Desafios da Transformação Digital para o Setor de Energia

Ricardo Afonso | Eng. de Produto - Divisão Automação | Ladder Automação

II Encontro Técnico ISA São Paulo na AES Eletropaulo
Transformação Digital no Setor de Energia

1° de setembro de 2017 - Barueri / SP

Desafios da Transformação Digital para o Setor de Energia

Ricardo Afonso
ricardoafonso@ladder.com.br

II Encontro Técnico Transformação Digital no Setor de Energia

ISA Sao Paulo Section

AES Eletropaulo

DIGITALIZAÇÃO

Entenda como este conceito pode lhe auxiliar na jornada da quarta revolução industrial

A Digitalização é o meio de alcançar objetivos e resultados de negócios, tornando as empresas mais produtivas, inovadoras e competitivas

II Encontro Técnico Transformação Digital no Setor de Energia

ISA Sao Paulo Section

AES Eletropaulo

A **TRANSFORMAÇÃO DIGITAL** e a **Internet de todas as coisas (IoT)** possibilitam a criação de valores entre diferentes áreas

Information Technology

IT

Operations Technology

OT

IoT

Internet of Things

Internet de Todas as Coisas

Iniciativas Governamentais

Visões para garantir a liderança da produção

Smart Manufacturing Leadership Coalition

Industrie 4.0

Made in China 2025

Manufacturing Innovation 3.0

Usine du Futur

Transformação Digital

Tecnologias

Inovações que irão redefinir e criar novas oportunidades de valor

IoT Internet of Things

Security

"Robôs Colaborativos"

Consorcio Industrial

Definir e Promover as melhores Práticas

Industrial IP ADVANTAGE — CONNECT INFORM TRANSFORM

industrial internet CONSORTIUM

MESA INTERNATIONAL — Driving Operations Excellence

Padrões Industriais

Permitem a Interoperabilidade e Uniformização

IEC · OPC FOUNDATION · ISA · IEEE · ISO

II Encontro Técnico Transformação Digital no Setor de Energia

ISA Sao Paulo Section

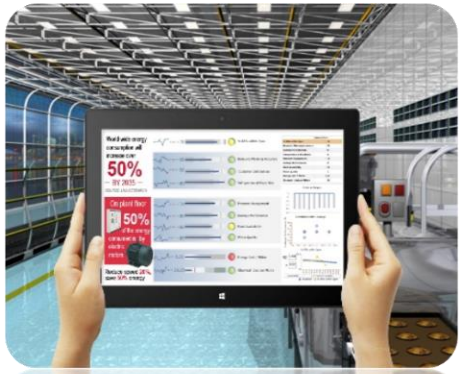
AES Eletropaulo

Tecnologias contemporâneas que habilitam a Digitalização

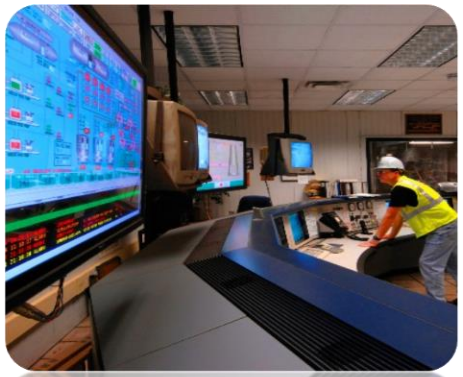
BIG DATA

CYBERSECURUTY

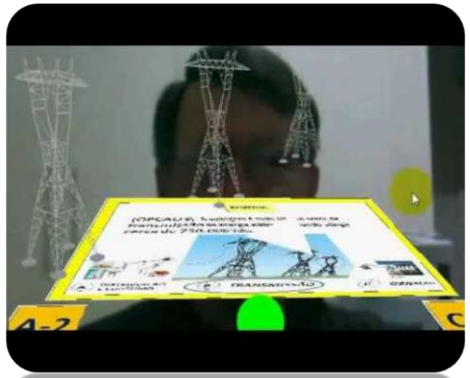
CLOUD / FOG



MOBILIDADE



VIRTUALIZAÇÃO



REALIDADE AUMENTADA

Data Analytics para Smart Grid

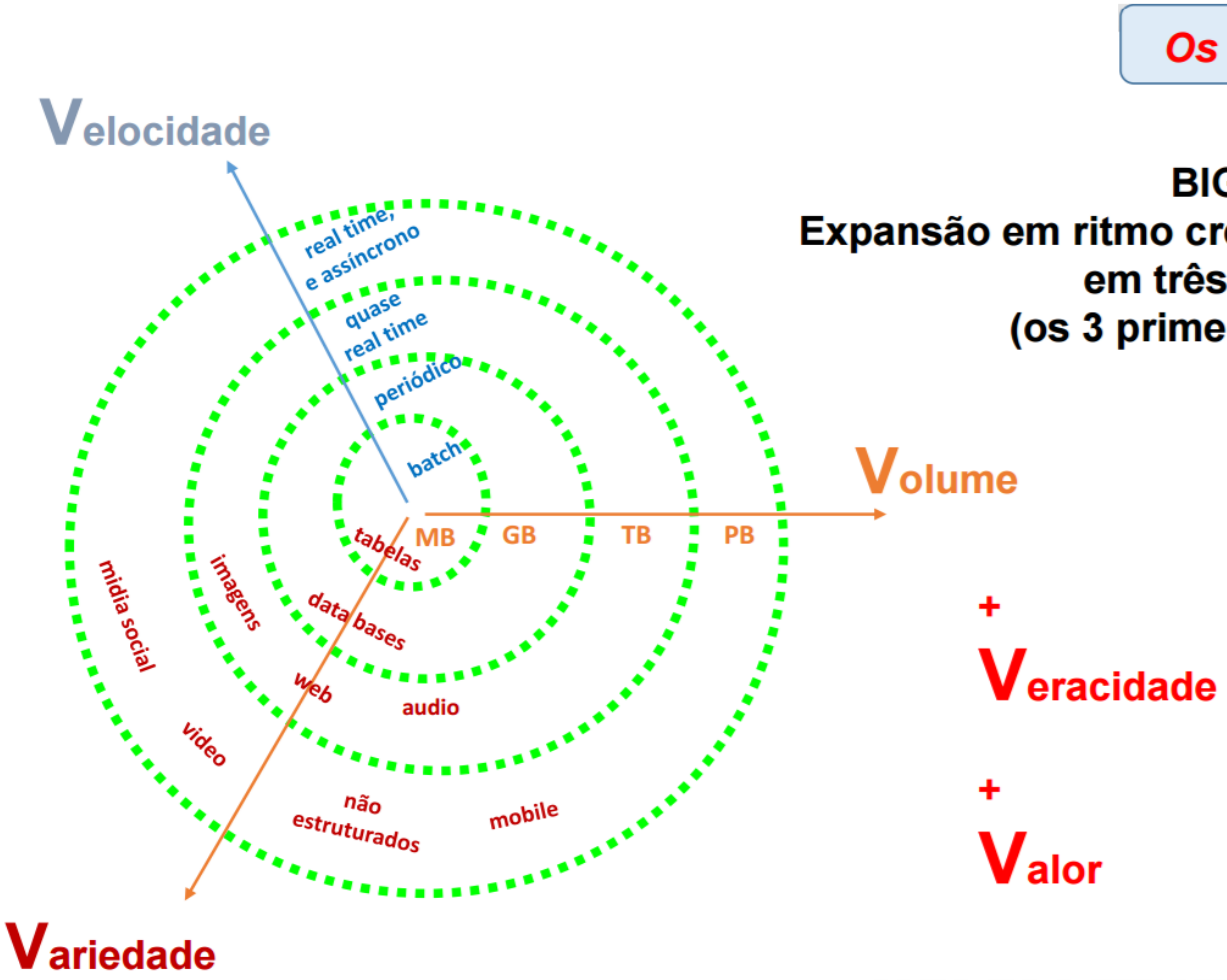
BIG DATA

Big Data é feito de informações estruturadas e não estruturadas.

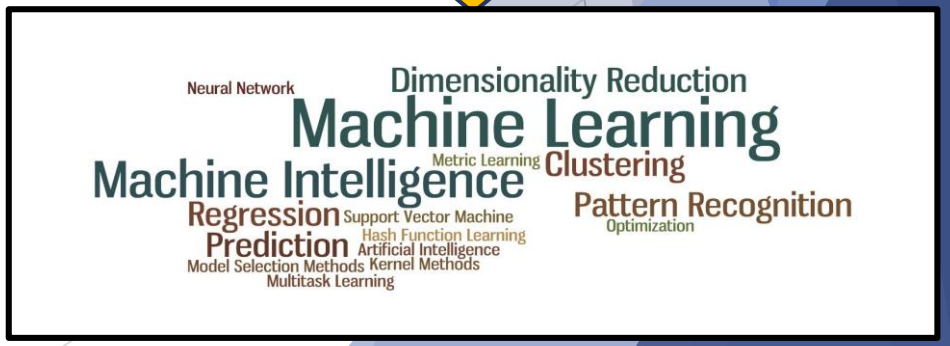
10%
ESTRUTURADA
Informação estruturada é o dado em base de dados e corresponde a 10% da história.

90%
NÃO ESTRUTURADA
Informações não estruturadas correspondem a 90% dos dados e consiste na informação produzida pelas pessoas, como e-mails, vídeos, tweets, posts no Facebook, conversas de call centers, imagens de circuitos fechados de TV, chamadas telefônicas ou cliques em sites.

Regra dos 5 Vs para análise do Big Data



BIG DATA:
Expansão em ritmo crescente em três frentes (os 3 primeiros Vs)

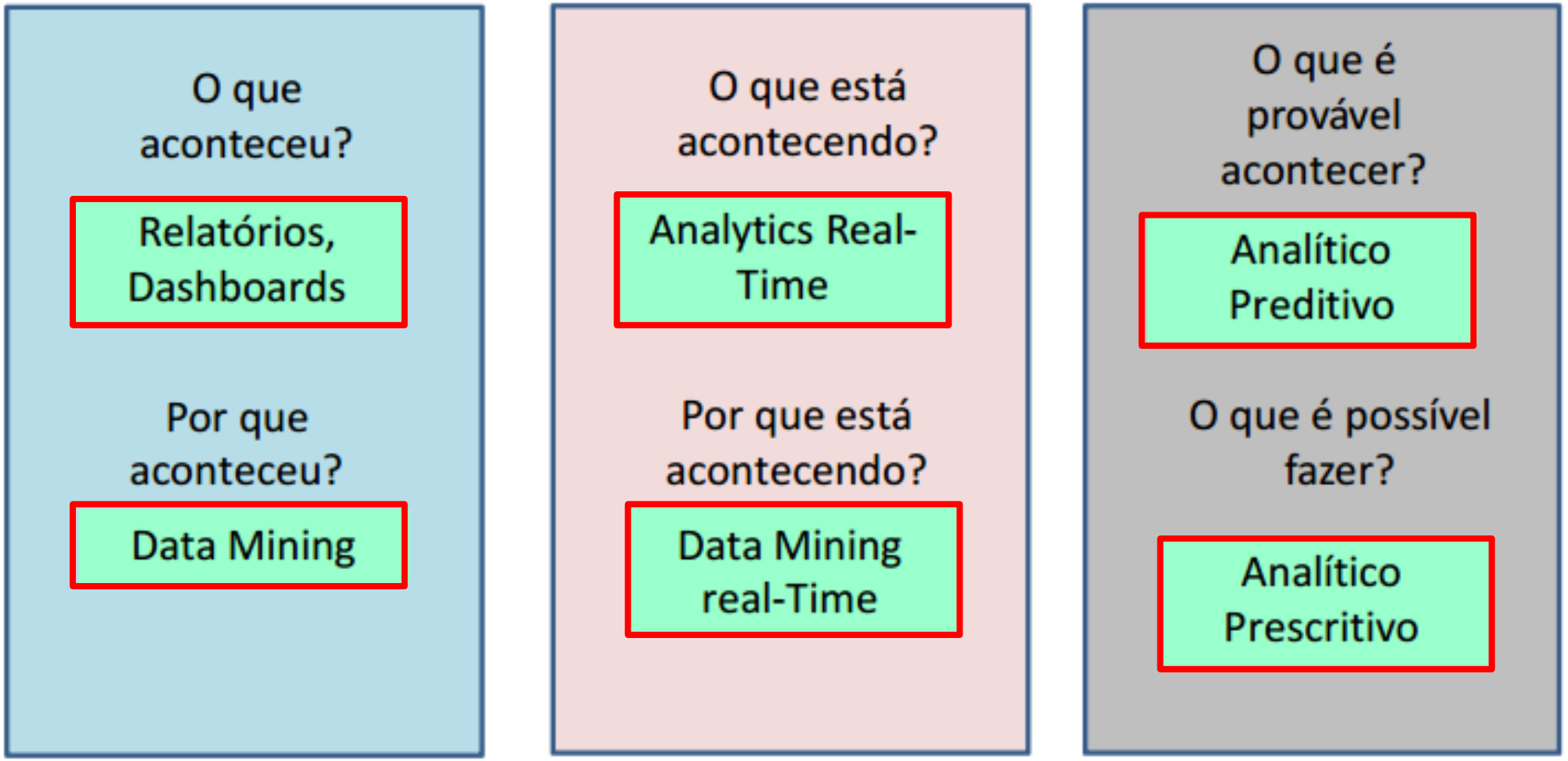


II Encontro Técnico
Transformação Digital
no Setor de Energia

ISA Sao Paulo Section

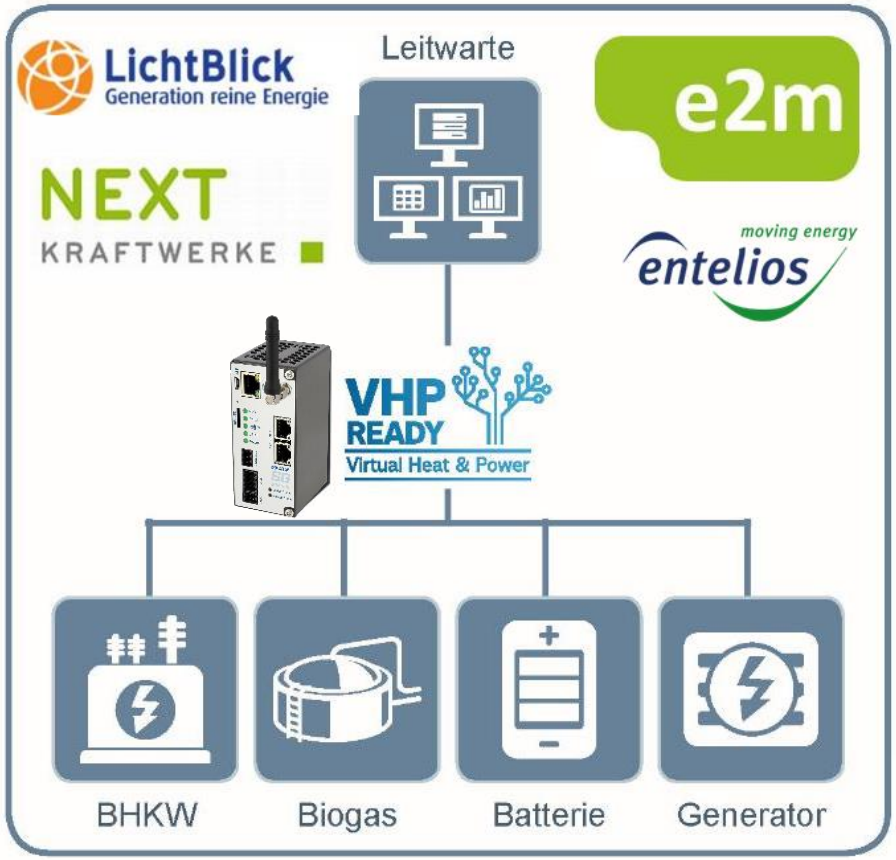
AES Eletropaulo

Indicadores globais



Aplicação com **VHP Ready / VPP

Virtual Power Plant / Demand Response



2G Energy AG

VIESMANN
climate of innovation

Younicos
Let the fossils rest in peace.

SONNEN BATTERIE

II Encontro Técnico
Transformação Digital
no Setor de Energia

ISA Sao Paulo Section

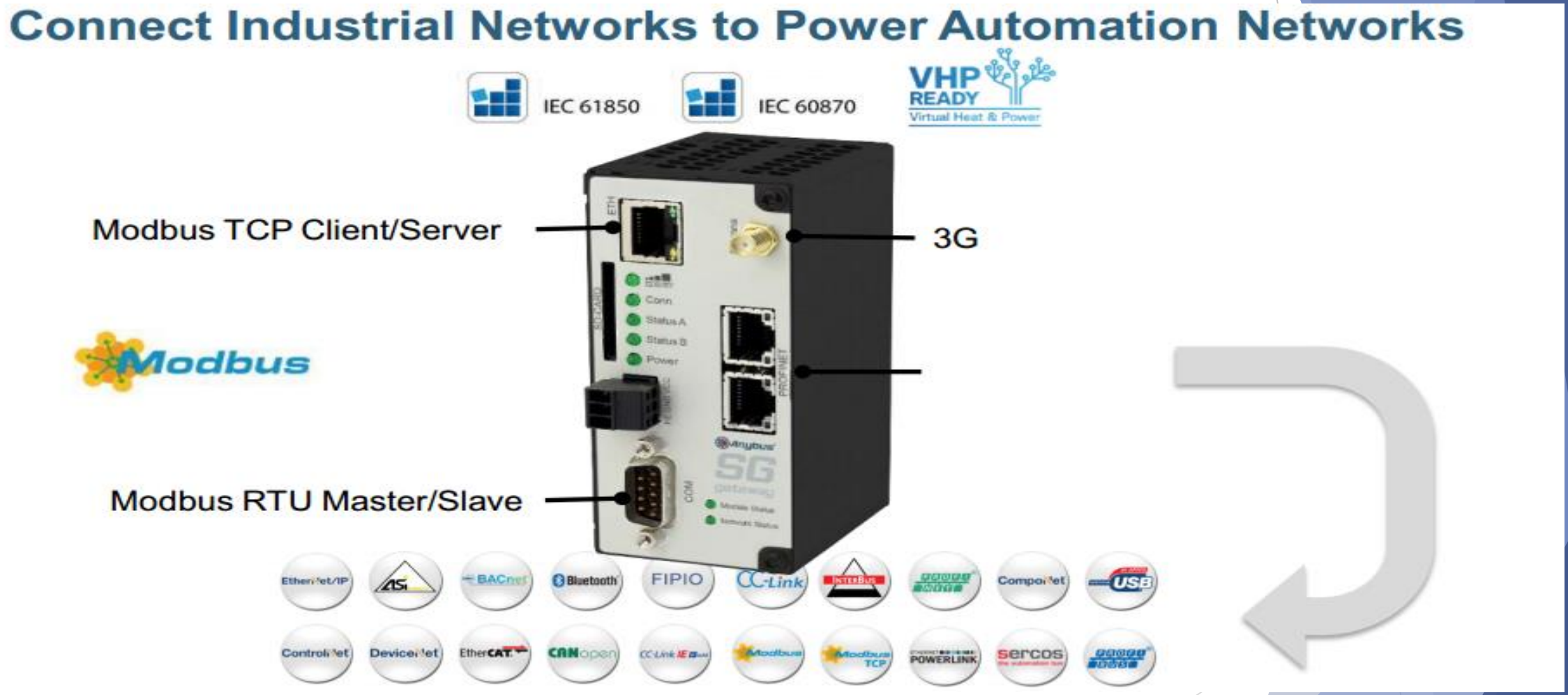
AES Eletropaulo

**Notas:

- VHP: Virtual Heat & Power Ready
- VPP: Virtual Power Plant

Aplicação com **VHP Ready / VPP

Virtual Power Plant / Demand Response



II Encontro Técnico
Transformação Digital
no Setor de Energia

ISA Sao Paulo Section

AES Eletropaulo

**Notas:

- VHP: Virtual Heat & Power Ready
- VPP: Virtual Power Plant

II Encontro Técnico
Transformação Digital
no Setor de Energia

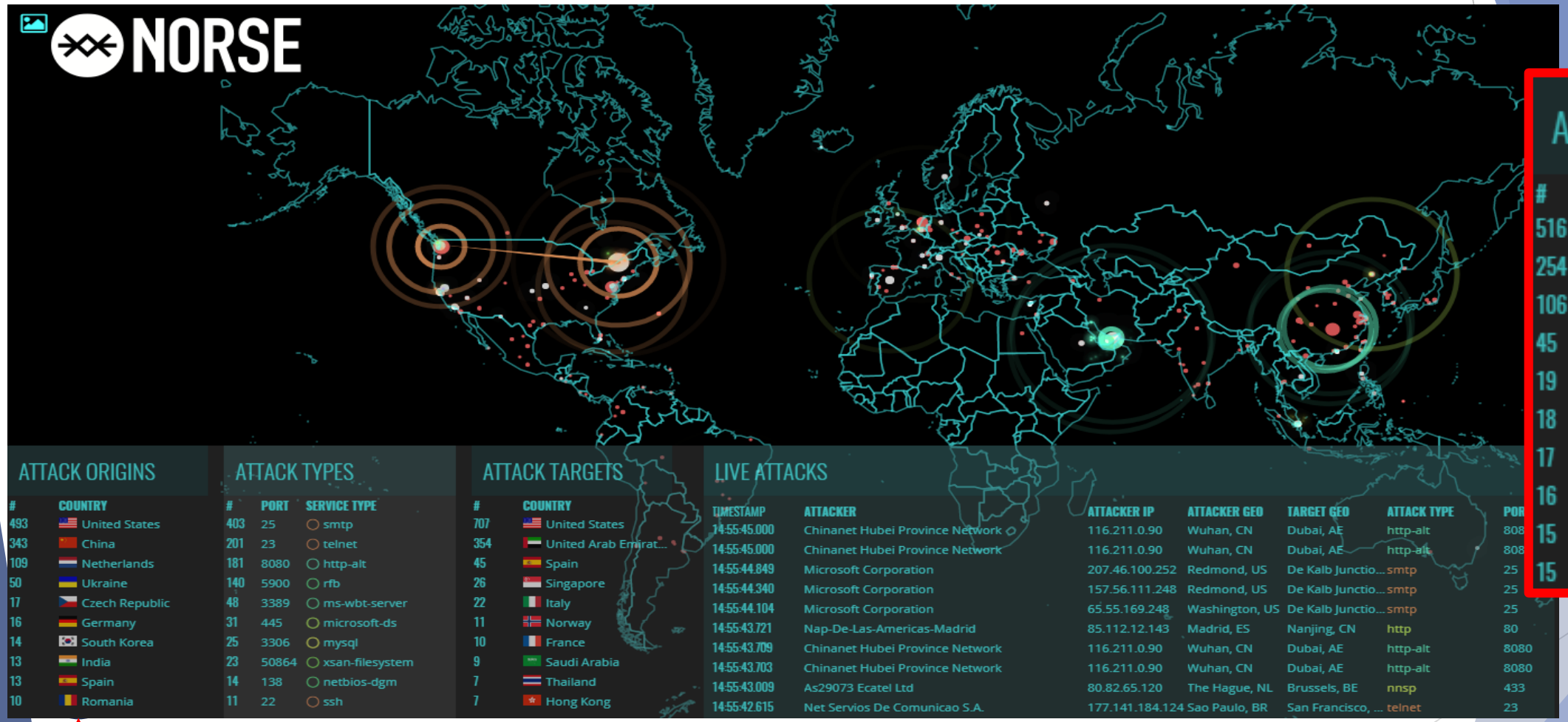
ISA Sao Paulo Section

AES Eletropaulo

Segurança de dados / Informação

- Por que isso é importante?
- Tendências de Segurança Industrial
- Defesa em Profundidade
- Estrutura de Segurança de Rede Industrial
- Pontos Importantes

Por que isso é importante?
Mapa em tempo real de ataques Cibernéticos



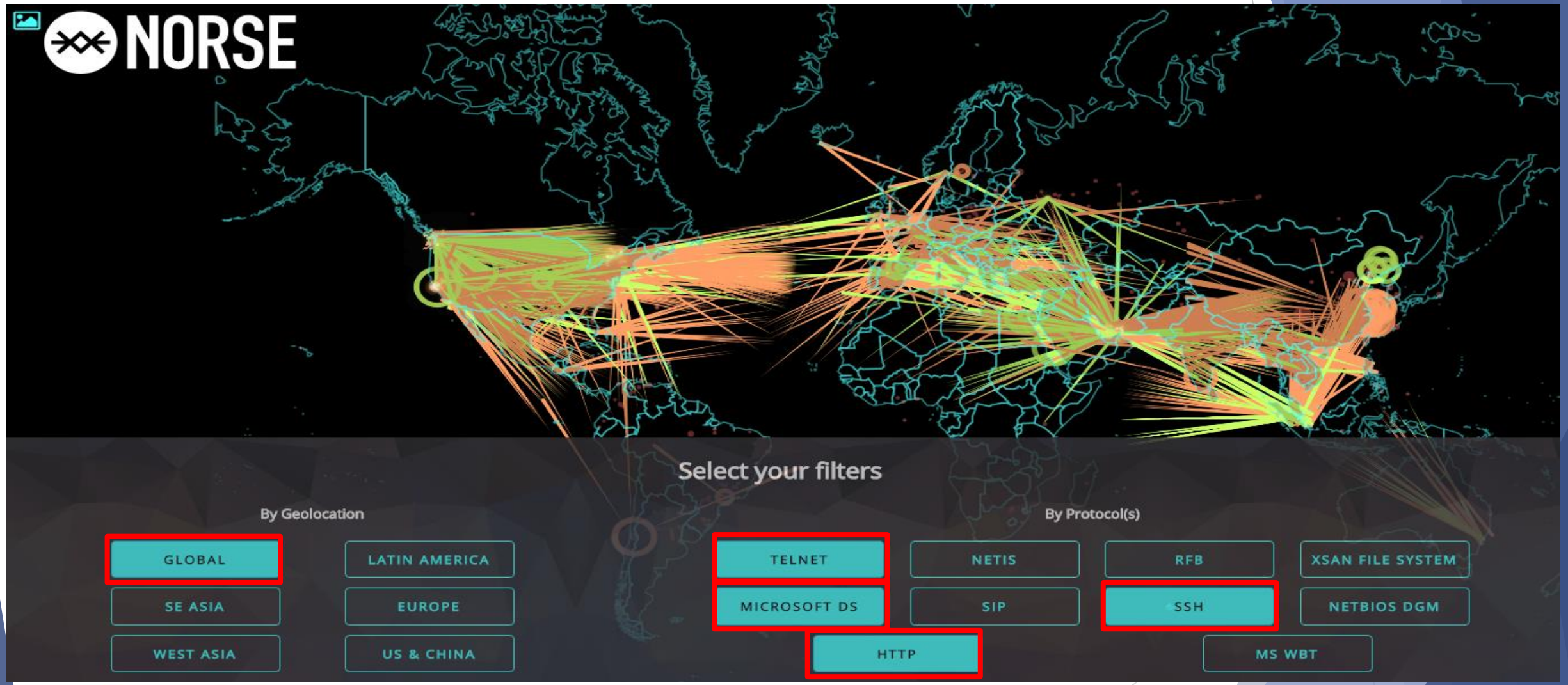
II Encontro Técnico
Transformação Digital
no Setor de Energia

ISA Sao Paulo Section

AES Eletropaulo

Fonte: http://map.norsecorp.com/#/

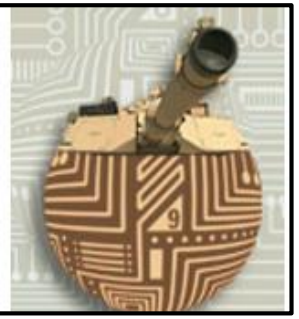
Por que isso é importante?
Mapa em tempo real de ataques Cibernéticos



Segurança da Informação
Realidade Agora.....

Ataques cibernéticos causam prejuízo de US$ 315 bilhões em um ano

Da redação ... 19/10/2015 ... Convergência Digital



Segurança ... 04/11/2015 ... 15:03

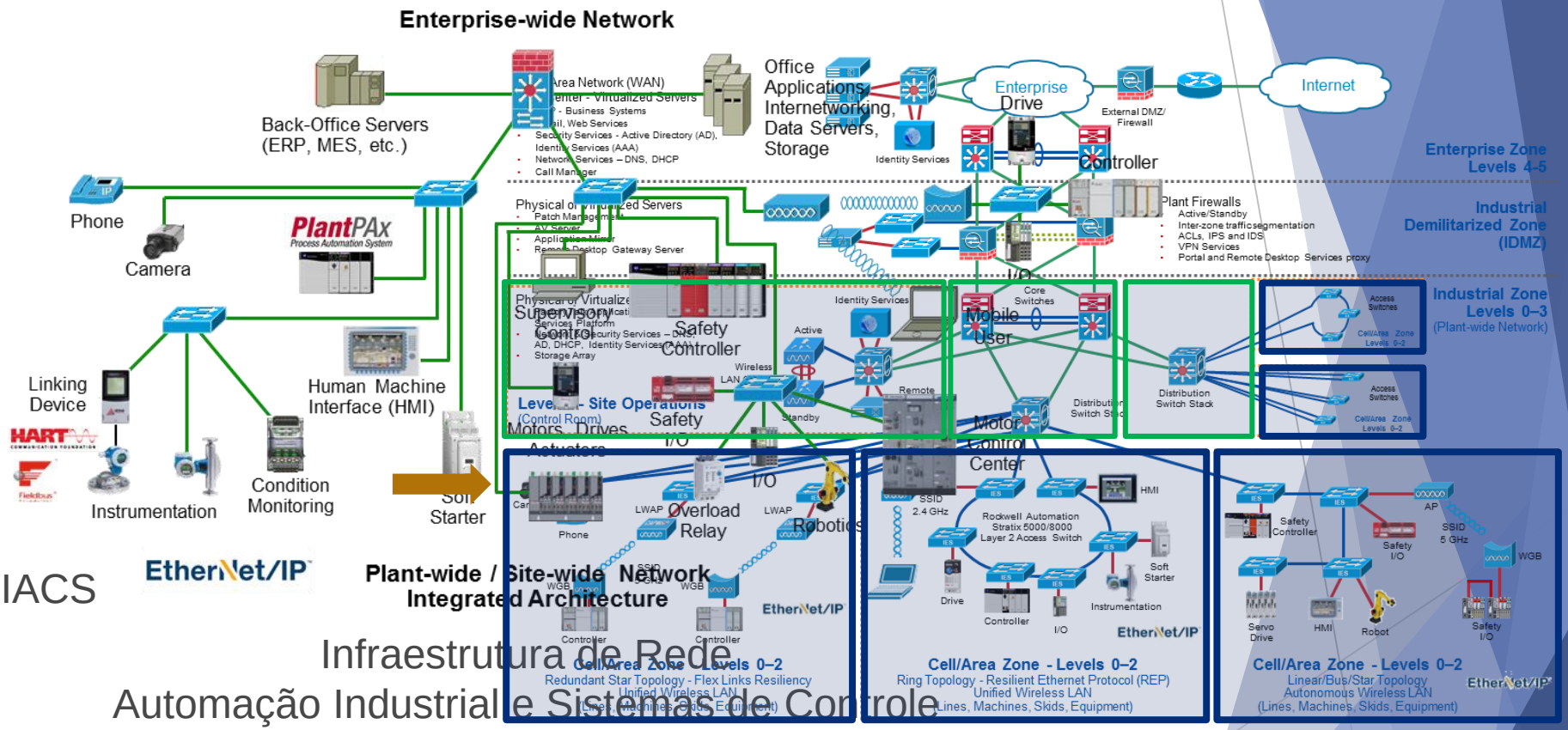
Um novo tipo de vírus de computador é criado a cada cinco segundos

Hackers atacam indústria, diz Fiesp (Valor Econômico)

Publicado em: 31 de março de 2015 | Visualizações: 101

Empresas de todos os portes no Estado de São Paulo foram atacadas no ano passado por hackers, sendo que 35% das invasões foram bem-sucedidas. O maior alvo foram as indústrias de grande porte - 22% delas afirmaram que sofreram de um a dez ataques no ano. Do total das invasões, 59% tinham motivação financeira, inclusive com transferências em dinheiro. Em 46,2% das grandes companhias, os hackers buscavam informações sigilosas.

Por que isso é Importante?
Convergência ⇔ Automação Industrial & Sistema de Controle



Infraestrutura de Rede IACS
Flat e Aberta

Infraestrutura de Rede
Automação Industrial e Sistemas de Controle
FLAT e Aberta

Estruturada e Robusta
IACS Network Infrastructure

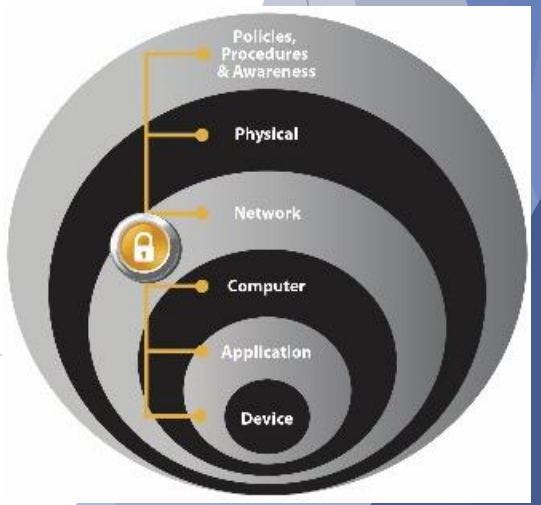
Tendências em Segurança Industrial
Padrões Estabelecidos de Segurança Industrial

- International Society of Automation
  - ISA/IEC-62443, Industrial Automation and Control Systems (IACS) Security
  - Zonas e Canais
  - Defesa em profundidade
  - Implantação de IDMZ
- National Institute of Standards and Technology
  - NIST 800-82, Industrial Control System (ICS) Security
  - Estrutura Cybersecurity: Identificar, Proteger, Detectar, Responder, Recuperar
  - Defesa em profundidade
  - Implantação de IDMZ
- Department of Homeland Security / Idaho National Lab
  - DHS INL/EXT-06-11478
  - Cyber Security em Sistemas de Controle: Estratégias de Defesa em Camada
  - Defesa em profundidade
  - Implantação de IDMZ

Defesa em Profundidade Abrangente

Rede EtherNet ⇔ Industrial Automation and Control System - IACS

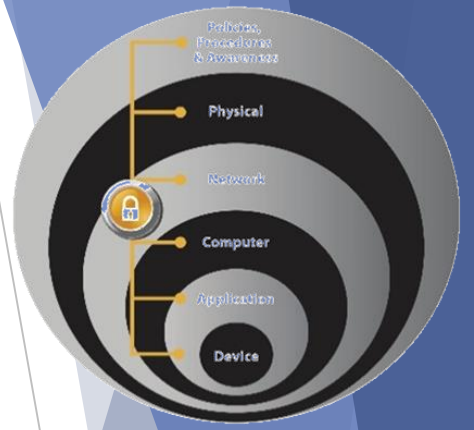
- Aberta por padrão para permitir a coexistência de tecnologia e a interoperabilidade entre dispositivos para Redes de Automação Industrial e Sistemas de Controle (IACS)
- Segurança via configuração e arquitetura:
  - Configuração
    - ✓ Fortalecer a infraestrutura através da adoção de multiplas camadas de segurança com o método de segurança em profundidade
  - Arquitetura
    - ✓ Estruturar a infraestrutura para defender a borda - DMZ Industrial (IDMZ)

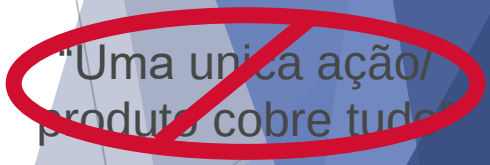


Defesa em Profundidade Abrangente
Elementos críticos para a Segurança Industrial

- Um programa de segurança industrial equilibrado deve abordar tanto os controles Técnicos e os controles não Técnicos
- **Controles não-técnicos** - Regras para ambientes:

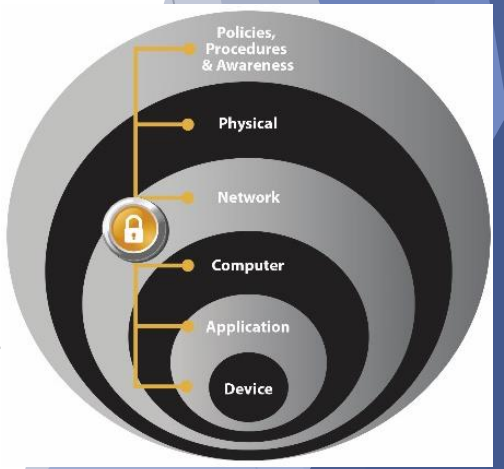
  Ex. práticas corporativas, normas e padrões, programas de políticas, procedimentos, gestão de risco, **programas de educação e sensibilização dos usuários.**
- **Controles Técnicos** - tecnologia para fornecer medidas restritivas para controles não-técnicos: por exemplo, Firewalls, Grupos de Segurança, Layer 3 com listas de controle de acesso (ACLs)
- A segurança é tão forte quanto o elo mais fraco
- Vigilância e atenção aos detalhes são a CHAVE para o sucesso da segurança a longo prazo





Defesa em Profundidade Abrangente
Rede EtherNet ⇔ Industrial Automation and Control System - IACS

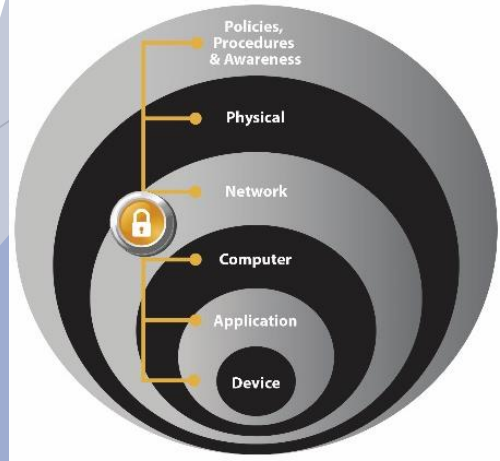
- Nenhum produto, tecnologia ou metodologia pode sozinho assegurar aplicações para redes IACS.
- Proteger os ativos da IACS requer uma abordagem de segurança em profundidade a qual aborde ameaças de segurança internas e externas.
- Esta abordagem se utiliza de multiplas camadas de defesa (física, procedimental e eletrônica) em níveis separados da IACS aplicando políticas e procedimentos para endereçar diferentes tipos de ameaças.



Defesa em Profundidade Abrangente

Políticas de Segurança Industrial ⇔ Direcionamento e Técnicas de Controle

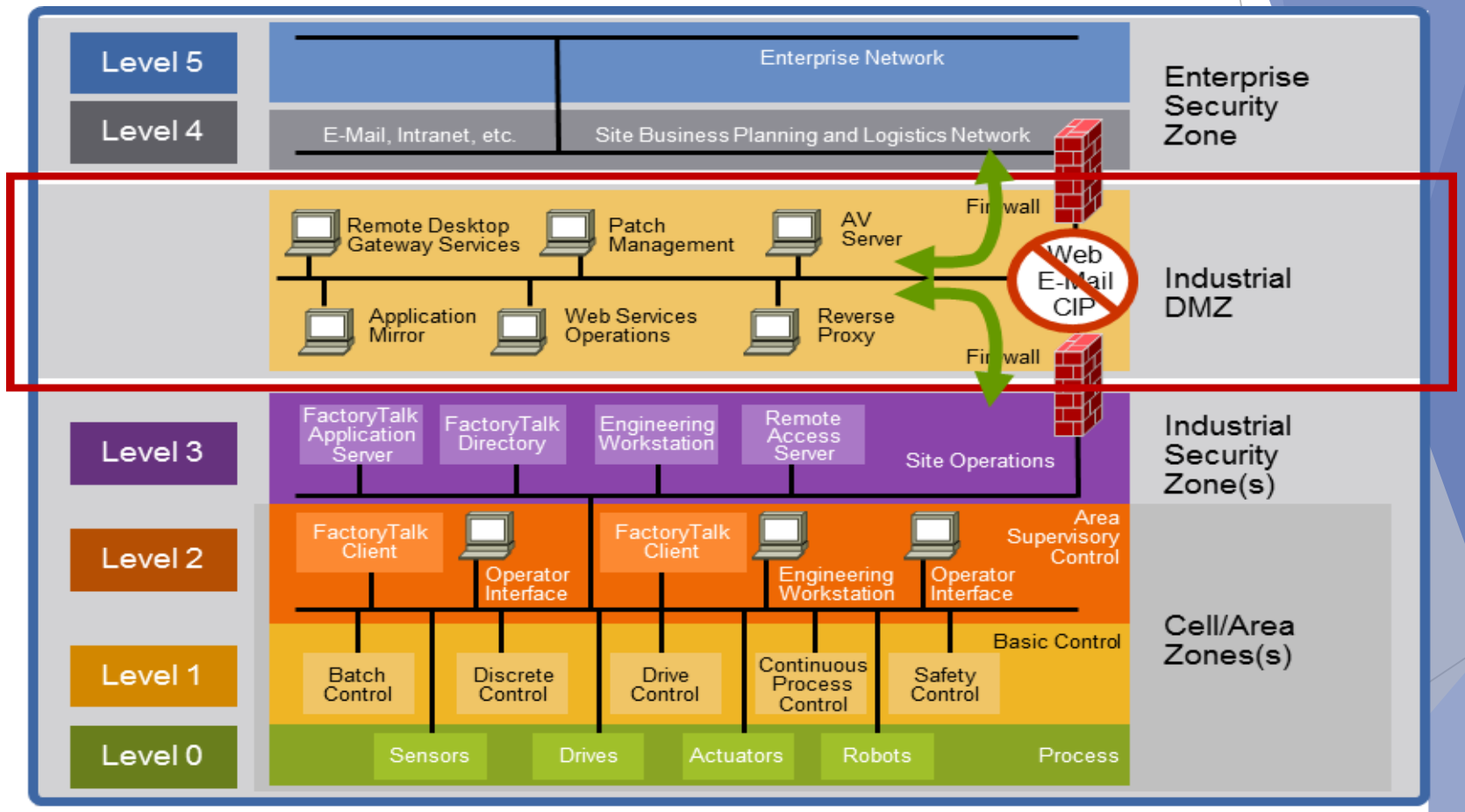
- **Programas de Educação e Sensibilização** – Treinamento da equipe de OT em políticas e procedimentos de segurança industrial em como agir no caso de um incidente de segurança
- **Físico** – limitar o acesso físico para pessoas autorizadas: sala de controle, celulas/areas, painel de controle, dispositivos IACS …. fechaduras, portões, chaves magneticas, biometria. Inclusão na politica de segurança, procedimentos e tecnologia para acompanhar e monitorar visitants
- **Rede** – CPwE Industrial Network Security Framework: modelo físico e lógico de rede com políticas de firewall, políticas de access control list (ACL) para switches e roteadores, AAA, IDS/IPS (detecção e prevenção de intrusão), Proteção Anti-Malware.
- **Computadores em ambiente Industrial** – gerenciamentos de patches, software anti-vírus, remoção de aplicações/ protocolos e serviços não utilizados fechando portas lógicas desnecessárias e protegendo portas físicas
- **Aplicação** – Autenticação, Autorização e Auditoria (AAA)
- **Dispositivos IACS**– Gerenciamento de mudanças, criptografia de comunicação e acesso restrito



Industrial Demilitarized Zone (IDMZ)
Industrial Network Security Framework

- Uma IDMZ, ou Zona Desmilitarizada Industrial, é uma sub- rede colocada entre uma rede confiável (industrial) e uma rede não confiável (corporativa) .
- A IDMZ contém ativos de contato com a camada de negócios da empresa que atuam como mediadores entre as redes confiáveis e não confiáveis.
- Tráfego nunca passa direto em uma IDMZ .
- Uma IDMZ corretamente projetada pode ser desligada se for comprometida e ainda permitir que a rede industrial possa operar sem interrupções.

Industrial Demilitarized Zone (IDMZ)
Industrial Network Security Framework



CPwE Logical Model
Converged Multi-discipline IACS

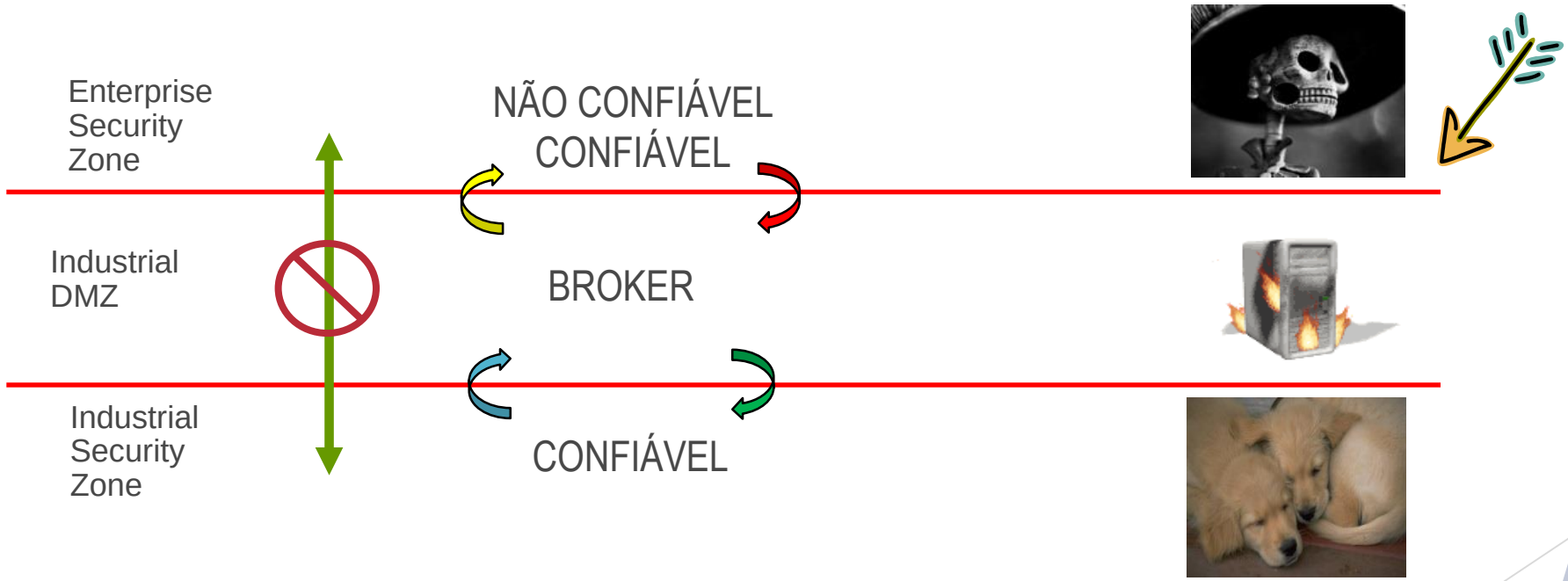
II Encontro Técnico
Transformação Digital
no Setor de Energia

ISA Sao Paulo Section

AES Eletropaulo

Industrial Demilitarized Zone (IDMZ)
Industrial Network Security Framework

- Algumas vezes referida como o perímetro de uma rede que expõe uma das organizações a serviços externos para uma rede de modo não confiável . O objetivo da IDMZ é adicionar uma camada adicional de segurança para a rede segura no sistema de manufatura



Pontos Importantes

- Educação e Sensibilização:
  - Dentro da sua organização, para seus clientes e parceiros de negócios
- Estabelecer um diálogo aberto entre os grupos de IT e OT
- Estabelecer uma política de Segurança Industrial, única e a partir da política de segurança corporativa existente na empresa
- Abordagem de Defesa em Profundidade Abrangente: nenhum produto, metodologia, ou segurança fornece sozinha segurança para redes IACS.
- Se familiarize com os padrões internacionais de segurança para IACS (Industrial Automation and Control System Security Standards)
  - IEC-62443 (Antiga ISA99), NIST 800-82, DHS External Report # INL/EXT-06-11478
- Utilize padrões, modelos e arquiteturas de referência.
- Trabalhe com parceiros reconhecidos e acreditados em seguranca da informação e automação industrial

CASE DE SUCESSO

EDGE GLOBAL SUPPLY

Automação das Subestações em Hospital, utilizando múltiplos protocolos para análise e controle do sistema.

II Encontro Técnico Transformação Digital no Setor de Energia

ISA Sao Paulo Section

AES Eletropaulo

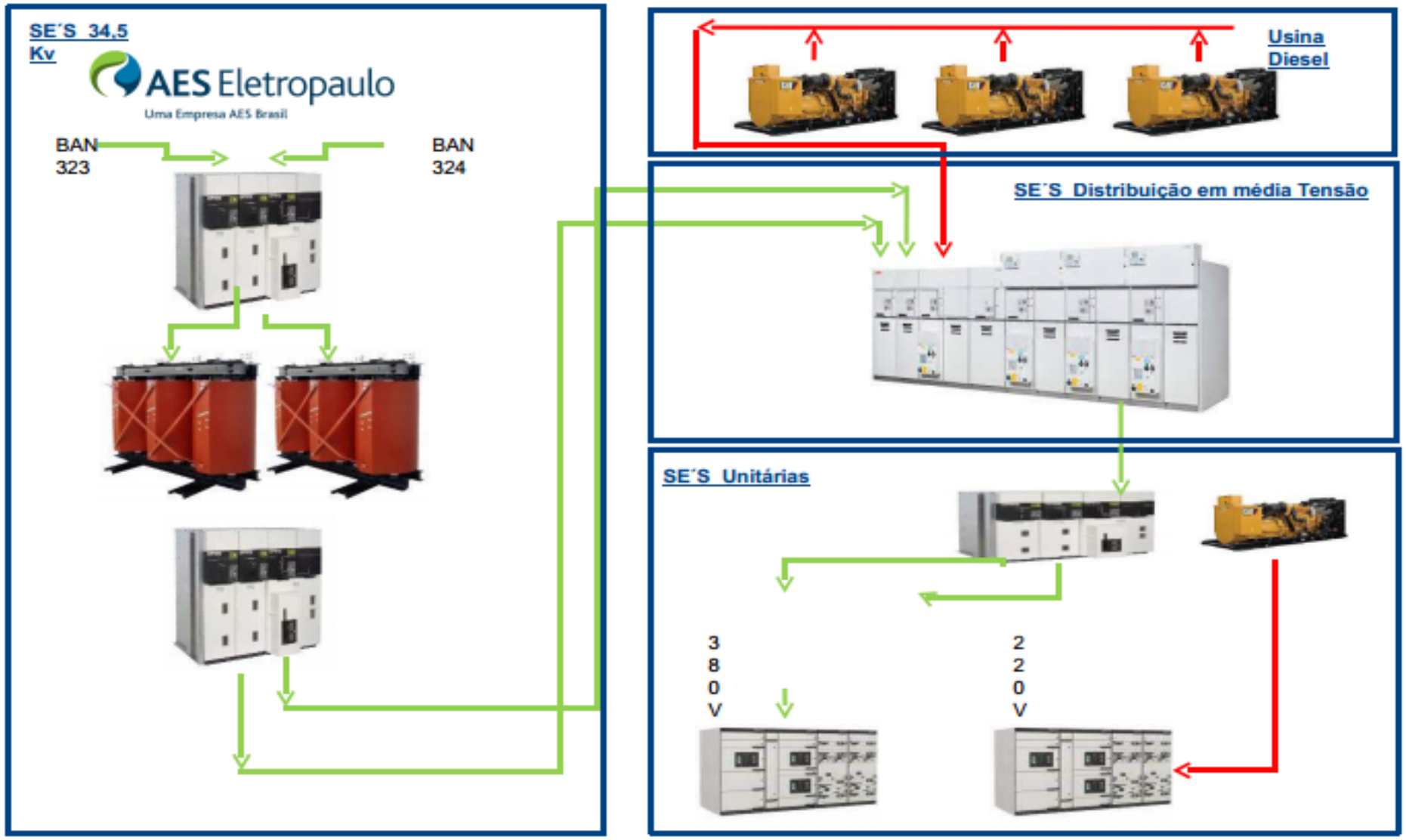
Motivação do Projeto

- **Histórico**
  - Hospital altamente focado na qualidade de atendimento e segurança do paciente;
  - Metas arrojadas de expansão e melhoria contínua dos processos;

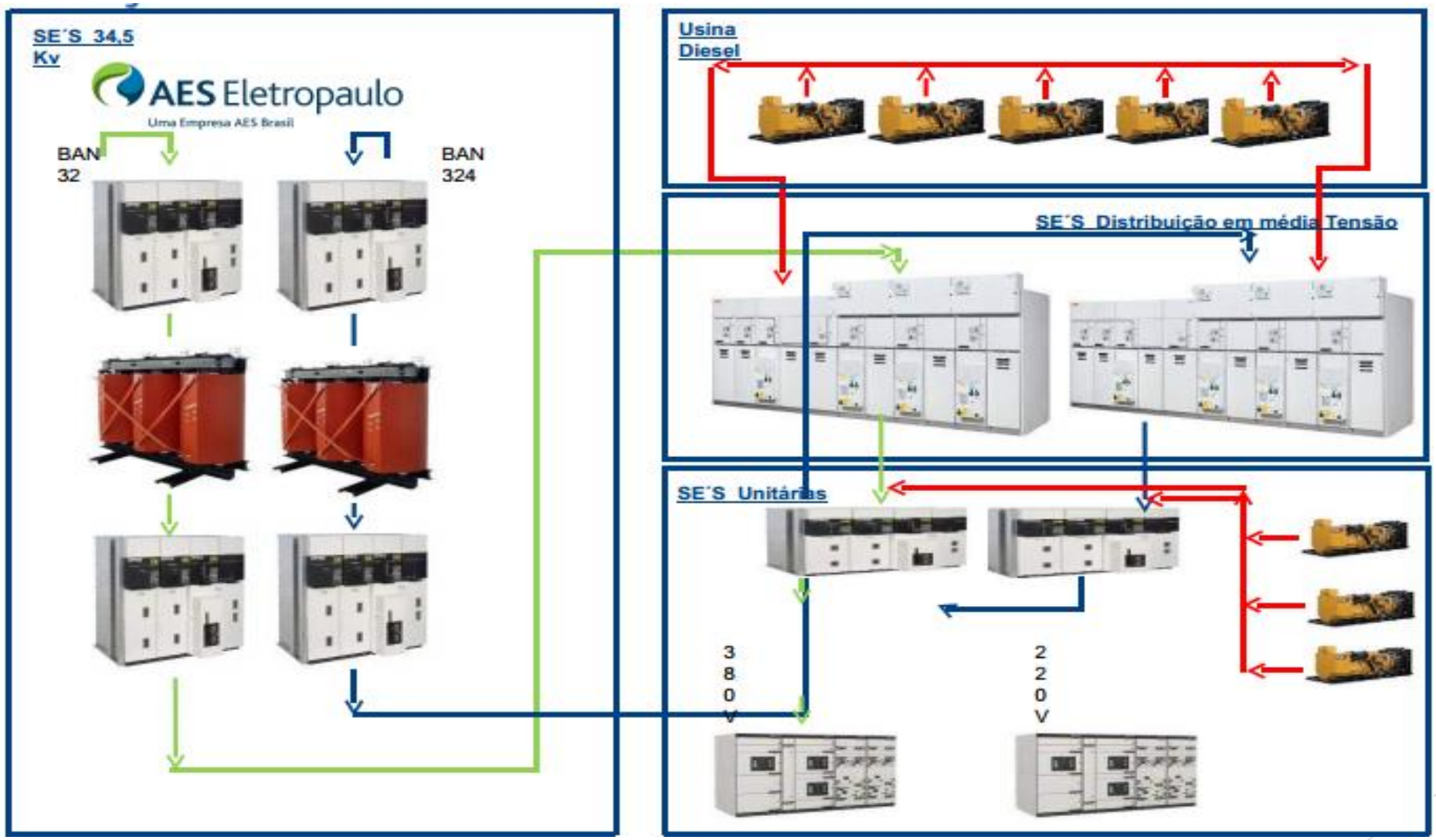
- **Desafio**
  - Modernizar os sistemas elétricos de potência com foco na segurança operacional do complexo, buscando as melhores práticas mundiais de segurança do paciente;

- **Ações**
  - Analisar as deficiências e fragilidades do sistema elétrico de potência
  - Projetar o crescimento do complexo para os próximos 20 anos
  - Estabelecer um plano diretor de implantação, com cinco anos de duração dividido em 7 fases

Topologia Inicial



Topologia Futura



Desafios da Automação

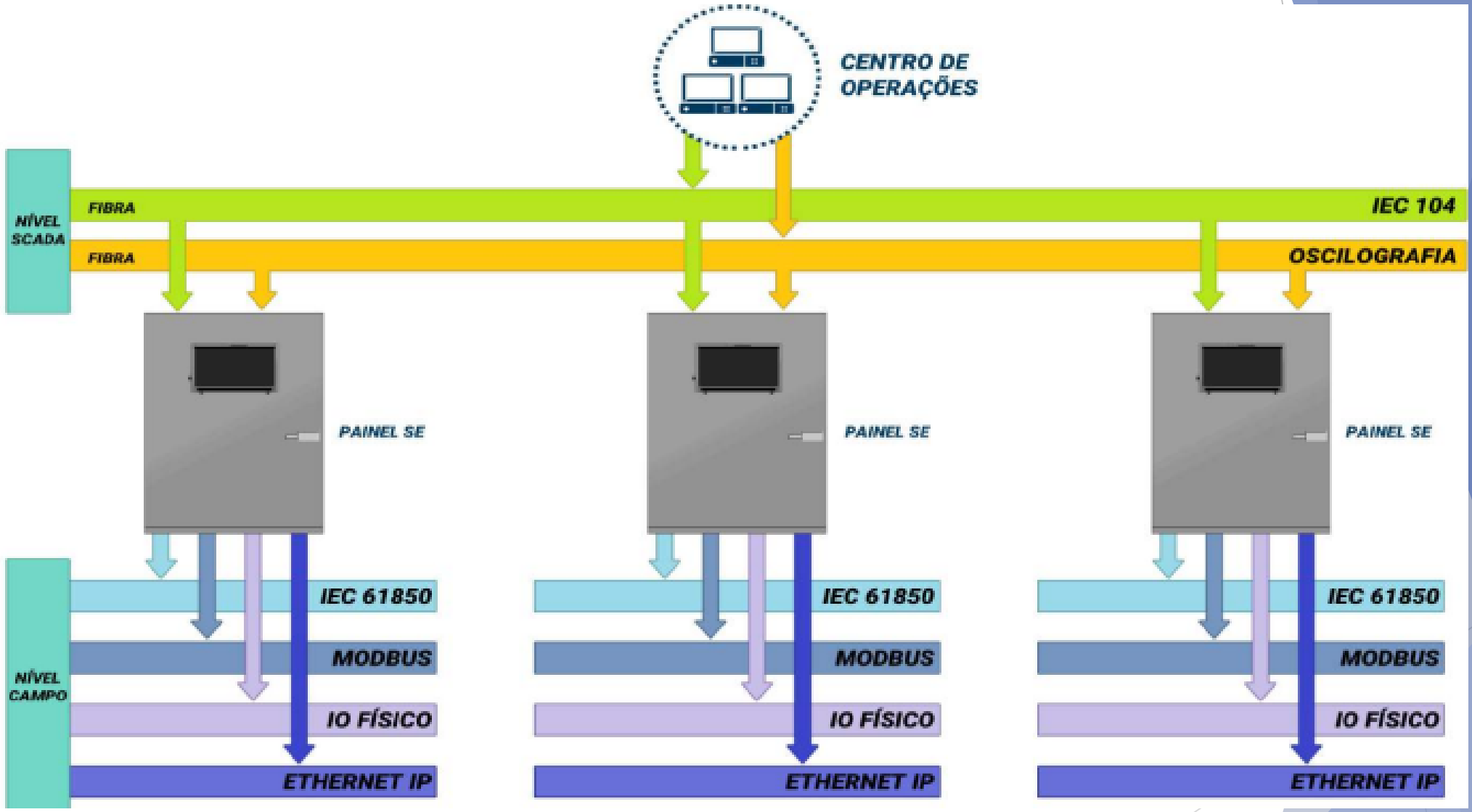
- Implantação sob rigorosos requisitos de segurança
- Projetar uma arquitetura de automação robusta e preparada para futuras expansões;
- Convergência de protocolos e com tecnologia legadas

- Aplicação do protocolo IEC-61850 com **MMS e **Goose
- Rede Ethernet/IP alta performance para análise e controle
- Load Sharing: Nível de decisão realizada por PLC

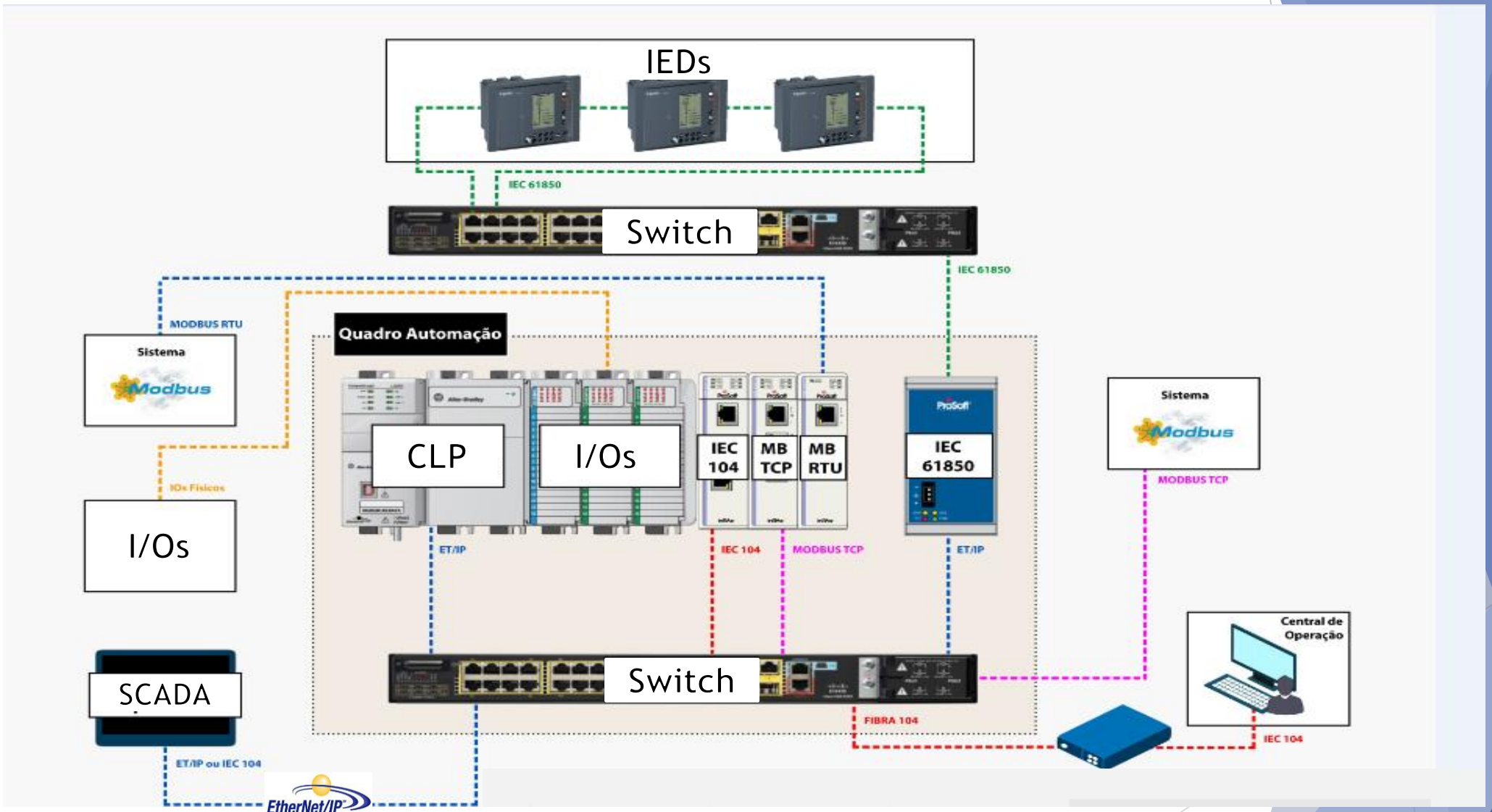
- Criação de um Centro de Operações
- Estrutura Robusta para **SLA de manutenção baixo

**Notas:
- MMS: Manufacturing Message Specification
- Goose: Generic Object Oriented Substation Event
- SLA: Service Level Agreement

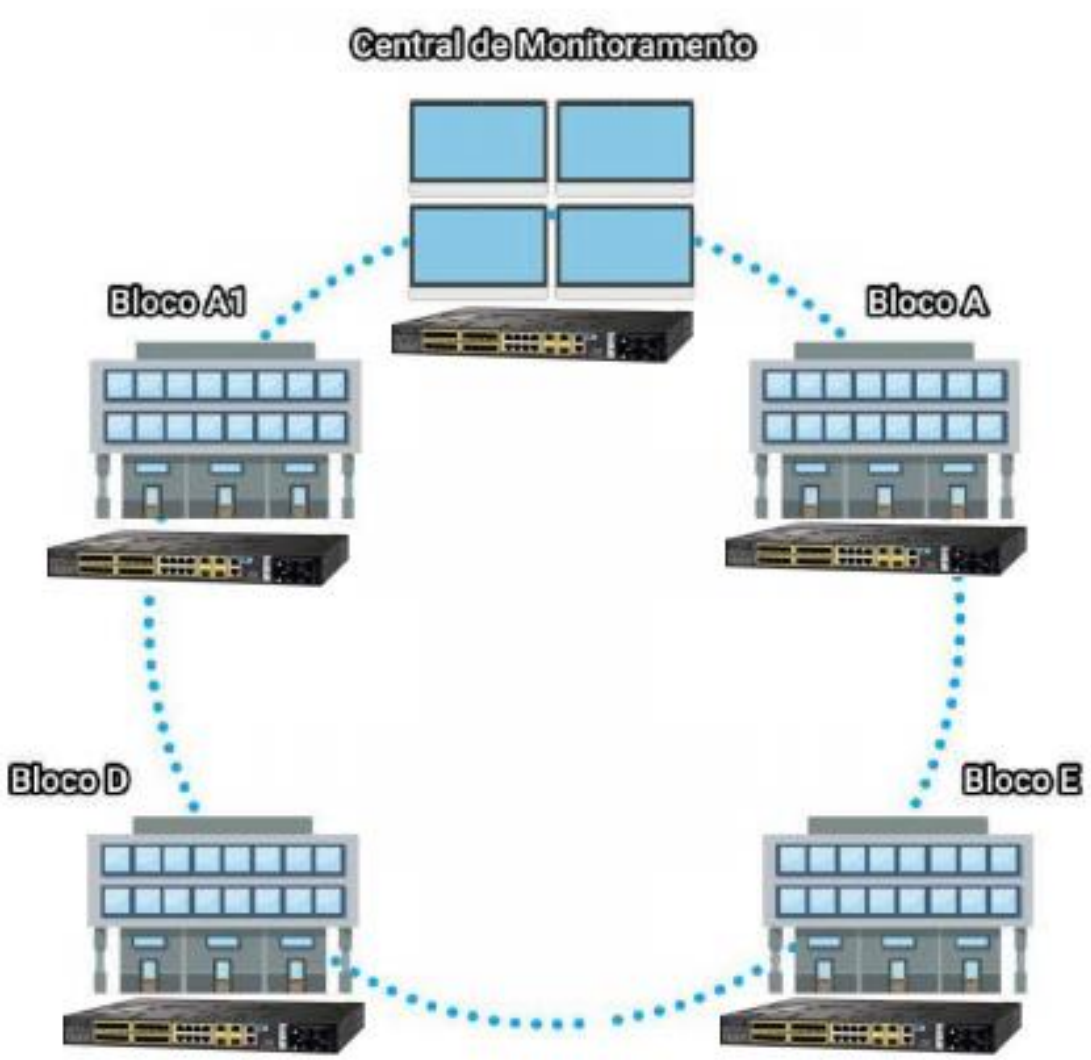
Arquitetura Conceitual



Arquitetura do sistema - Final



Disponibilidade da rede com topologia em ANEL

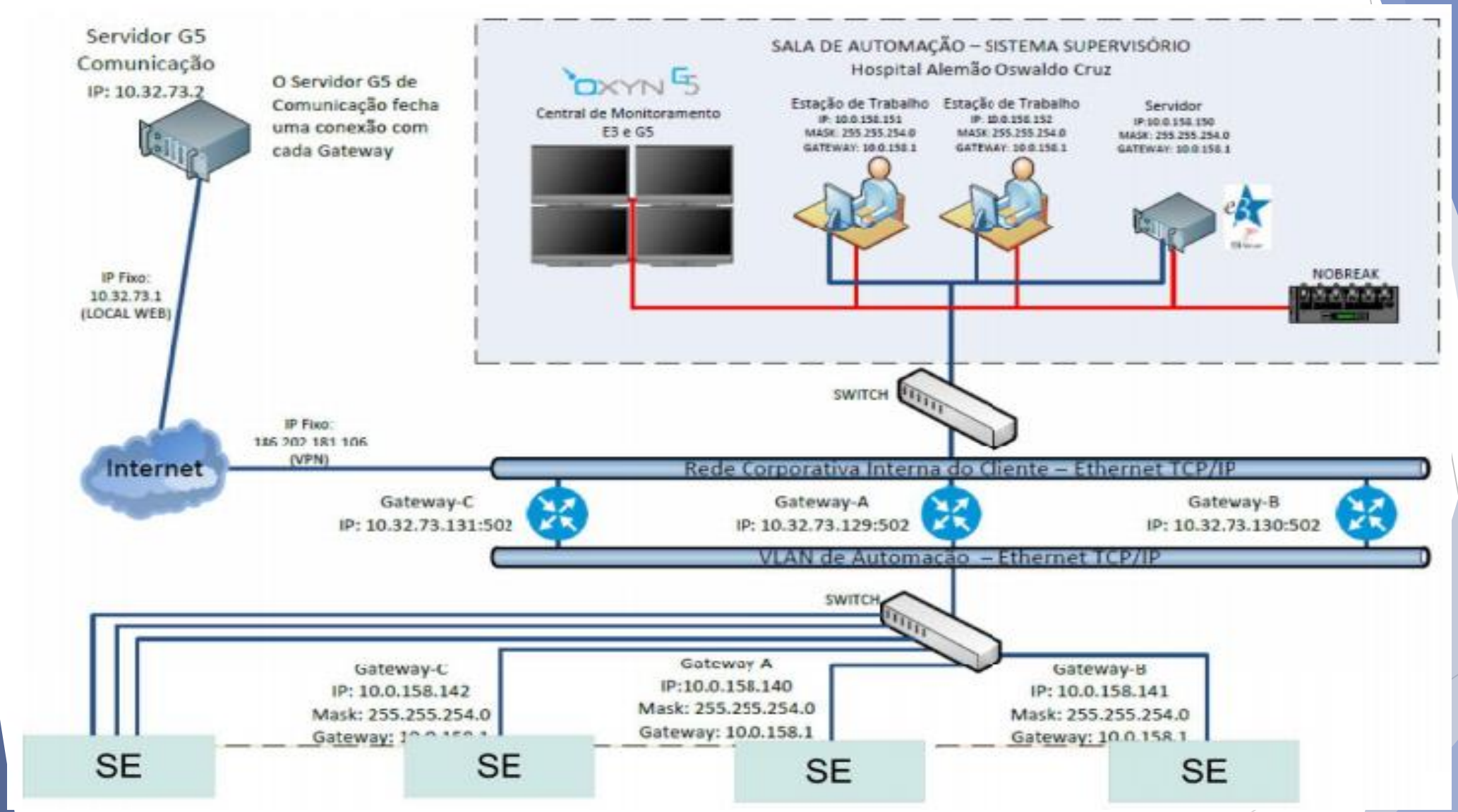


Gerenciamento de rede anel

Rede fibra entre blocos

Rede MMS/Goose entre IEDs

Gestão Analítica de Múltiplos Sites



Benefícios de um sistema integrado

- Acesso aos dados de forma rápida para tomada de Decisões;
- Rede com alta disponibilidade de Informação;
- Operação do Segura;
- Registro de Dados para Análise e geração de relatórios;
- Manutenção Padronizada o otimizada;
- Implantação de Load Sharing;
- Interoperabilidade;
- Tempo de retorno de energia em até 15s
- Equipamentos 100% monitorados com histórico para 4 meses

EDGE Group Mundial

- ✓ *A **EDGE Global Supply** é um grupo formado por **11 distribuidores independentes** de eletrica.*

- ✓ ***Os membros da EDGE coletivamente representam;***

+ US$ 4 BILHÕES

+ 4.600 COLABORADORES

+ 200 LOCALIDADES

II Encontro Técnico Transformação Digital no Setor de Energia

ISA Sao Paulo Section

AES Eletropaulo

Sobre a Ladder Automação | EDGE Group Brasil

✓ O ***Grupo EDGE Brasil*** *é constituído por* ***4 empresas que juntas somam mais de 25 anos de experiência no Mercado de Automação Industrial, Elétrica e Datacom.***

Ladder Automação Industrial

Distribuidor Automação Elétrica e Industrial

Mercado de atuação

- SP - Região Metropolitana
- Baixada Santista
- Vale do Paraiba
- Sorocaba
- Rio de Janeiro;

Intereng Automação Industrial

Distribuidor Automação Elétrica e Industrial

Mercado de atuação

- SP – Jaboticabal / Americana / Bauru
- Mato Grosso do Sul
- Sul de Minas Gerais

Laax Tecnologia de Informação

Distribuidor de Soluções Elétricas e Datacom

Mercado de atuação

- São Paulo
- Rio de Janeiro
- Mato Grosso do Sul
- Sul de Minas

Inbox Painéis Elétricos

Especialista na industrialização de painéis elétricos de baixa e média tensão

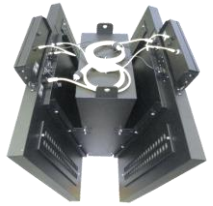
Mercado de atuação

- São Paulo
- Rio de Janeiro
- Mato Grosso do Sul
- Sul de Minas

Soluções Ladder Automação | EDGE Group

PLCs e IHMs para aplicações complexas


Telas com PC embarcado industriais 8” até 90”


Alicates amperímetors e Multímetros

PLCs e IHMs para aplicações de médio porte


PLCs e IHMs para pequenas aplicações


Supervisórios, coleta de dados via Web


FactoryTalk

Componentes e Safety (NR12/NR10)

Switches Ly2/Ly3, Gateways, Wi-fi, Rádio I/O e GSM



Acionamentos com até Frame 8


Virtualização e Cloud


II Encontro Técnico
Transformação Digital
no Setor de Energia

ISA Sao Paulo Section

II Encontro Técnico ISA São Paulo na AES Eletropaulo
Transformação Digital no Setor de Energia

1° de setembro de 2017 - Barueri / SP

Perguntas

Ricardo Afonso

ricardoafonso@ladder.com.br

+55 1199135-0275

II Encontro Técnico Transformação Digital no Setor de Energia

ISA Sao Paulo Section

AES Eletropaulo