Encontro Técnico: Automação na Rede Aérea de Distribuição de Energia

Sede da AES Brasil, Barueri – SP
10 de outubro, 8h às 13h50

AES Eletropaulo
por onde a vida acontece

ISA Sao Paulo Section

Segurança Cibernética Industrial em Redes de Comunicação de Sistemas de Automação de Subestações (SAS)

BELDEN
SENDING ALL THE RIGHT SIGNALS

Segurança Cibernética Industrial em Redes de Comunicação de Sistemas de Automação de Subestações (SAS)

Leandro Pires
Gerente de Produto - LATAM

Guilherme Normanton
Engenheiro de Produto - LATAM

Encontro Técnico:
Automação na Rede Aérea de Distribuição de Energia

ISA Sao Paulo Section

AES Eletropaulo
por onde a vida acontece

BELDEN
SENDING ALL THE RIGHT SIGNALS

Agenda

- Requisitos e tendências para comunicações de dados em SAS

- Como implementar Cyber Security em uma Subestação Elétrica: Estratégia ‘Defense in Depth’

Requisitos e tendências para comunicações de dados em SAS

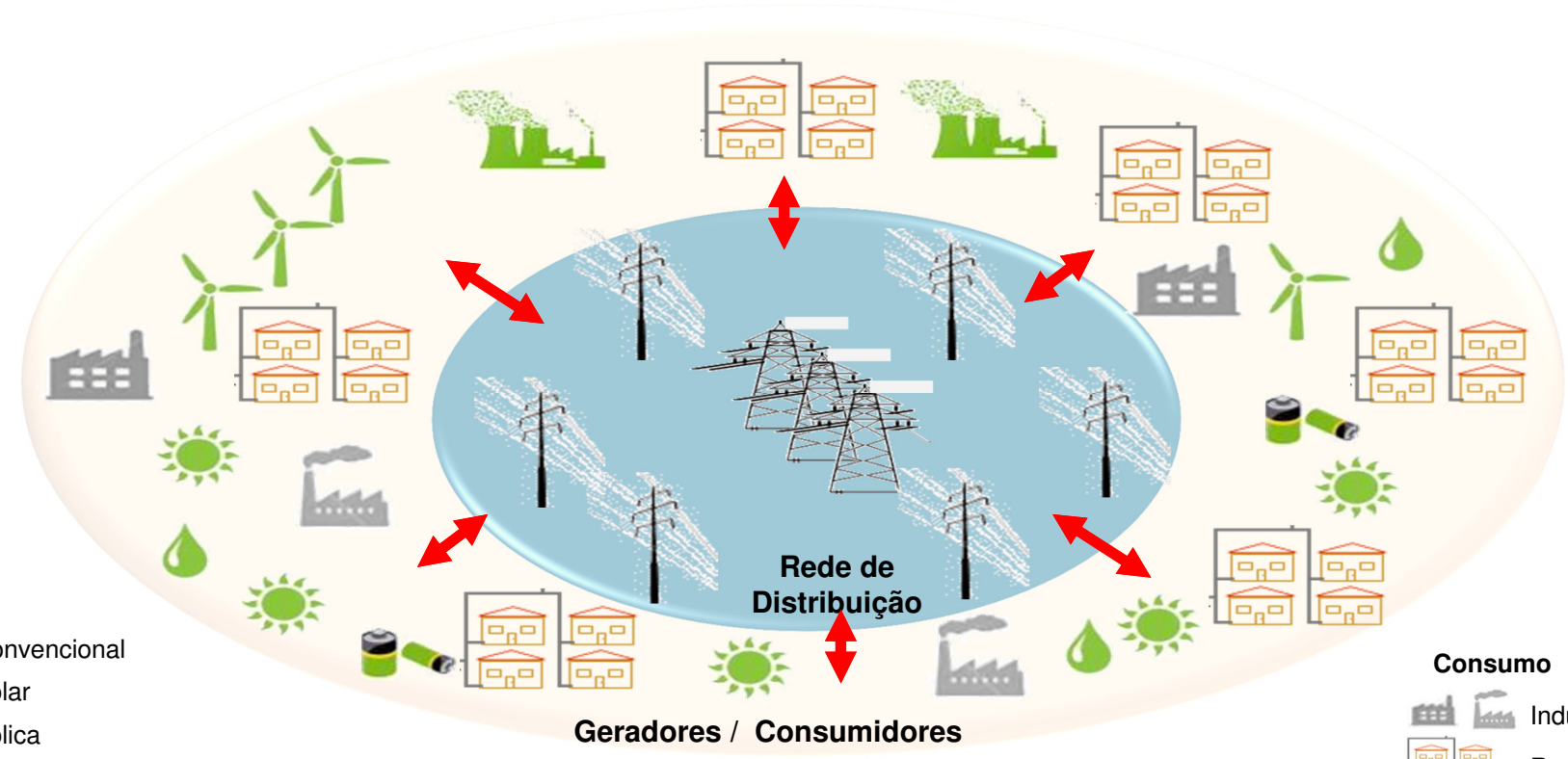
Encontro Técnico:
Automação na Rede Aérea de Distribuição de Energia

ISA Sao Paulo Section

AES Eletropaulo
por onde a vida acontece

BELDEN
SENDING ALL THE RIGHT SIGNALS

Distribuição de Energia – Projeção Futura



Geração

- Convencional
- Solar
- Eólica
- Célula Combustível

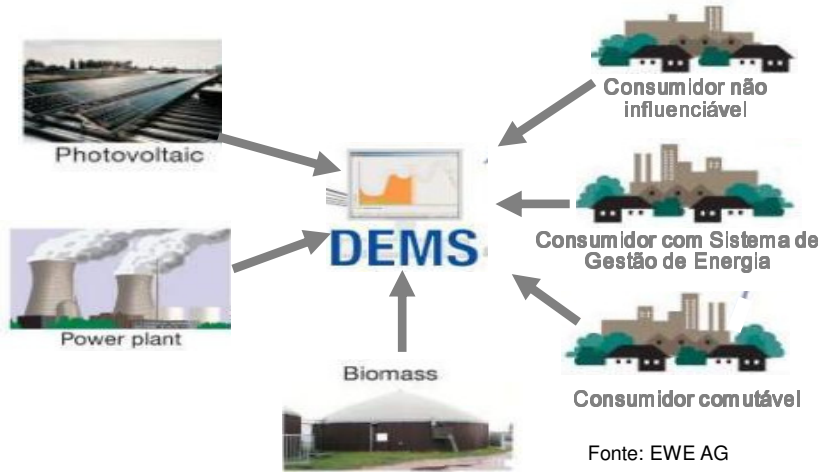
Consumo

- Industrial
- Residencial

Geração Descentralizada de Energia e Smart Grid

Geração de energia descentralizada está aumentando constantemente(Fotovoltaica, Energia Eólica, Célula Combustível, Biomassa, Hidrelétrica)

As grandes oscilações na energia produzida geram a necessidade de um Sistema Descentralizado de Gestão de Energia ("**D**ecentralize **E**nergy **M**anagement **S**ystem") para equilibrar a oferta e a procura em tempo real = SMART GRID



Fonte: EWE AG

TI e comunicação são necessários

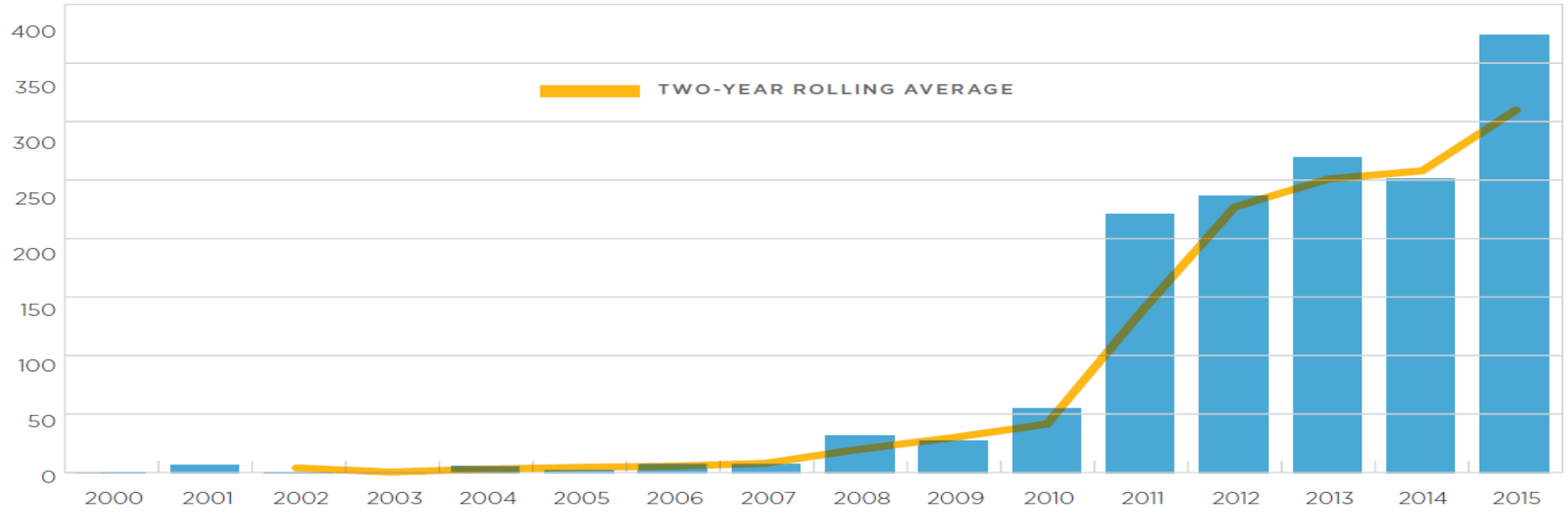
Objetivos do Projeto de Rede de uma Subestação

1. **Integração da Rede**
   - Reduzir custos através da consolidação da rede
   - Tornar mais fácil a adição de novas aplicações
   - Gerenciar a transição de tecnologias antigas para novas
2. **Confiabilidade da Rede**
   - Maximizar a disponibilidade da rede
   - Reduzir os custos de falhas, recuperação e reparação
3. **Segurança da Rede**
   - Cumprir com os requisitos e normas industriais
   - Aumentar a confiabilidade

Projetos de Rede estão (devem estar) estritamente relacionados à SEGURANÇA CIBERNÉTICA

Violações na Segurança Cibernética Industrial

ICS- Divulgação de vulnerabilidades específicas por ano



Ataques à segurança cibernética dentro do ambiente industrial estão crescendo exponencialmente

1. *"Overload: Critical Lessons From 15 years of ICS Vulnerabilities", FireEye iSight Intelligence*

Sistema de Automação de Subestações (SAS)

A automação de subestações modernas está estruturada em três níveis básicos:

Station

- **Station Level:** fornece uma visão geral em toda a subestação e está localizado em geral em uma sala de controle. Inclui IHMs, Estações de Engenharia e Operação, Servidores master e backup, receptores GPS, etc.

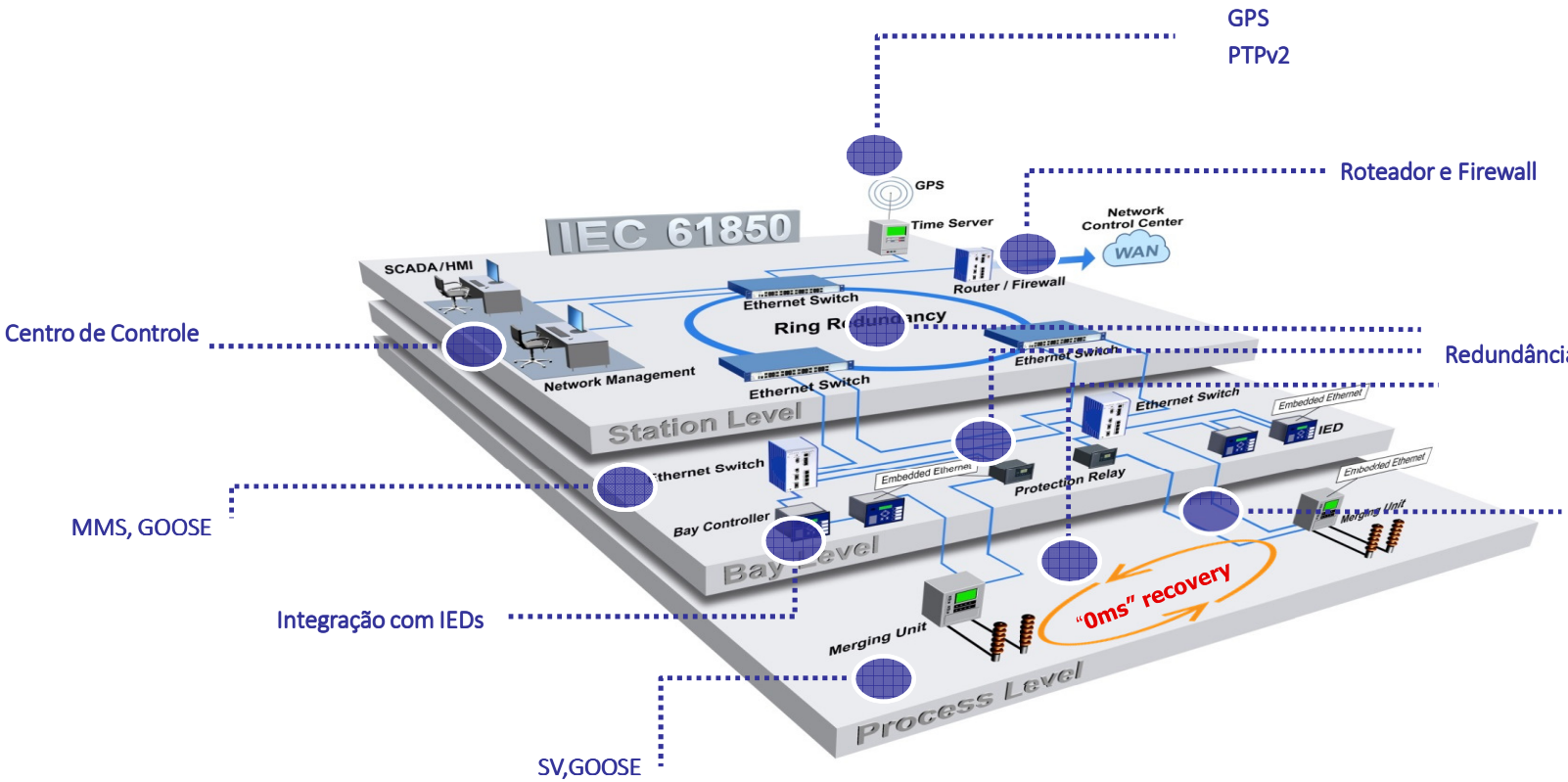
Bay

- **Bay Level:** onde são realizados os trabalhos de manutenção dentro dos vãos. Normalmente estão perto dos equipamentos de proteção elétrica. Inclui IEDs de Proteção e Controle para diferentes equipamentos como disjuntores, transformadores e bancos de capacitores. Equipamentos nesse nível são chamados de equipamentos secundários.

Process

- **Process Level:** fornece a interface entre o SAS e os equipamentos de proteção elétrica. O nível de processo inclui equipamentos primários como: TCs / TPs, remotas I/O, atuadores, “merging units” etc.

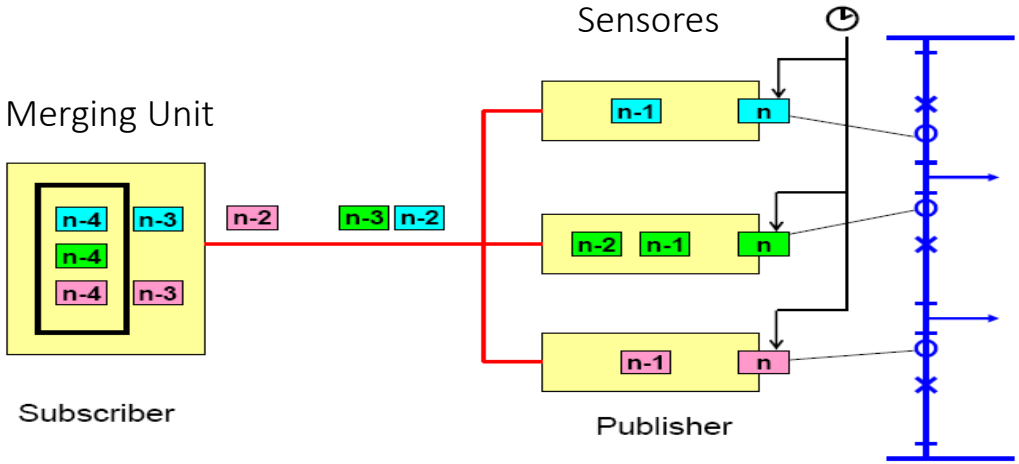
Subestação IEC 61850



IEEE1588 Sincronismo de Tempo – PTPv2

Dado de sensores: „Sampled Values“

Sincronização usando IEEE1588



Merging Unit:

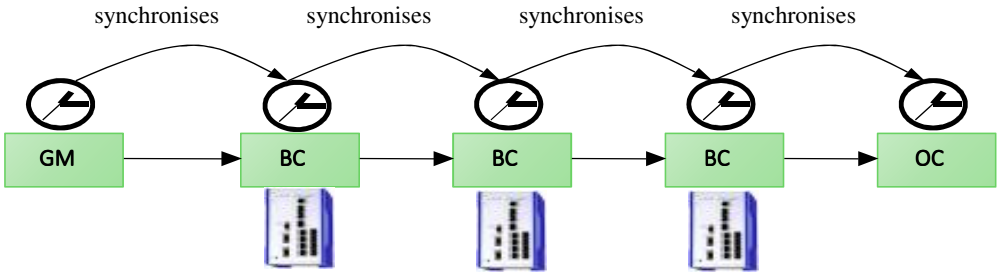
- Amostragem (coerente em tempo) de corrente, fases e valores de tensão para fornecer saídas digitais (IEC 61850-9-2)
- Precisam ser altamente sincronizados para a correta operação de funções de proteção

Fonte: UTInnovation & NettedAutomation

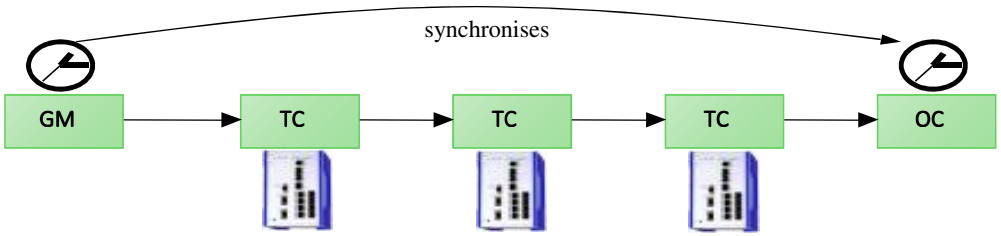
‘TIME CRITICAL application’ também em relação à SEGURANÇA CIBERNÉTICA

IEEE1588 Sincronismo de Tempo – PTPv2

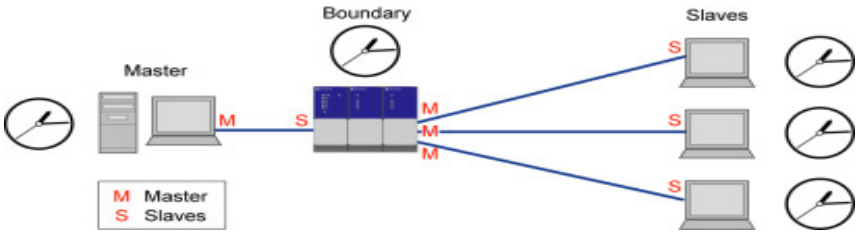
cascaded boundary clocks



cascaded transparent clocks



Fonte: UTInnovation & NettedAutomation



BC: sincronização ponto a ponto, cascateamento de loops de controle

TC: corrige apenas o "tempo de residência", é transparente para os "end devices"(Grandmaster, Master, Ordinary Clock)

O TC causa menos instabilidade em uma grande cascateamento na rede

Topologias de Rede – IEC 61850

A norma descreve diversas topologias:

"Essas referências de topologias foram escolhidas baseadas em práticas comuns em SAS desde pequenos sistemas de distribuição a grandes subestações com múltiplos níveis de tensão. Elas são representativas dos diversos problemas de rede descritos neste documento.

Não existe uma 'melhor' topologia de rede nem 'melhor' protocolo de redundância.

Todos possuem seus pontos fracos e fortes e a ***escolha correta para uma determinada aplicação depende de vários fatores.***"

Fonte: IEC61850 Network Engineering Guideline

Nas orientações, estão inclusas:

Topologias

Estrela, Anel / Anéis Múltiplos e redes duplas. Não há recomendação clara mas há uma tendência a topologias de anel.

Tecnologias de Redundância

RSTP – IEC 62439-1, PRP, HSR

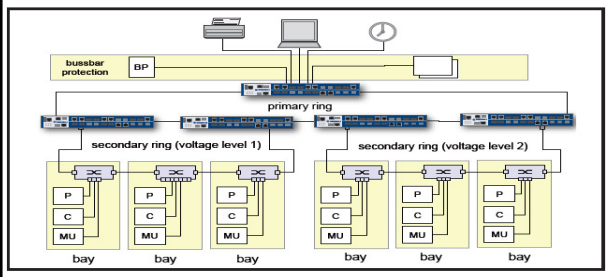
- Cada rede de comunicação é construída com uma topologia diferente.

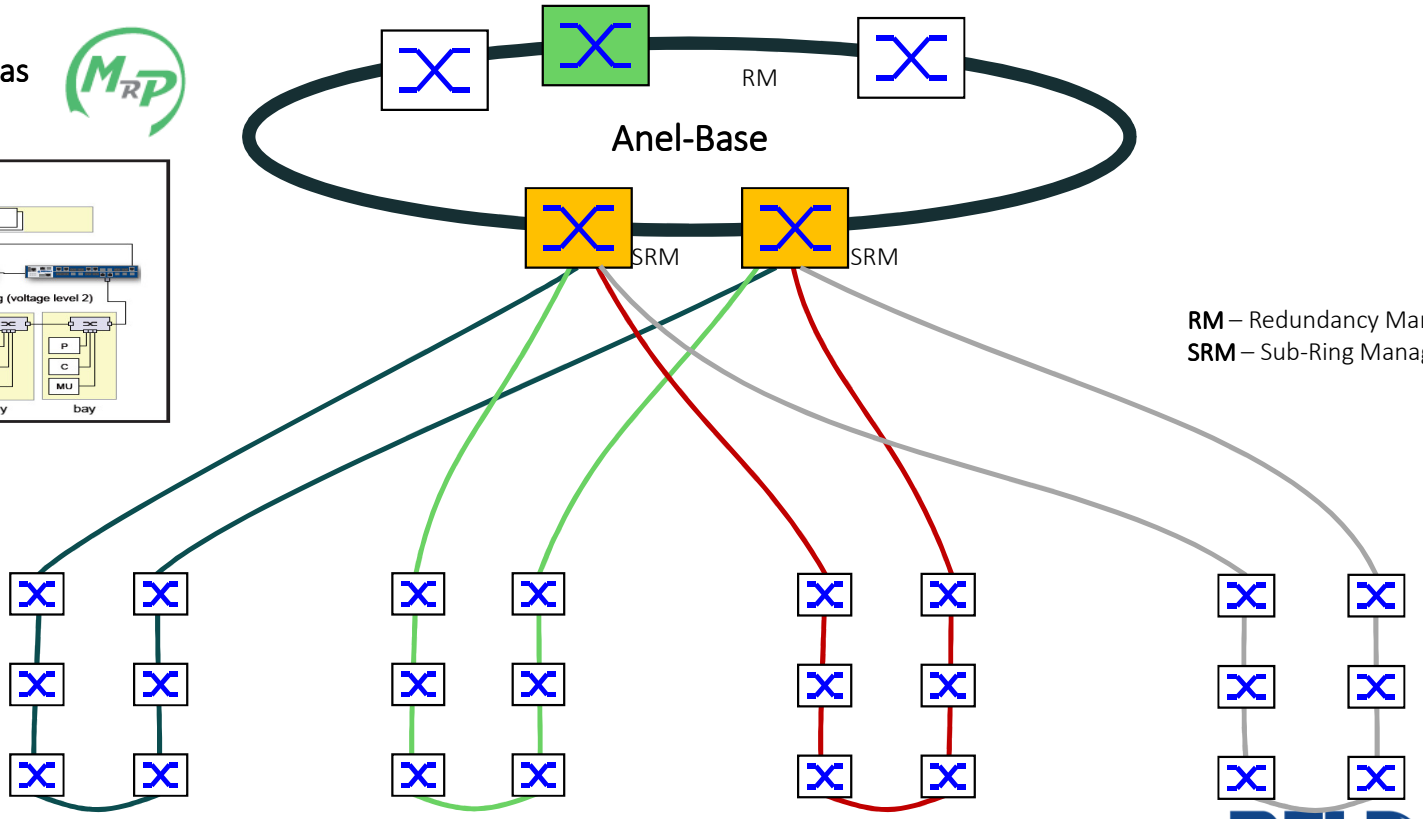
A topologia de rede é separada nos diferentes níveis da Subestação por razões de SEGURANÇA e DISPONIBILIDADE.

Topologia de Múltiplos Anéis

A norma IEC61850 define apenas o RSTP

→ MRP + SRM são tecnologias mais rápidas e confiáveis





RM – Redundancy Manager
SRM – Sub-Ring Manager

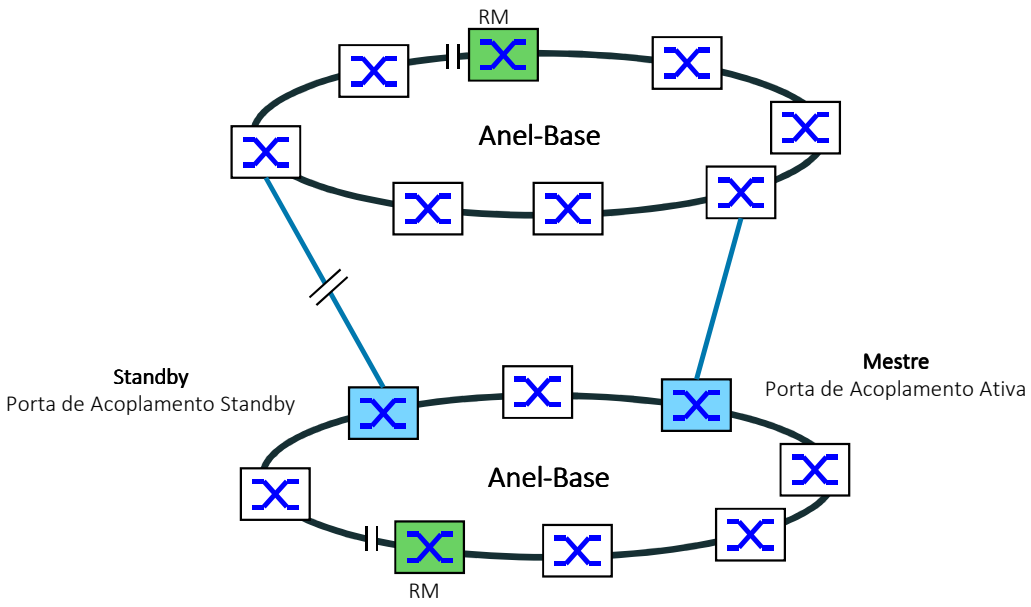
Topologia de Múltiplos Anéis

Conexão redundante de
múltiplos anéis ou redes

- Permite o acoplamento redundante de anéis e segmentos de rede.
- Dois anéis ou segmentos de rede (ou várias combinações de ambos) são ligados através de dois caminhos separados.

Protocolos de Redundância:

- Nos Anéis-Base: qualquer protocolo de anel (RSTP, MRP, HSR)
- Protocolo para acoplamento redundante



Como implementar Cyber Security em um SAS: Estratégia ‘Defense in Depth’

Encontro Técnico:
Automação na Rede Aérea de Distribuição de Energia

ISA Sao Paulo Section

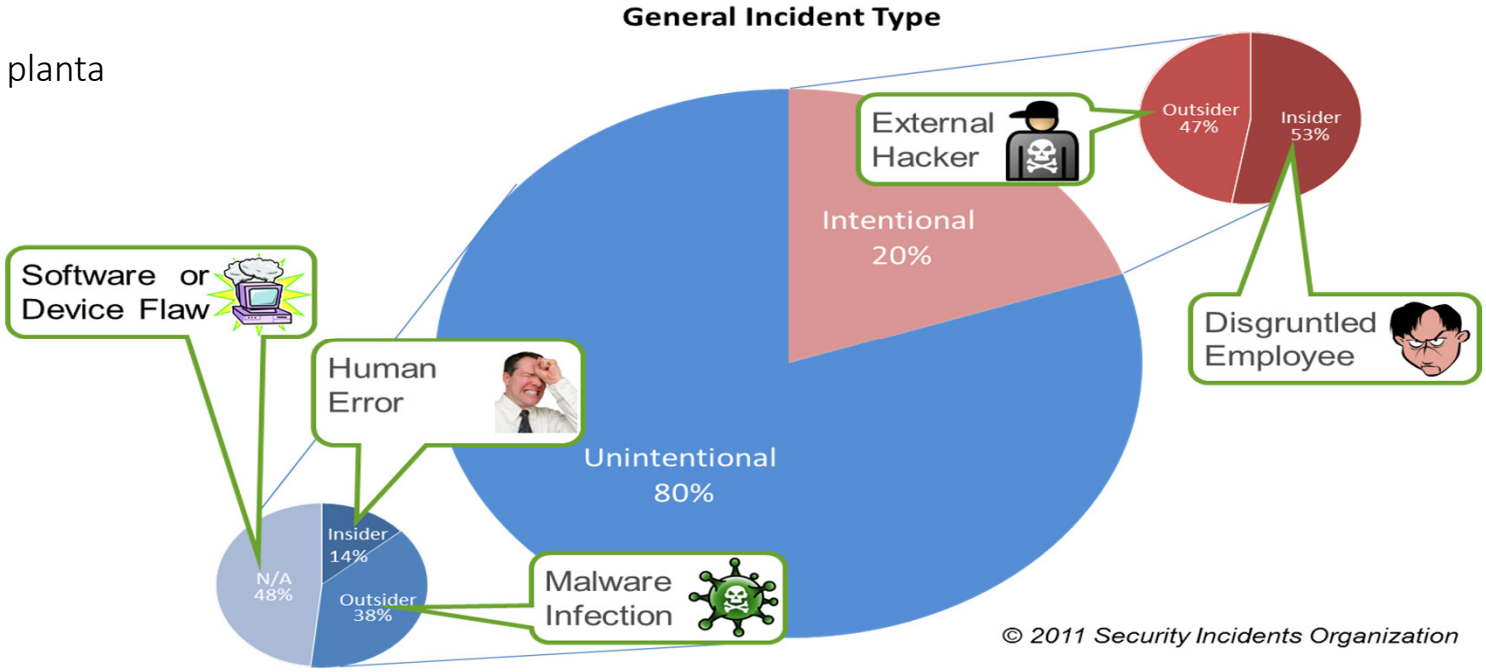
AES Eletropaulo
por onde a vida acontece

BELDEN
SENDING ALL THE RIGHT SIGNALS

Objetivo da Segurança Cibernética

O foco de **Segurança Cibernética** é manter o seu sistema seguro e em operação!

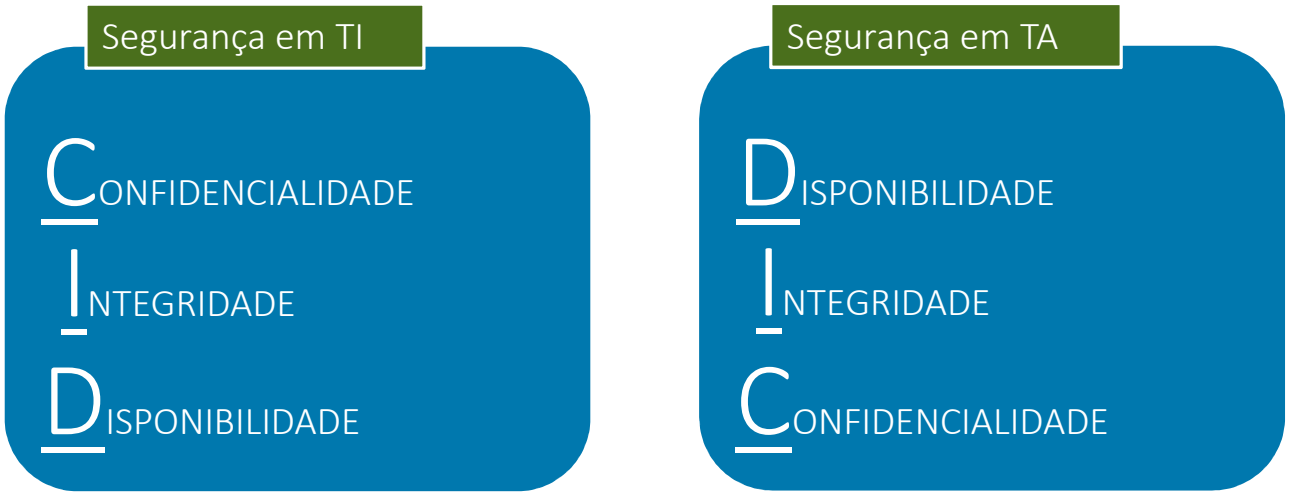
- Reduzir o tempo de parada da planta
- Aumentar a produtividade
- Reduzir custos operacionais
- Garantir **segurança**



TI e TA: Diferentes objetivos e prioridades de Segurança

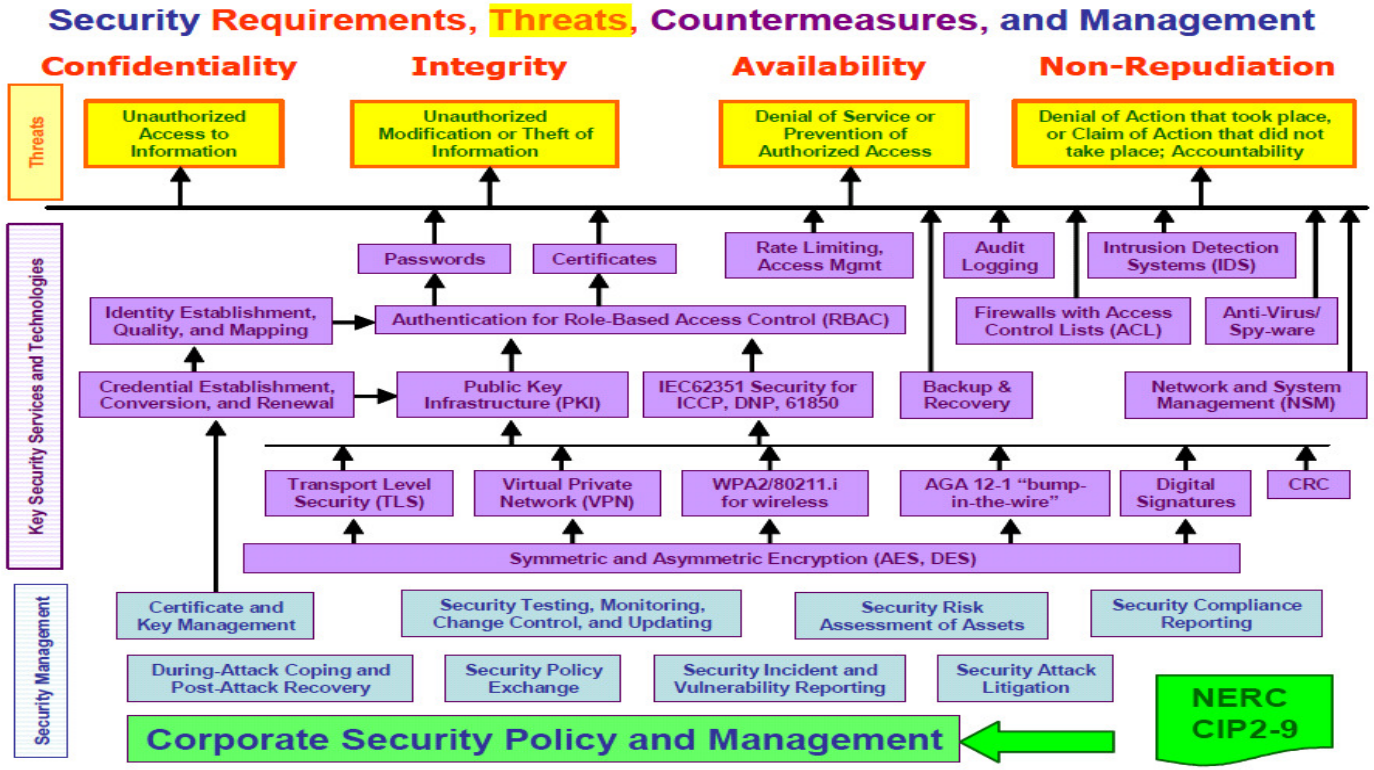
TI: Proteger informações críticas ao negócio

TA: Proteger recursos críticos à segurança e à produtividade



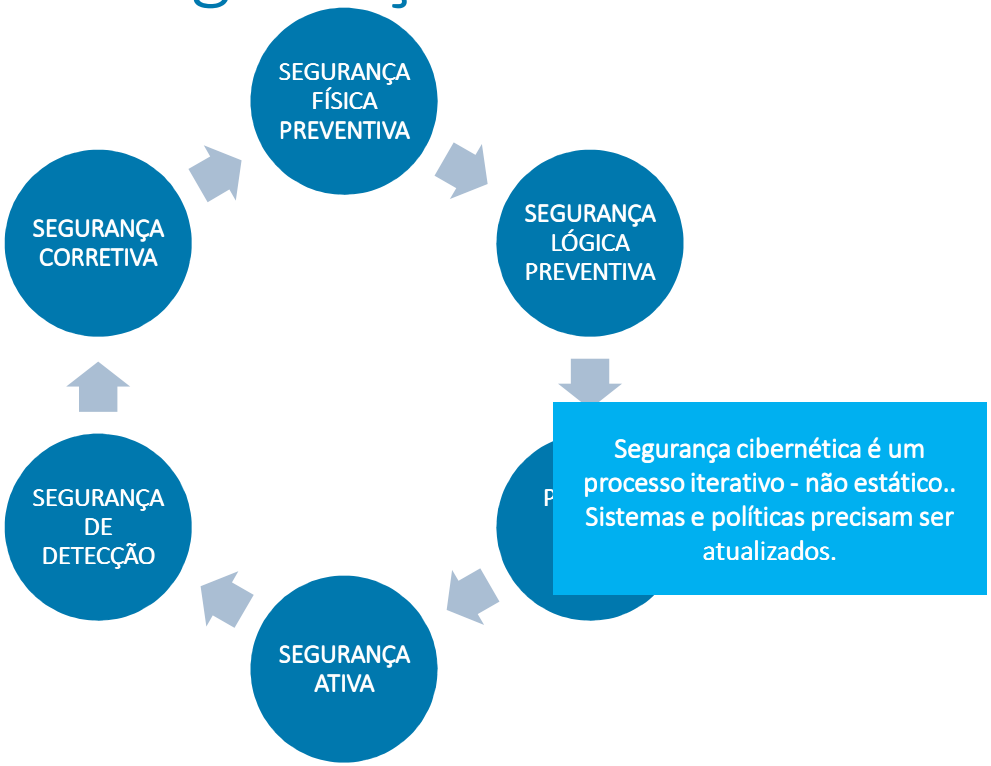
Segurança Cibernética: Modelo de Segurança IEC 62351

IEC 62351:
Gestão dos sistemas de potência e da troca de informações associoadas – Segurança de Comunicação e Dados



A Belden adota os requisitos de segurança cibernética da IEC 62351 (entre outras).
Em todos os novos produtos estes requisitos são considerados caso sejam aplicáveis

Ciclo de Segurança de Redes



Segurança cibernética é um processo iterativo - não estático.. Sistemas e políticas precisam ser atualizados.

Segurança de Redes

Segurança Preventiva - Física	Proteção Física Perimetral Gabinetes Seguros Inexistência de drives externos ou portas disponíveis em PCs na Rede de Operação Evite etiquetas com informações sobre senhas ou MAC / endereço IP / máscaras
Segurança Preventiva - Lógica	Desativar portas console após o comissionamento Política de senhas (evitar senhas fracas, obrigar alteração de senhas padrão) Utilização de servidores Radius, Tacacs+ Informações limitadas no “Hello Banner” Limitação nas tentativas de acesso Configurar usuários com diferentes níveis de acesso Limite de tráfego por porta Bloquear portas não utilizadas Bloquear Telnet, HTTP, e permitir HTTPS e SSH Política para Backup de arquivos de configuração “Port Security” (por endereços IP)

Segurança de Redes

Segurança no Projeto de Rede	Estabelecer fisicamente os “Conduites” (limitar o número de conexão entre “Zonas”) Filtro por endereço MAC MAB: “MAC Authorization Bypass” para equipamentos sem 802.1x Apenas SNMPv3 por conta da encriptação Uso de MMS(menos comum) e apenas um sistema de gestão Estabelecer processos e políticas de Registro de Logs-Alarmes-Ações FW – Segmentação DMZ Deferentes Subredes (IP) Segmentação por VLAN’s 802.1Q e “QinQ” NAT 1:1 e 1:N VPN Usar SFTP ao invés de FTP

Segurança de Redes

Segurança Ativa	Uso de “ACL’s” Firewall Layer 3 (Filtro de IP, Stateful Inspection, Aplicação) “Dynamic ARP Inspection” Encriptação (SSH/SSL 128bit Encryption) VPN Filtro de porta de destino (TCP/UDP) DPI (Deep Packet Inspection) para protocolo específico Antivirus (Spyware, Malware, Trojans…)
Segurança de Detecção	Análise de Logs Monitoramento (IDS, traps pelo “NMS”…)
Segurança Corretiva	Política de backup de configurações Update de Firewalls Update de Antivirus

Outras recursos de segurança de Switches de alta performance

- Procedimento de start-up
  fácil, seguro e rápido

- Operação Segura
  Proteção contra erros de configuração, estatus de segurança, “impressão digitar” do arquivo de configuração, gerenciamento de certificados HTTPS …

- Manutenção
  Manutenção preditiva, substituição rápida (MTTR), versão backup de software, notificação por email…

- “Troubleshooting”
  Testador de cabos, verificador de configurações “built-in”, “Remote Switched Port Analyzer” (RSPAN)

Problemas de Segurança em Redes Industriais

Cenário

Computadores operando 24x7 sem atualizações de segurança ou mesmo anti-vírus

Controladores são otimizados para trabalharem em tempo real, não para conexões de rede robustas

Múltiplos Pontos de Entrada para a Rede

A maioria dos incidentes com segurança cibernética são originários de pontos de entrada secundários da rede

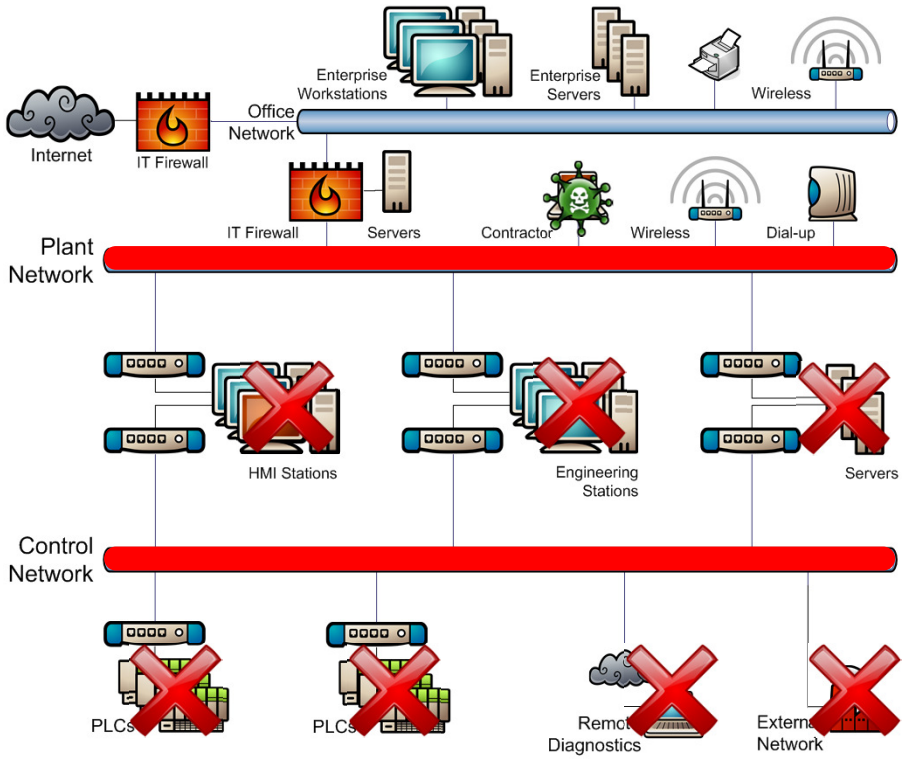
USBs não verificadas, equipe de manutenção terceirizada, laptops não verificados, etc.

Pobre Segmentação de Rede

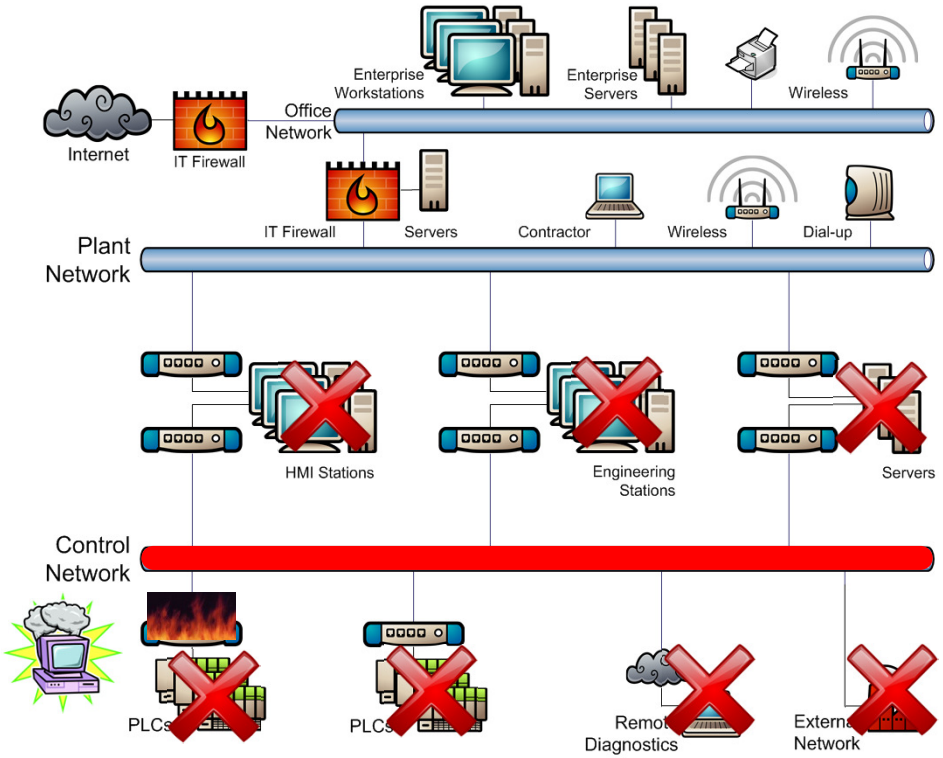
Muitas redes de controle são "totalmente abertas", sem isolamento entre seus diferentes sub-sistemas (sub-redes)

Como resultado os problemas espalham-se rapidamente através da rede

Estamos realmente seguros com um Firewall?



Estamos realmente seguros com um Firewall?



A Defesa “Perimetral” não é suficiente

Não podemos apenas instalar um “firewall” na ponta da rede e esquecermos de outros detalhes de segurança.

- Acessos não autorizados poderão eventualmente ocorrer
- Muitos problemas se originam de DENTRO da rede

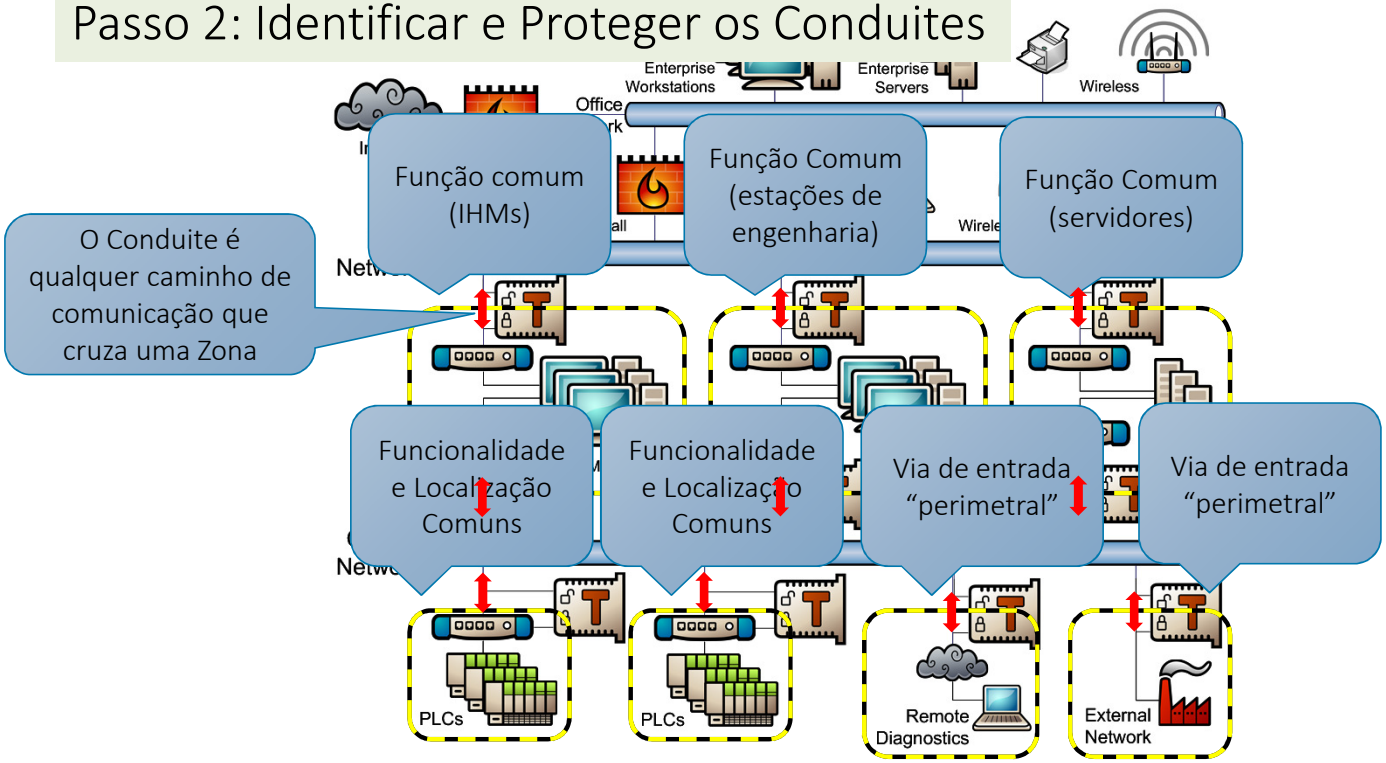
Precisamos do conceito “Defense in Depth”:

- Identificar as ‘Zonas’ e ‘Conduites’ na rede conforme definido na norma ISA99
- Permitir somente o tráfego de dados necessários entre as Zonas da rede
- Gerar alarmes quando algum tráfego é bloqueado

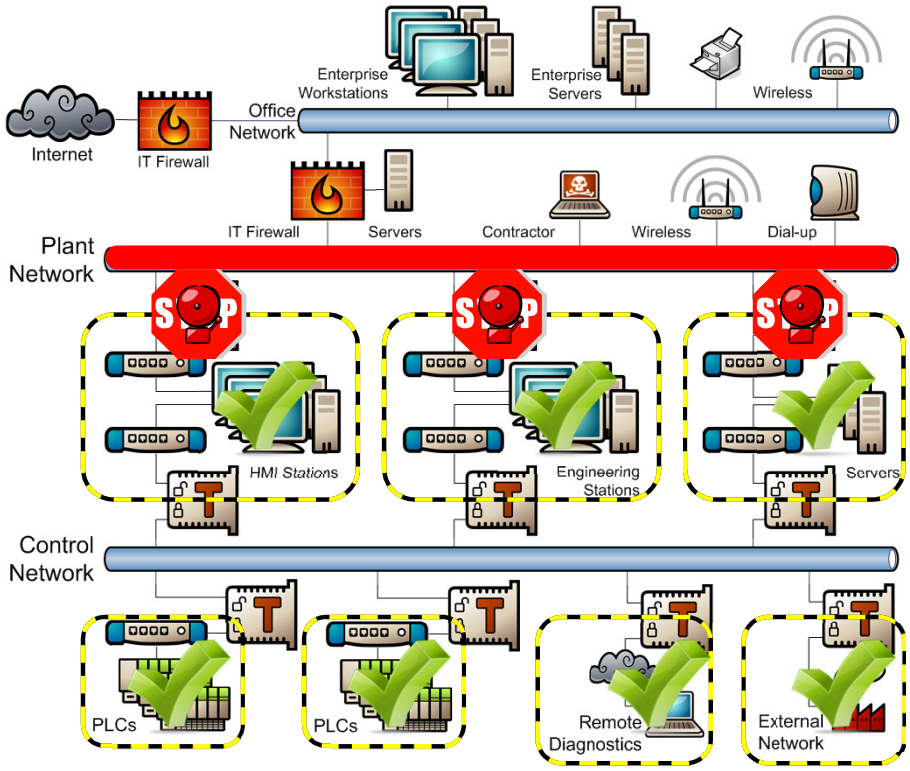
ISO/ISA 62443: Zonas e Conduites - Defense in Depth

Passo 1: Identificar Zonas de Segurança baseado na funcionalidade

Passo 2: Identificar e Proteger os Conduites



ISO/ISA 62443: Zonas e Conduites - Defense in Depth

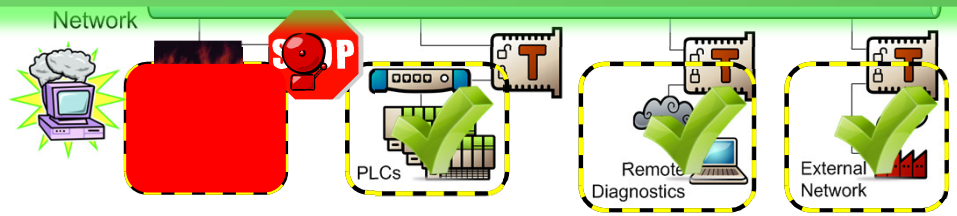


ISO/ISA 62443: Zonas e Conduites - Defense in Depth

"Defense in Depth" é uma estratégia que FUNCIONA

As Soluções Belden facilitam esta implementação

Firewalls Industriais para proteger as zonas (SPI e DPI)
Switches industriais com segurança interna (built-in)
Sistema de gerenciamento (SNMP) para identificar riscos e manter a rede



Por que ainda temos problemas?

Os engenheiros de TI lidam satisfatoriamente contra as ameaças de segurança cibernética há anos.

Por que não aplicar as mesmas soluções na Rede de Controle e SCADA?

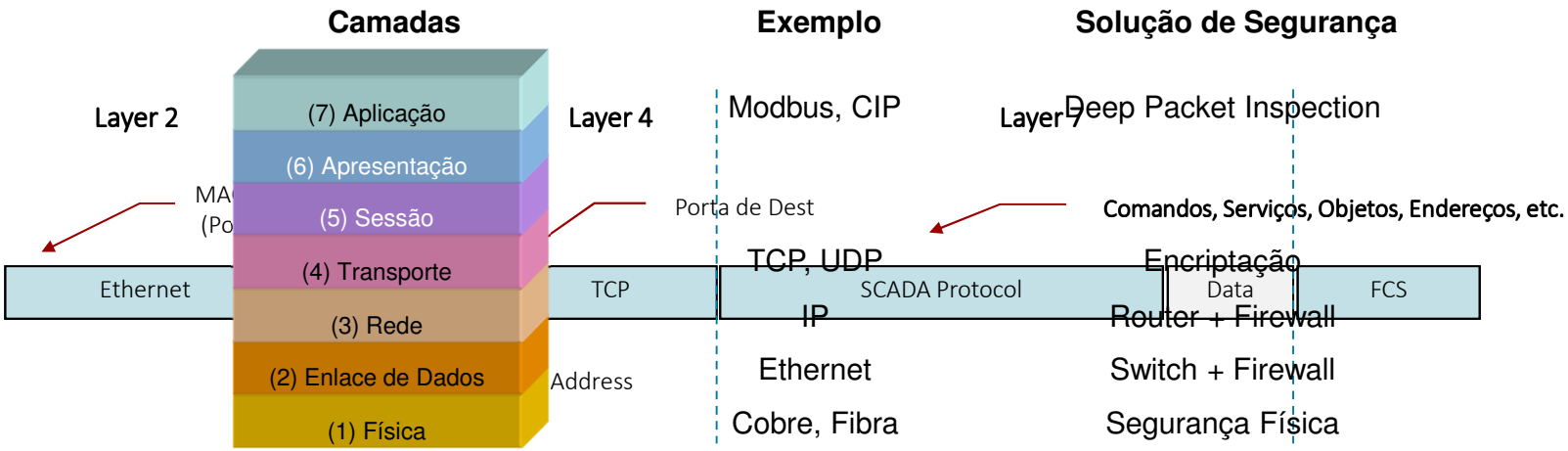
Soluções de Segurança devem ser especialmente adaptadas para o ambiente industrial:

- Suportar sistemas SCADA e protocolos industriais (MMS, GOOSE, MODBUS, DNP3, etc.)
- Realizar configuração, teste e manutenção sem interromper o funcionamento da rede
- Hardware construído para sobreviver à condições elétricas e ambientais adversas
- Longo ciclo de vida (décadas para sistemas de controle vs anos para IT)
- Reduzida complexidade para evitar o risco de erro humano
- Interface de Configuração amigável dedicada a Engenheiros de Automação

Segurança Cibernética e DPI

Segurança Cibernética

"Uma coleção de medidas adotadas para prevenir a utilização não autorizada, utilização maliciosa, bloqueio do uso ou modificação de informações, fatos, dados ou recursos ...."



Deep Packet Inspection (DPI)

Wikipedia:

- "Deep Packet Inspection" (DPI) é uma forma de filtragem de pacotes de rede que analisa a parte de dados de um pacote que passa por um ponto de inspeção em busca de inconformidade no protocolo, vírus, spam, invasões ou critérios customizados para escolher se o pacote pode passar"

Em outras Palavras:

- Um firewall permite verificar **quais dispositivos estão autorizados a falar uns com os outros** (endereços IP) e **que tipo de serviço(s) eles estão autorizados a acessar** (número da porta)
- Deep Packet Inspection permite controlar ***o que eles podem "dizer" uns para os outros***

Deep Packet Inspection - DPI

Após aplicar as regras de tradicionais de firewall (Statefull Packet Inspetion - SPI) o DPI inspeciona o conteúdo dentro das mensagens TCP / IP e aplica regras mais dedicadas.

É projetado para compreender o protocolo específico e aplicar filtros em campos e valores importantes para os sistemas de controle. Dependendo do protocolo esses campos podem incluir comandos, objetos, serviços e intervalos de endereçamentos.

Bons firewalls DPI também podem fazer a "verificação da sanidade" de estranhos formatos de mensagens ou comportamentos incomuns (como 10.000 mensagens de resposta à uma única mensagem de solicitação). Esses tipos de mensagens anormais podem indicar tráfego criado por um hacker tentando travar um CLP/IED.

Confiabilidade de Rede no modelo OSI

Onde as falhas de rede ocorrem...

Deep Packet Inspection

HIRSCHMANN A BELDEN BRAND

TOFINO SECURITY A BELDEN BRAND

Roteadores & Firewalls

HIRSCHMANN A BELDEN BRAND

GarrettCom A BELDEN BRAND

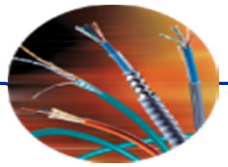
Switches

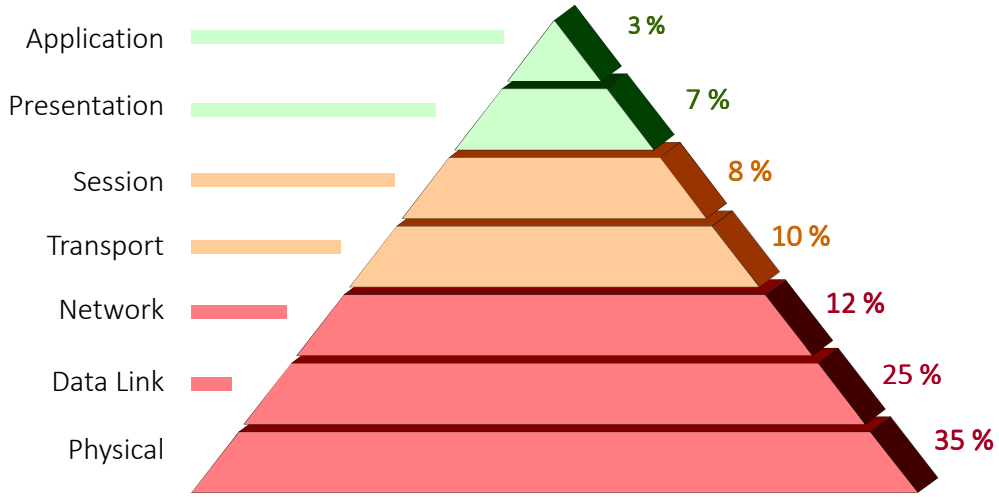
HIRSCHMANN A BELDEN BRAND

GarrettCom A BELDEN BRAND

Cabos

BELDEN SENDING ALL THE RIGHT SIGNALS





Source: Datacom, Network Management Special

Belden 1-2-3: Segurança Cibernética Industrial

#1: Redes Industriais

- Segmentação
- Criação de Zonas
- Monitoramento
- Acesso wireless seguro
- Proteção contra intrusos

TOFINO SECURITY
A BELDEN BRAND

HIRSCHMANN
A BELDEN BRAND

GarrettCom
A BELDEN BRAND

#2: Controladores Industriais

- Detecção e resposta a ataques
- Identificação de alterações não autorizadas e maliciosas
- Identificação de controladores vulneráveis & exploráveis

TOFINO SECURITY
A BELDEN BRAND

#3: Endpoints e Ativos críticos Industriais

- Inventário dos ativos conectados
- Identificação de alterações não autorizadas e maliciosas
- Identificação de sistemas vulneráveis & exploráveis
- Certificação de configurações adequadas

tripwire

Soluções Belden para TI Industrial

Sistemas de redes para missões críticas que oferecem os mais altos níveis de confiabilidade, disponibilidade e segurança

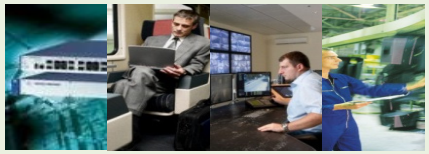
TOFINO SECURITY A BELDEN BRAND · HIRSCHMANN A BELDEN BRAND · GarrettCom A BELDEN BRAND

Mercados Chaves

- Energia
- Discrete
- Processos
- Sistemas de Transportes

Aplicações Chaves

- Infraestrutura de Rede
- Wireless
- Segurança



Soluções

Firewalls

Switches Ethernet

Roteadores e Gateways

Software de Gerenciamento de Rede

Sistemas Wireless

Alguns de nossos clientes no mercado de ENERGIA - Latam

AES Eletropaulo · ISA CTEEP · CPFL · CEEE · Chesf · Furnas · Eletrosul · Eletronorte · ELEKTRO · COPEL · enel Green Power · neoenergia · epm estamos ahí. · electroperu · CFE Comisión Federal de Electricidad · EPSA

Encontro Técnico: Automação na Rede Aérea de Distribuição de Energia

ISA Sao Paulo Section

AES Eletropaulo por onde a vida acontece

BELDEN SENDING ALL THE RIGHT SIGNALS

Exemplo de Seleção de Produtos

Roteador / Firewall


EAGLE


TOFINO


10RX


DX940

Layer 3


MACH


GRS


DX940

Layer 2 – Rack 19"


MACH


GRS

Layer 2 – Trilho DIN


RSPE


RSP / RSPS / RSPL

Conversores de Comunicação Serial para Ethernet


10XTS


DX40


DX940

Centro de Controle

10XTS

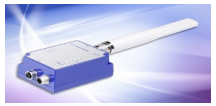

MACH4000

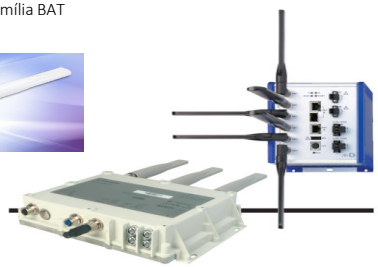
Gerenciamento da Rede

Industrial HiVision

Soluções Wireless 802.11

Hirschmann Família BAT





Encontro Técnico:
Automação na Rede Aérea de Distribuição de Energia

ISA Sao Paulo Section

AES Eletropaulo
por onde a vida acontece

BELDEN
SENDING ALL THE RIGHT SIGNALS

Destaques da Belden para Proteção de Redes

Modos "Self-learning", passivo e teste garantem que não haja interrupção das operações

Self-learning para preencher regras e proporcionar visibilidade usando dados atuais (não apenas o que alguém "acha" que está acontecendo), reduzir possibilidade de erro humano e aumentar a consistência

Instalação Plug and Protect™ sem interrupção nem mudanças na arquitetura e sub-redes da rede: não altera a rede existente e não necessita de reconfiguração de sub-redes

Notificação de alarme e registro de eventos - útil para notificação em tempo real, resolução de problemas e análise forense

Criar facilmente Zonas e Conduites de segurança para proteger equipamentos de controle e ICS/SCADA críticos

Engenheiros de automação pode configurar facilmente as regras

Altamente classificados para ambientes agressivos e perigosos

A Belden é o único fabricante que pode abranger verdadeiramente a proteção de rede Corporativa e ICS/SCADA
Tofino, GarrettCom, Hirschmann

Dúvidas?