vs IT



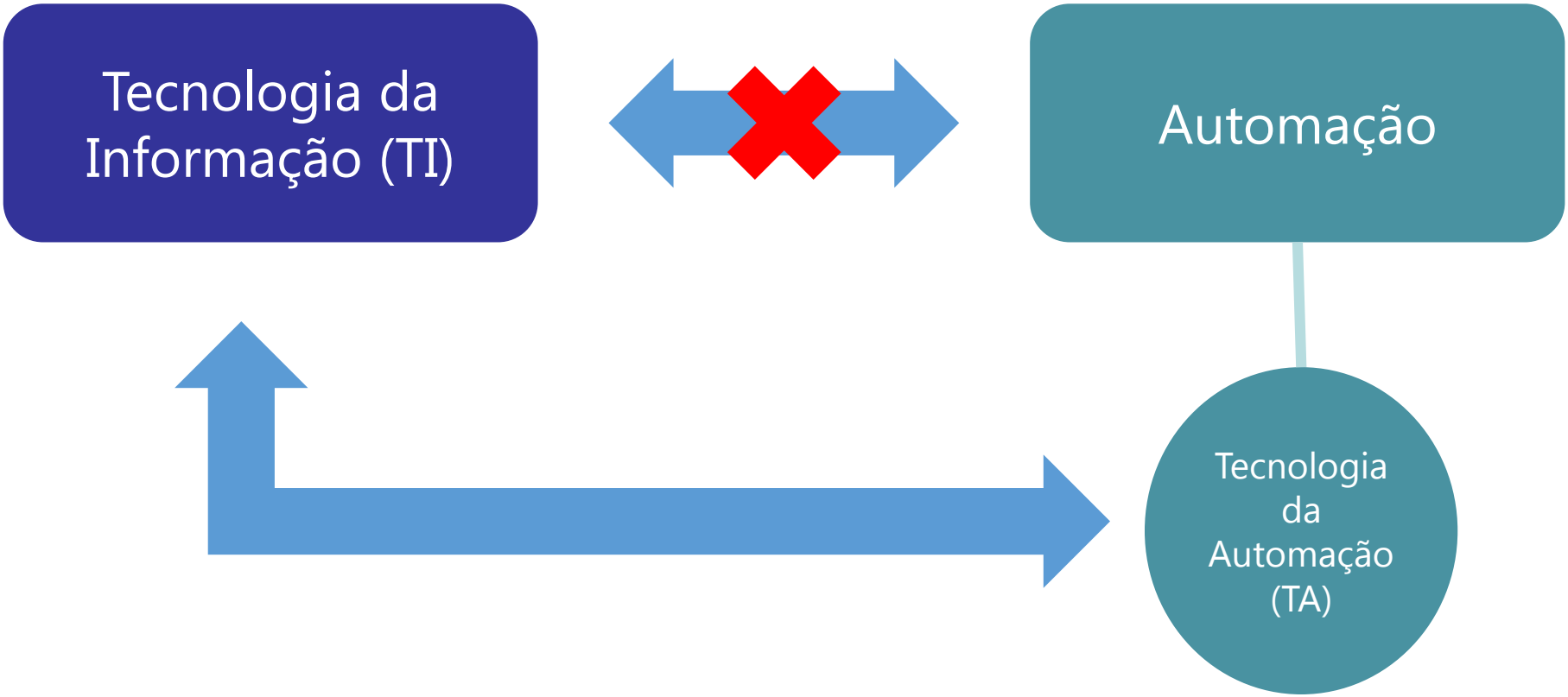
Diferenças OT/IT

A infraestrutura crítica de TI é passível de centralização, ao passo que na automação industrial, quanto mais próximo ao processo industrial, mais crítico é o dispositivo. Esta diferença estrutural faz com que, apesar de utilizarem as mesmas tecnologias, a TI e a automação atuem de forma muito distinta.

- Diferentes níveis de agilidade e criticidade na prestação de serviços e atendimento;
- Considerável nível de subordinação à área de produção/manutenção de cada site;
- Conhecimento técnico e do negócio das plantas é imprescindível – Diversidade de perfil profissional;
- Requer conhecimento de normas típicas industriais: ISA-95, ISA-88, IEC-62443, ISA-10, RC 14001, etc.
- Dispositivos e ativos não padronizados e gestão de portfólio distribuída;
- Intervenções requerem planejamento crítico de processo;
- Ocorrência de falha leva a paradas severas e afetam ativos, produção, segurança, saúde e meio ambiente.



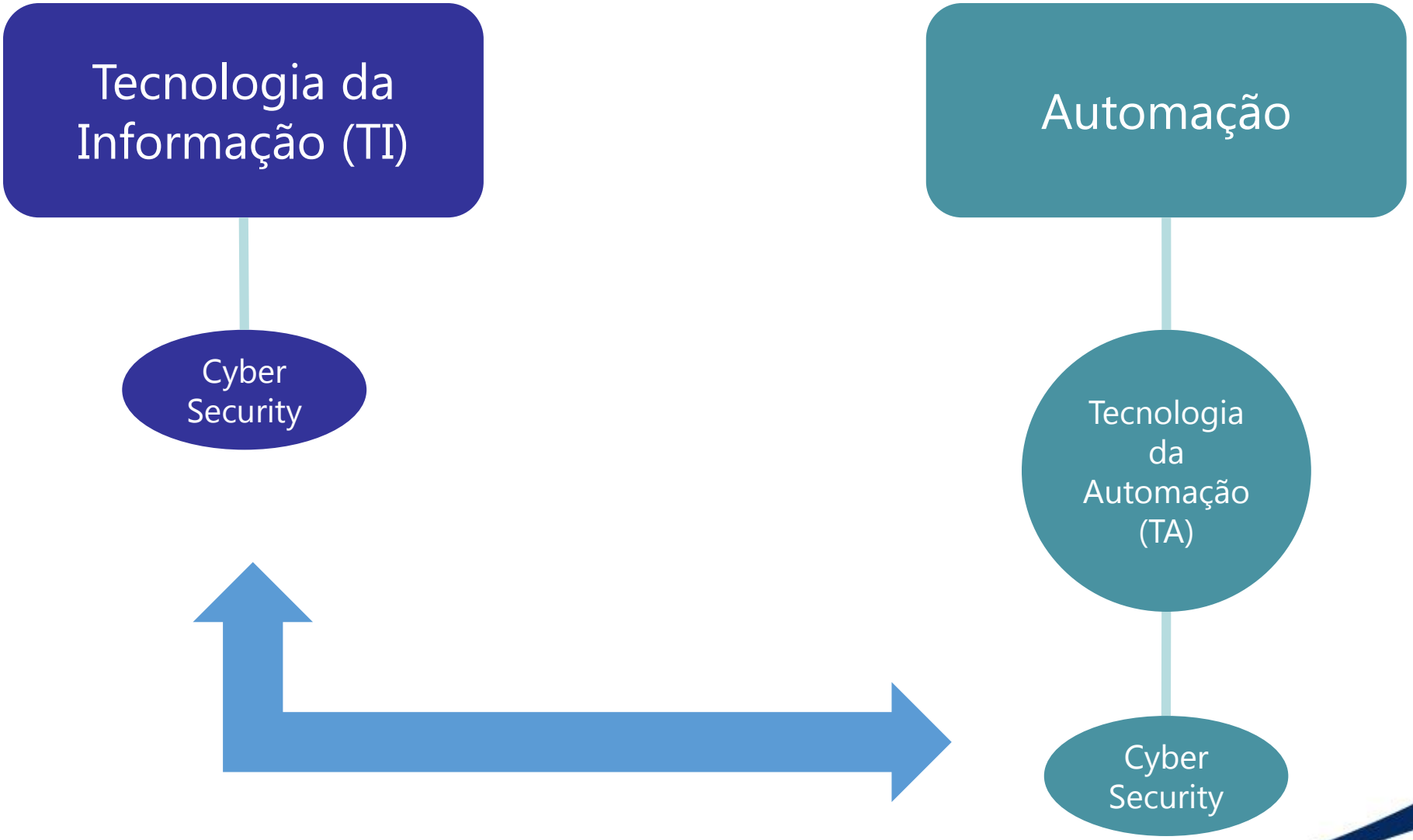
Case Braskem



Independência de:

- Ativos
- Redes
- Investimentos
- Processos
- Gestão
- Times

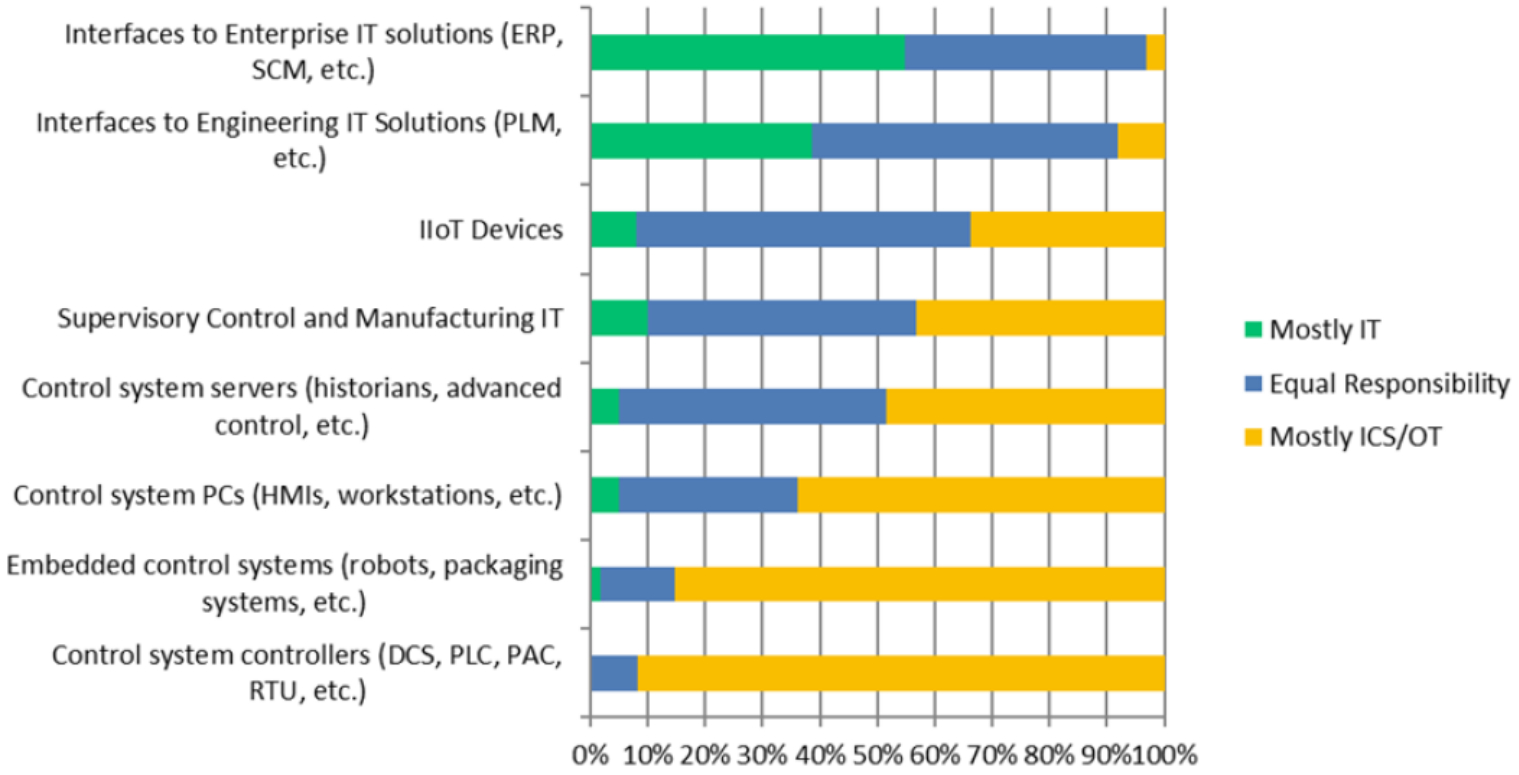
Case Braskem



BENCHMARKING

ARC 2017 INDUSTRIAL CYBER SECURITY SURVEY

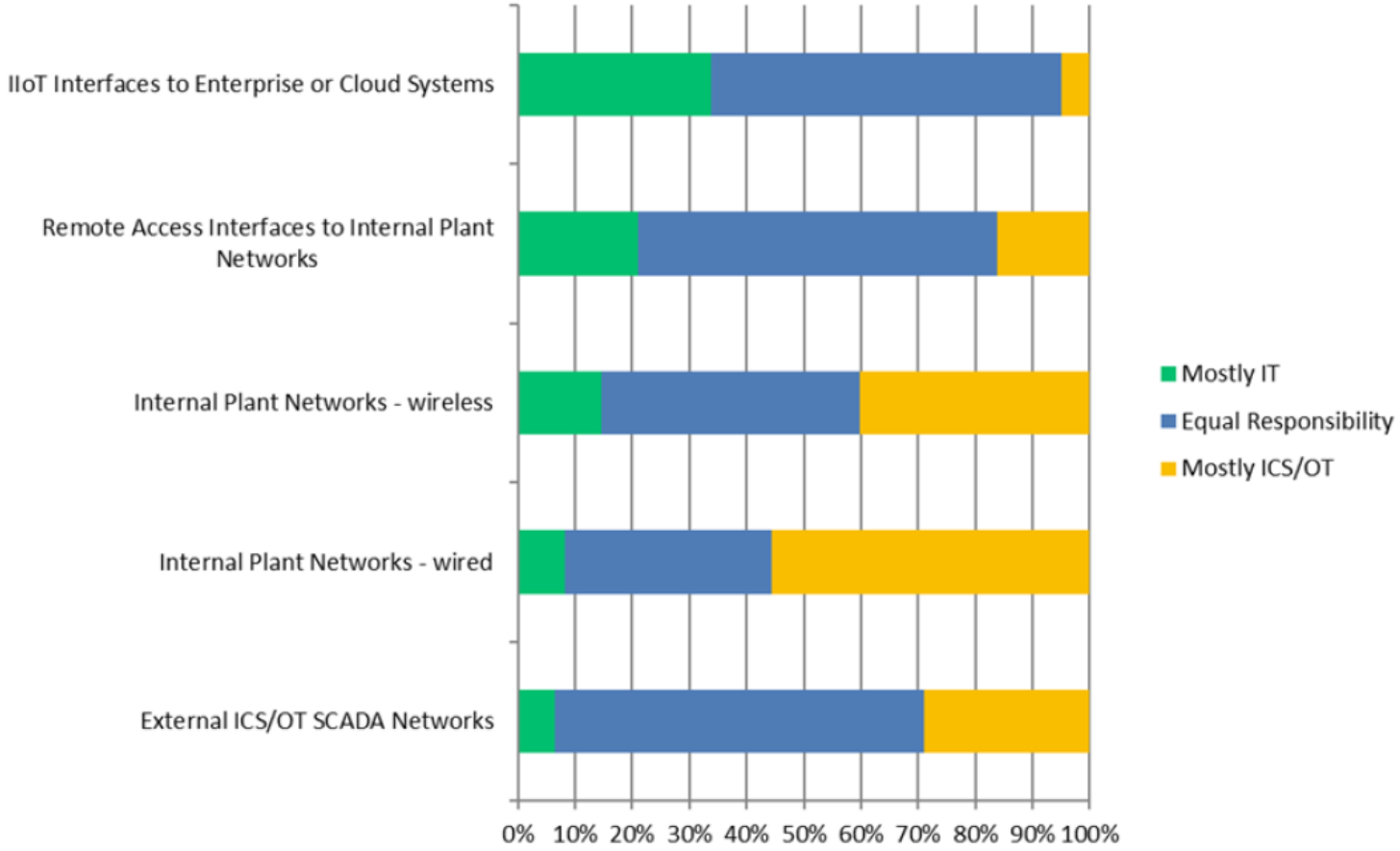
How would you assign responsibility for the cyber security of the following ICS/OT equipment, applications, and interfaces?



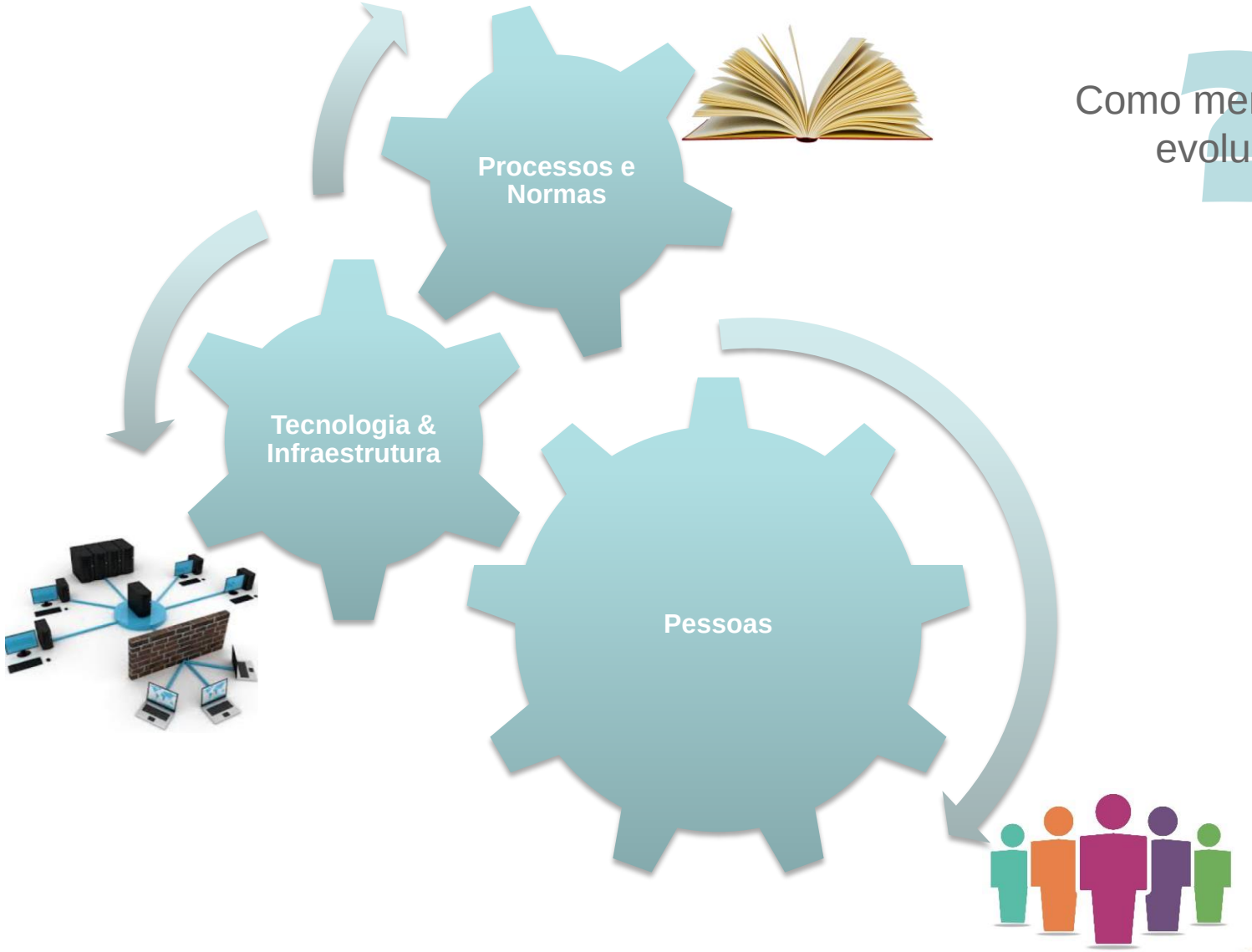
BENCHMARKING

ARC 2017 INDUSTRIAL CYBER SECURITY SURVEY

How would you assign responsibility for the cyber security of industrial networks?



Desafios



Como mensurar a evolução

Índice de Vulnerabilidade

Objetivo

Criar um instrumento de gestão para medir o nível de segurança da informação do ambiente industrial. Com ele se torna possível:

- Acompanhar a realização das metas traçadas
- Quantificar a melhoria ou piora em relação a cenários passados

Criando em 2014, o primeiro formato do indicador foi denominado Índice de Vulnerabilidade (IV) e tinha relação inversa: quanto menor, melhor.

ISO/IEC 27002

5. Políticas de segurança da informação
6. Organização da segurança da informação
7. Segurança em recursos humanos
8. Gestão de ativos
9. Controle de acesso
10. Criptografia
11. Segurança física e do ambiente
12. Segurança nas operações
13. Segurança nas comunicações
14. Aquisição, desenvolvimento e manutenção de sistemas
15. Relacionamento na cadeia de suprimento
16. Gestão de incidentes de segurança da informação
17. Aspectos da segurança da informação na gestão da continuidade do negócio
18. Conformidade

Cyber Security KPI

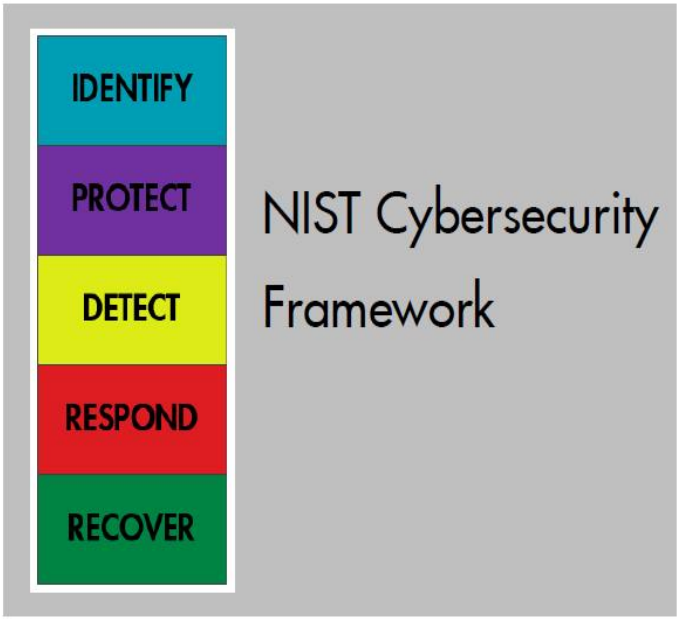
Segmentação lógica	→	13.1.3 Segregação de redes
Gestão de acesso lógico	→	6.2.2 Trabalho remoto
Acesso remoto seguro	→	9 Controle de acesso
Antivírus + Whitelist	→	12.2 Proteção contra malware
Atualizações (patches)	→	12.6 Gestão de vulnerabilidades técnicas
Backup	→	12.3 Cópias de segurança
Ciclo de vida de Hardware	→	17.1 Continuidade da segurança da informação
Ciclo de vida de Software	→	12.5 Controle de software operacional
Políticas e padrões internos	→	5 Políticas de segurança da informação
Recuperação de Desastre	→	17.1 Continuidade da segurança da informação
Gestão da Mudança	→	12.1.2 Gestão de mudanças
Segurança física	→	11 Segurança física e do ambiente
Monitoramento de Risco	→	12.4 Registros e monitoramento
Gestão de configurações	→	8.1.1 Inventário dos ativos
Gestão de capacidade	→	12.1.3 Gestão de capacidade
Gestão de inventário	→	8 Gestão de ativos

Benchmarking SHELL

Standard and Recommended Practices (Operate & Projects)

Identify	Protect	Detect	Respond
Governance ✓	Secure Architecture ✓ ■ PCD boundary and zoning ■ Remote Operations ■ Virtualisation	Malware Protection ✓	System Backups ✓
Asset Inventory ✓	Access Control ✓ ■ User Access ■ Access to safety systems ■ Device Disposal	Event Monitoring ✓	Incident Management ✓
Risk Assessment ✓	Vulnerability Management ✓ ■ System hardening ■ System patching		
Management of Change ✓	Portable Device Control		
	Awareness and Training		

- Engineering & IT work together
- Based on NIST Cybersecurity Framework and IEC Standards
- Over time, plan to further align with IEC 62443 risk based controls



✓CS KPI

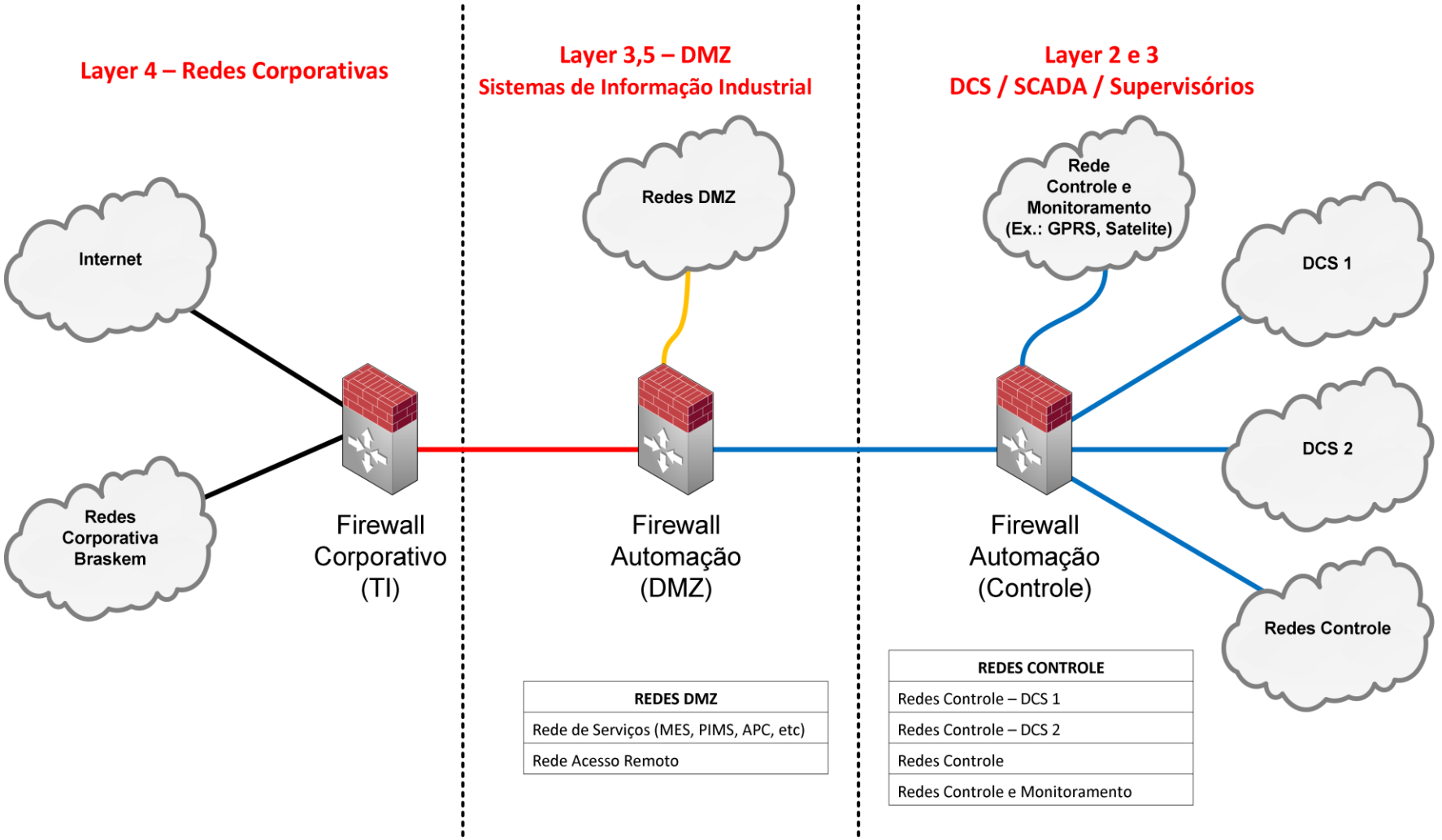
Benchmarking ARC

ARC CyberSecurity Maturity Model

✓Physical Security, ✓ Asset Inventory, ✓ Device Hardening, ✓ Pacth Mgmt	✓Unidirectional Gateways; ✓ DMZs, ✓Firewalls, ✓Anti-Malware, ✓Access Control	✓ Zone Firewalls, ✓ICS Device Firewalls, ✓ Whitelisting	✓ SIEM, ✓Incident Management	Anomaly & Breach Detection, Threat Intelligence
Secure	Defend	Contain	Manage	Anticipate
Segurança Fisica Gestão de inventário Gestão de configurações Ciclo de Vida Hardware Ciclo de Vida Software Atualizações (Patches)	Segmentação Logica Antivirus Gestão de Acesso Logico Acesso Remoto Seguro	Antivirus + Whitelisting	Monitoramento de Risco Recuperação de Desastre Backup	

✓CS KPI

Segmentação Lógica



REDES DMZ
Rede de Serviços (MES, PIMS, APC, etc)
Rede Acesso Remoto

REDES CONTROLE
Redes Controle – DCS 1
Redes Controle – DCS 2
Redes Controle
Redes Controle e Monitoramento

Gestão de Acesso Lógico

Desafios & Restrições:

- Existem sistemas de automação sem qualquer controle de acesso;
- Não há meios de controle de concessão e revogação (sem conexão com AD TI ou ferramenta própria);
- A implantação de um sistema central de autenticação pode interferir na disponibilidade do sistema;
- Sem possibilidade de autenticação integrada (rede/SO/aplicação);
- Perfis de acesso não baseados no princípio de privilégio mínimo;
- Impossibilidade de usuários individuais: limitações técnicas e operacionais (Ex.: operadores);
- Armazenamento de senhas em meios não controlados;
- Usuários e senhas fixas (padrão);
- Dificuldades de estabelecer frequência de troca de senhas;
- Baixa complexidade das senhas.

Acesso Remoto Seguro

Importância:

- Agilidade de diagnóstico e intervenção;
- Segurança pessoal dos integrantes.

Desafios: acesso remoto à sistemas de segurança/ configuração remota de parâmetros

Riscos:

- Maior risco de acesso remoto não autorizado;
- Problemas relacionados ao tráfego de dados na rede, como por exemplo, perda de pacotes que ocasionem erros ou transferências parciais de dados/comandos;
- Maior vulnerabilidade a Malwares.

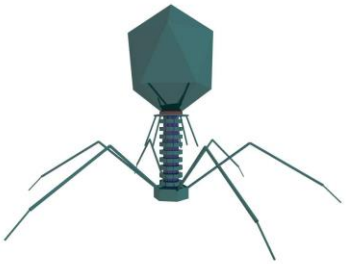
Controles:

- Configurações restritas das regras dos firewalls;
- Centralização da estrutura de acesso remoto;
- Utilização de duplo fator de autenticação.

Antivírus & Whitelisting

Desafios & Restrições:

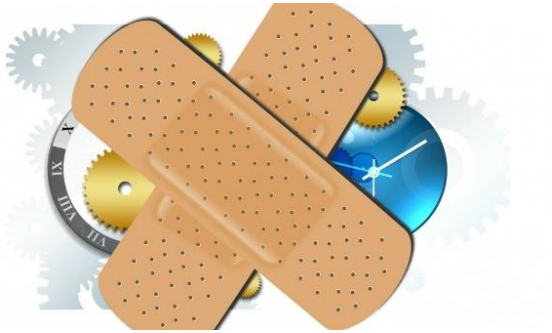
- Restrições de implantação dos sistemas (totalidade de implantação)
- Monitoramento parcial (proteção em profundidade e limitação dos sistemas)
- Homologação dos patches de atualização (periodicidade);
- Gerenciamento/ atualização manual;
- Terceirização associada às dificuldades de gestão;
- Perturbações no desempenho e/ou funcionamento dos sistemas;
- Restrição de funções;
- Manipulação por usuários administradores;
- Equipamentos isolados;
- Histórico de código malicioso disponibilizado no repositório do fornecedor;
- Na ocorrência de infeção até o processo de remoção pode afetar a produção da planta;
- Extensa fase de testes (Whitelisting).



Atualizações (patches)

Desafios & Restrições:

- Sistemas operacionais obsoletos;
- Restrições das ferramentas;
- Homologação dos patches de atualização (periodicidade);
- Gerenciamento/ atualização manual;
- Terceirização associada às dificuldades de gestão;
- Negociação de janela de parada;
- Perturbações no desempenho e/ou funcionamento dos sistemas;
- Equipamentos isolados.



Backup

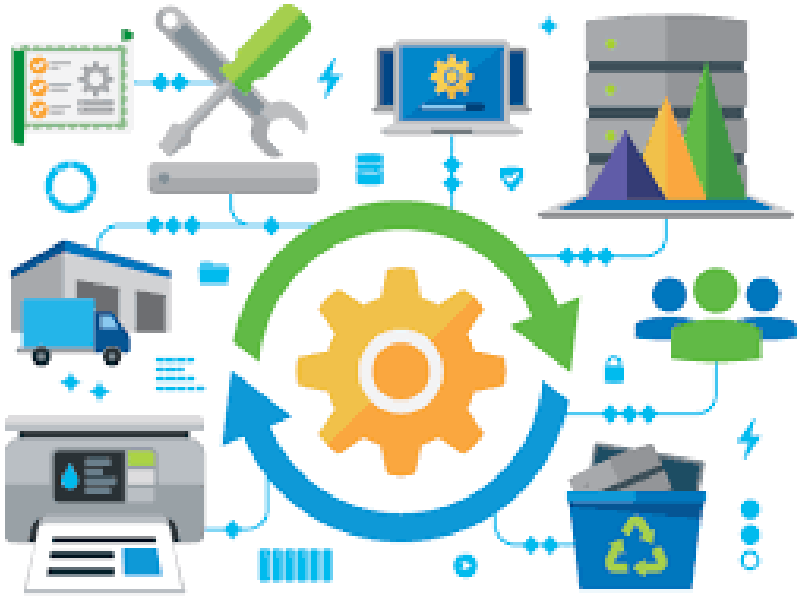
Desafios & Restrições:

- Comprometimento do tráfego de informações entre sistemas na rede;
- Armazenamento das informações em local seguro;
- Gerenciamento/ realização manual;
- Terceirização associada às dificuldades de gestão;
- Perturbações no desempenho e/ou funcionamento dos sistemas;
- Equipamentos isolados;
- Volumetria de dados e definição do tempo de retenção;
- Descarte;
- Verificação e testes.

Ciclo de vida de Hardware & Software

Desafios & Restrições:

- O tempo do ciclo de vida de sistemas de automação é muito diferente dos seus recursos computacionais;
- Há uma completa dependência dos fornecedores;
- As substituições/ migrações muitas vezes depende de paradas de manutenção programadas;
- Os investimentos requeridos são muito maiores;
- Com relação aos softwares existe o desafio do controle de licenciamento.



Políticas e Padrões Internos

Desafios & Restrições:

- Quantidade e diferenças entre sistemas;
- Divergências operacionais entre sistemas;
- Gestão descentralizada;
- Requisitos dos fornecedores.

Recuperação de Desastre

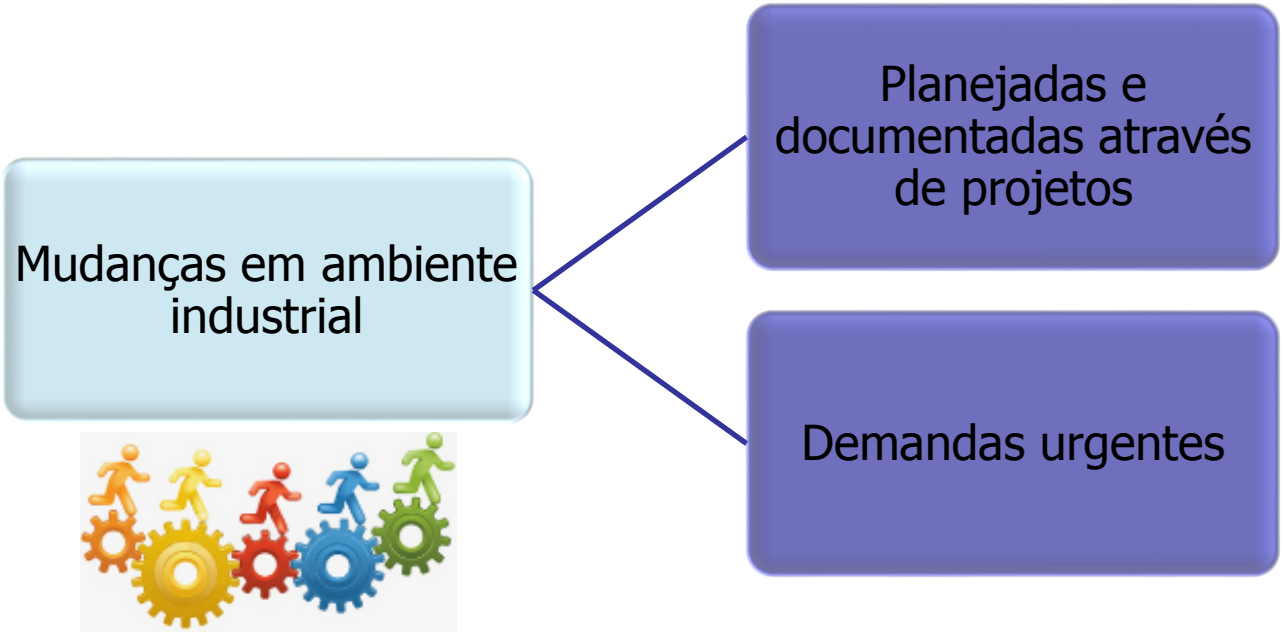
DRP1

DRP2

DRP3

DRP4

Gestão da Mudança, Inventário e Configuração



- Requisitos de disponibilidade e criticidade da área industrial não propiciam o registro formal das requisições, não existe uma cultura abertura de chamados para a realização de alterações emergenciais, diferentemente de mudanças de processos;
- A carência de ferramentas específicas para o ambiente industrial demanda adaptações;

Segurança Física

Desafios & Restrições:

- Os sistemas surgiram de forma espontânea nas plantas industrias e se expandiram em espaços não planejados e previamente compartilhados;
- Existem dispositivos distribuídos na área industrial e é muito difícil restringir o acesso;
- A cultura de manutenção cria algumas vulnerabilidades como por exemplo, diagramas esquemáticos de painéis armazenados em painéis abertos.

Monitoramento de Risco

Desafios & Restrições:

- A proteção em profundidade e o isolamento das redes ainda são fatores que dificultam o monitoramento;
- A deficiência deste monitoramento compromete os pilares da antecipação e da prevenção contra as ameaças;
- Ferramentas desenvolvidas para o ambiente de TI, começam a surgir opções específicas para a área industrial com elevado custo e funcionalidades parciais;
- Intrusão;
- Falsos positivos.

❖ Como podemos prover monitoramento contínuo dos processos industriais sem possuir monitoramento contínuo dos nossos próprios sistemas e infraestrutura?

Perspectivas Futuras

Renata Valente de Araújo
renata.araujo@braskem.com

Muito Obrigada!