TI Safe

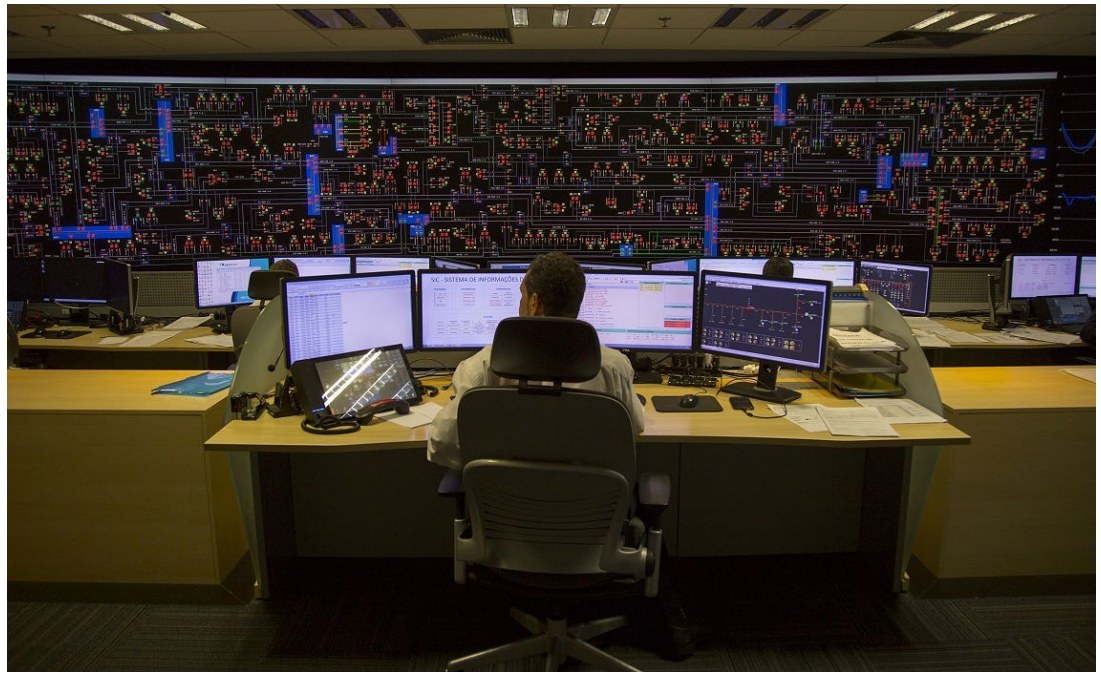
Segurança Cibernética no Setor Elétrico

Webinar GESEL, Março de 2021

© 2007-2021 – TI Safe Segurança Cibernética Industrial
Todos os direitos reservados

Desafios do setor de energia

- Concessionárias de energia enfrentam grandes desafios na busca por maior eficiência dos processos e melhoria da qualidade de fornecimento.
- O monitoramento da qualidade e do controle da geração, transmissão e distribuição de energia elétrica são processos importantes, e totalmente automatizados.
- A transformação digital é necessária e urgente
- E para piorar, estamos no meio de uma pandemia, com empresas inteiras fazendo Home Office



© 2007-2021 – TI Safe Segurança Cibernética Industrial
Todos os direitos reservados

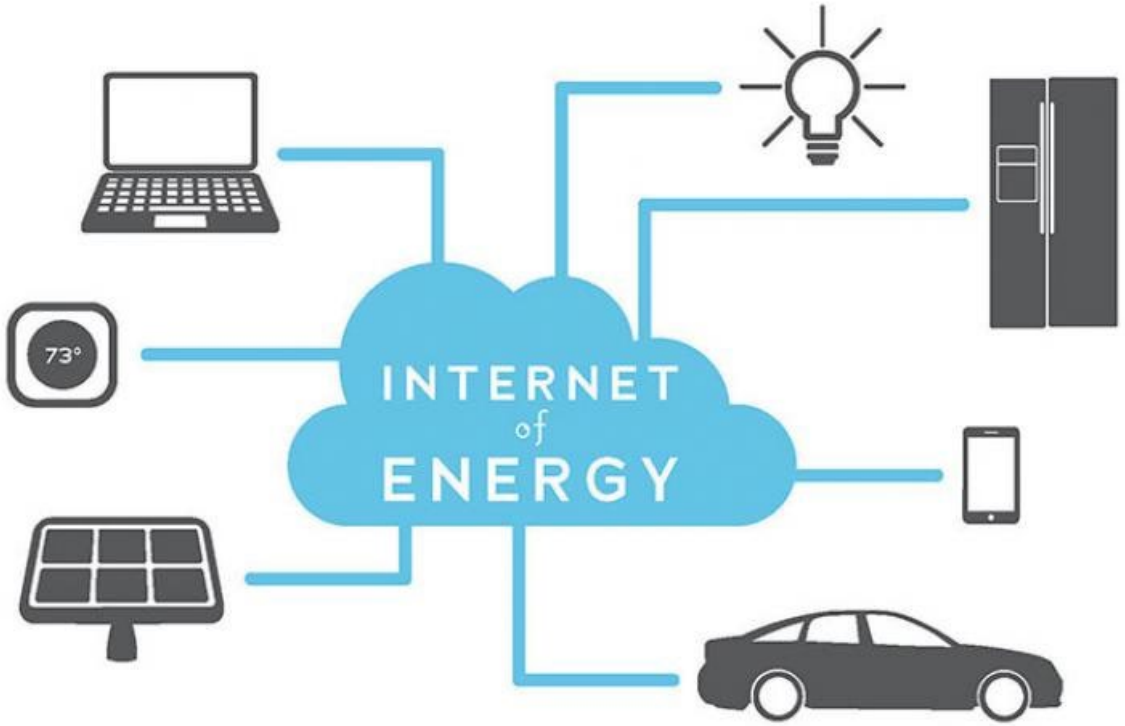
Digitalização de redes de energia

- A digitalização é pré-requisito para a Indústria 4.0 em redes de energia.
- Ela possibilita otimizar processos , aumentar eficiência e produtividade, antecipar riscos e falhas e, assim, resultar em decisões mais inteligentes.
- A digitalização do setor elétrico representa inovação e ganho de produtividade.
- A digitalização permite a integração de diferentes fontes de energia renováveis em uma malha energética única e interligada, capaz de suprir de forma sustentável, as demandas de cidades e indústrias.

© 2007-2021 – TI Safe Segurança Cibernética Industrial
Todos os direitos reservados

IoE - IIoT em Redes de Energia (Internet of Energy)

- Internet de Energia (IoE) refere-se à modernização e automatização de infraestruturas de eletricidade para produtores de energia.
- Isso permite que a produção de energia avance de forma mais eficiente e limpa com a menor quantidade de resíduos.
- Um exemplo da tecnologia IoE inclui a utilização de sensores inteligentes, comuns entre outras aplicações da tecnologia IoT, que permitem a mecânica facilitada pela IoE, como monitoramento de energia, armazenamento distribuído e integração de energia renovável.

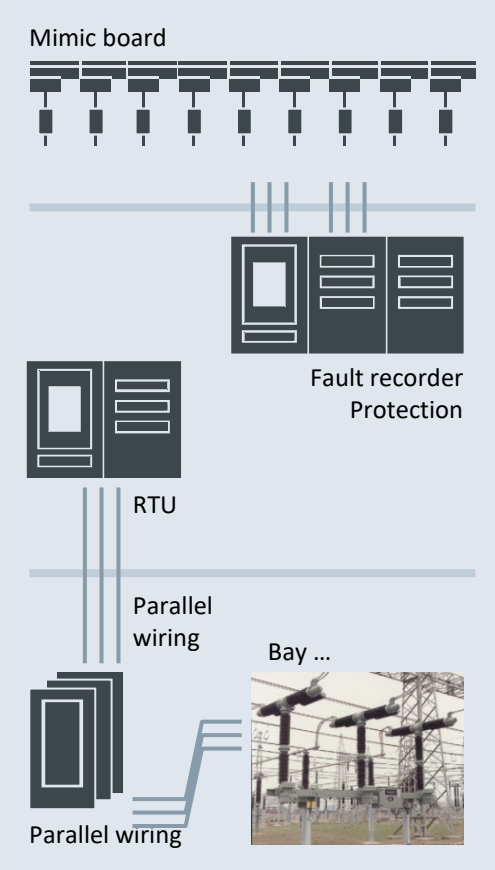


© 2007-2021 – TI Safe Segurança Cibernética Industrial
Todos os direitos reservados

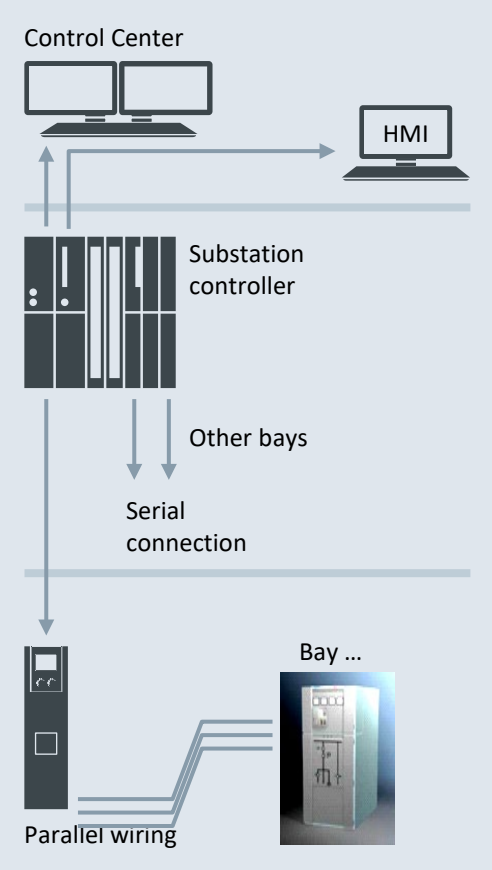
Subestação Digital 4.0

Evolução das Subestações de Energia

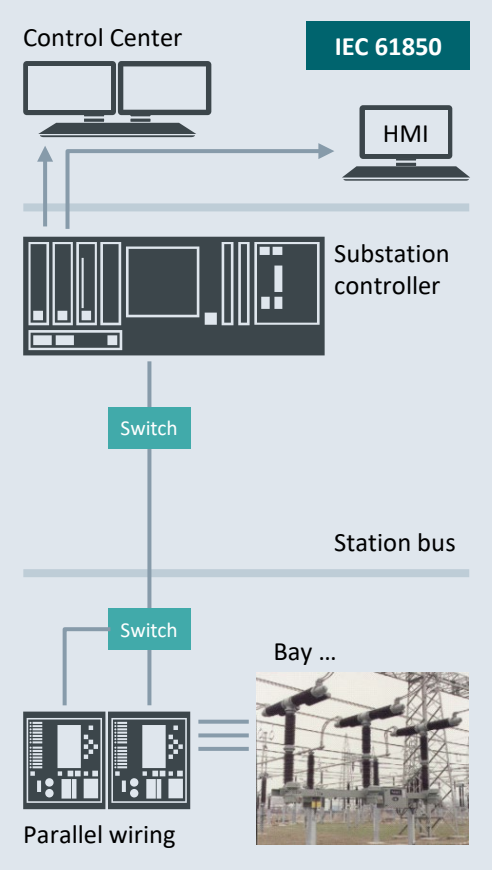
1st generation – Standard cabling



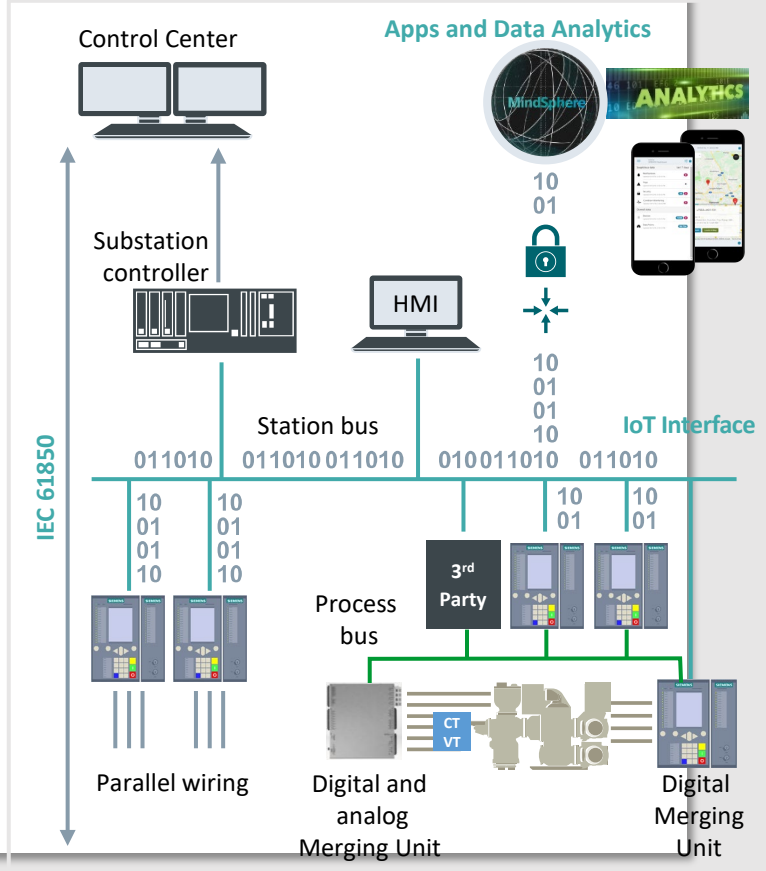
2nd generation – Point- to-point connections since 1985



3rd generation – Digital Station bus since 2004



Digital Substation 4.0 - Process bus and IoT Connectivity



TI Safe

© 2007-2021 – TI Safe Segurança Cibernética Industrial
Todos os direitos reservados

www.tisafe.com

Subestações digitais inteligentes

- A digitalização de subestações tem arquitetura baseada no padrão IEC 61850
- A digitalização converte dados provenientes de equipamentos primários na subestação – como transformadores de corrente, transformadores de tensão, disjuntores, chaves e transformadores de potência para proteções digitais por valores de amostra e mensagens GOOSE
- Todos os sinais são transmitidos através de fibra ótica, eliminando completamente o uso de cabos metálicos e reduzindo o risco de acidentes fatais causados por choques elétricos e circuitos abertos em transformadores de corrente, o que pode reduzir custos de infraestrutura e manutenção na subestação.

© 2007-2021 – TI Safe Segurança Cibernética Industrial
Todos os direitos reservados

E se uma subestação digital tiver seu **funcionamento comprometido** por um cyber ataque?

© 2007-2021 – TI Safe Segurança Cibernética Industrial
Todos os direitos reservados

Lembram disso?

G1 AMAPÁ REDE AMAZÔNICA

Após 22 dias de apagão no Amapá, distribuidora e governo dizem que rodízio terminou e que energia foi retomada em 100%

Segundo transformador entrou em operação nesta terça-feira (24), três semanas após incêndio atingir a principal subestação do estado.

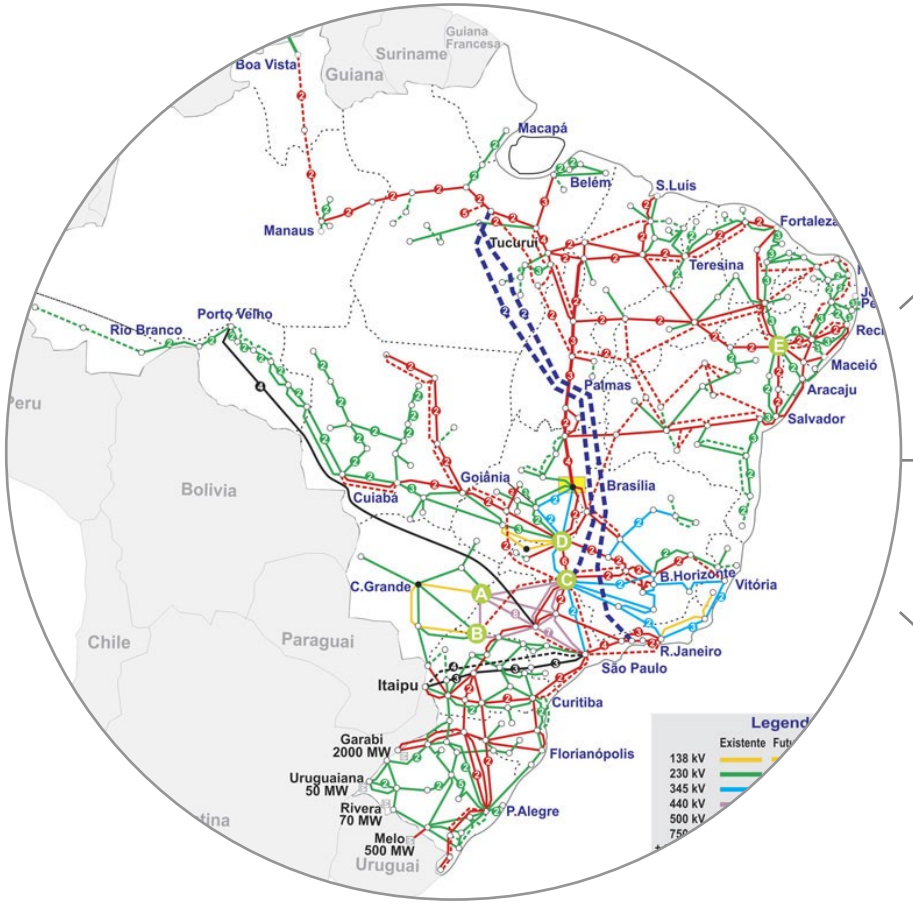
Por G1 AP — Macapá

© 2007-2021 – TI Safe Segurança Cibernética Industrial
Todos os direitos reservados

Por causa de apenas uma subestação, um estado inteiro ficou sem energia

© 2007-2021 – TI Safe Segurança Cibernética Industrial
Todos os direitos reservados

Sistemas Interligados – Desligamentos em cadeia



- Geração e distribuição integrados
- Caminhos críticos em poucas subestações
- Exploração de vulnerabilidades podem levar a blackouts

© 2007-2021 – TI Safe Segurança Cibernética Industrial
Todos os direitos reservados

Diferença das consequências entre um ataque cibernético na TI e na TA

- **ATAQUE À REDE DE T.I. DE ENERGIA**
  - Perda de serviços básicos de sistemas internos
  - Perda de bases de dados necessárias para o faturamento
  - Danos à imagem da empresa
  - Comunicação à CVM, o que impacta as ações na bolsa
  - Prejuízos imediatos com empresas terceiras para a recuperação do ambiente operativo

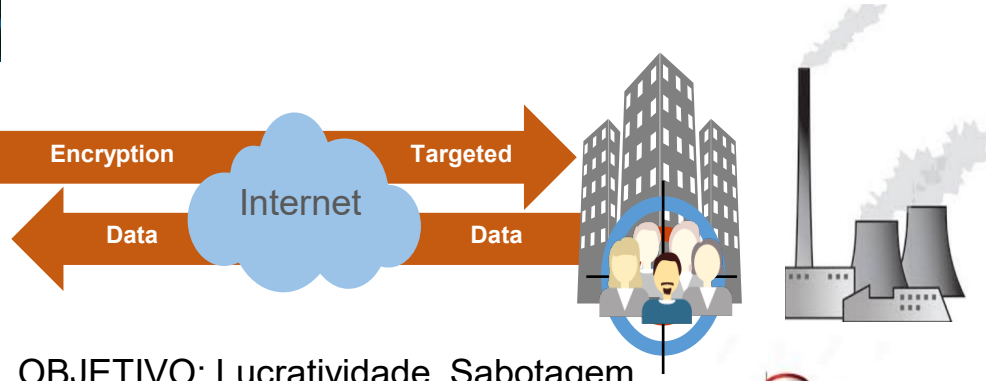
- **ATAQUE ÀS REDES OPERATIVAS (T.A.)**
  - Afeta diretamente com o core business da Empresa, que é o fornecimento de E.E.
  - Blecaute de energia para a POPULAÇÃO
  - Recuperação do ambiente de automação é MUITO MAIS COMPLEXA que a recuperação do ambiente de TI
  - Prejuízo imediato inestimável, cassação da concessão e possível intervenção do Governo Federal.
  - Queda no valor das ações e liquidez da empresa

© 2007-2021 – TI Safe Segurança Cibernética Industrial
Todos os direitos reservados

Ameaças mudaram: Ataques avançados

OBJETIVO: Notoriedade

- Uma pessoa, grupos pequenos
- Conhecimento e Recursos limitados
- Ataques básicos



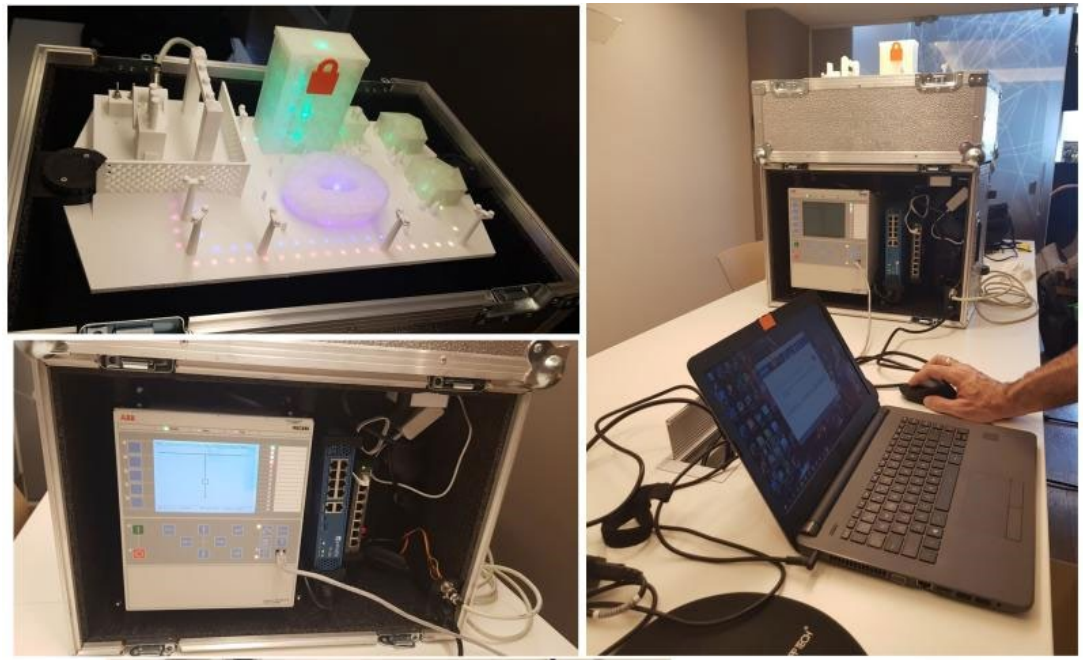
OBJETIVO: Lucratividade, Sabotagem e conflitos entre nações

- Organizados
- Ataques direcionados - Ransomware
- Financiado – Industria foco crescente

© 2007-2021 – TI Safe Segurança Cibernética Industrial
Todos os direitos reservados

Laboratório – Simulador de Subestação de E.E.

- Desenvolvido pela TI Safe em parceria com a ABB
- Simulador usado pela TI Safe em sua academia e também para apresentação em eventos e congressos
- Será usado pela primeira vez em público no CLASS 2021, Dezembro em Curitiba
- **www.class.tisafe.com**

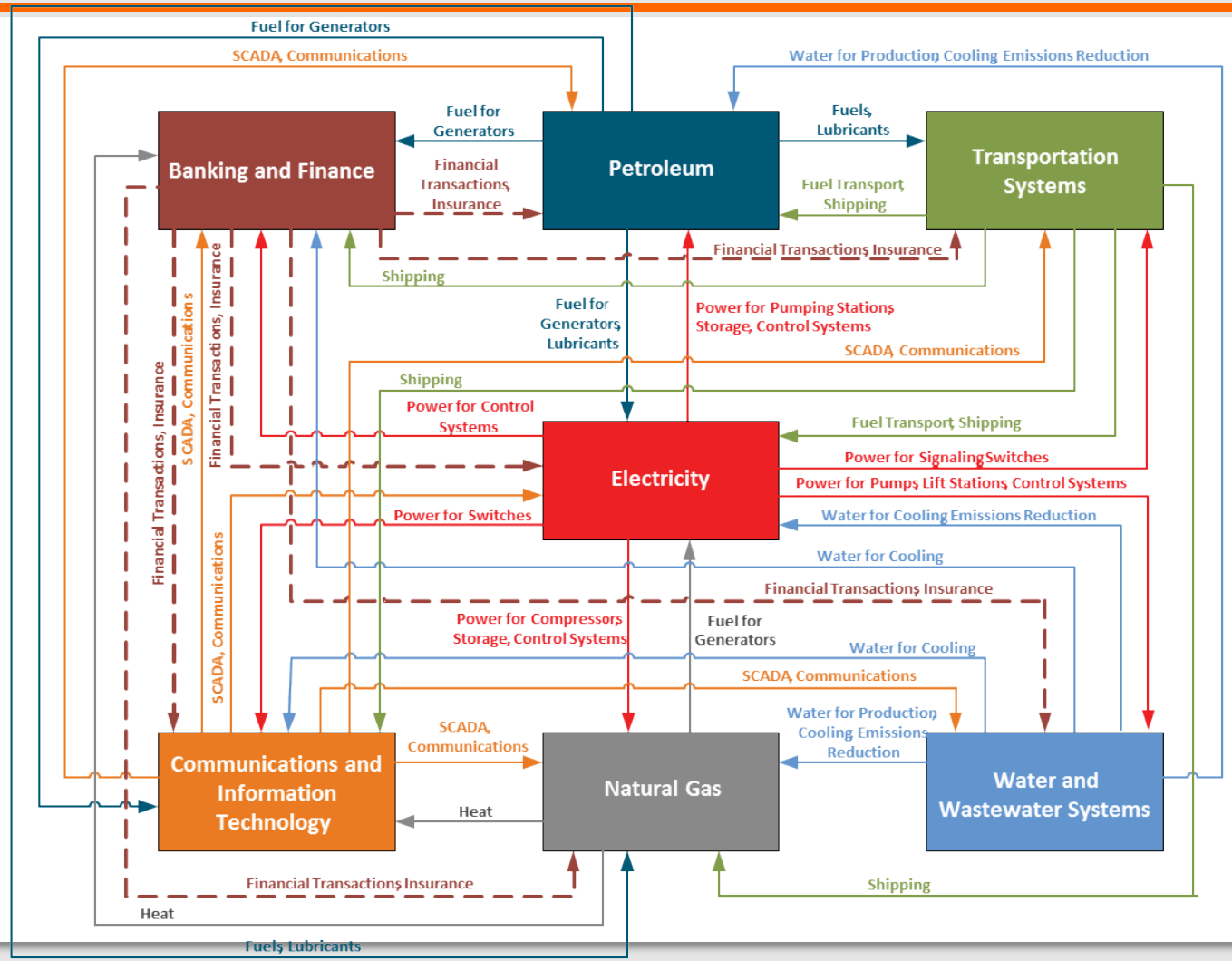


© 2007-2021 – TI Safe Segurança Cibernética Industrial
Todos os direitos reservados

A Transformação digital no setor elétrico sem segurança cibernética pode se transformar em um **desastre** num piscar de olhos!

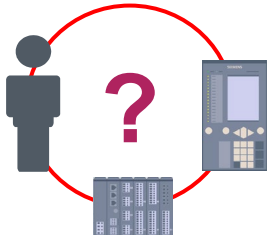
© 2007-2021 – TI Safe Segurança Cibernética Industrial
Todos os direitos reservados

A Eletricidade é o núcleo da infraestrutura crítica



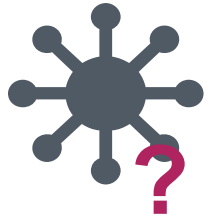
© 2007-2021 – TI Safe Segurança Cibernética Industrial
Todos os direitos reservados

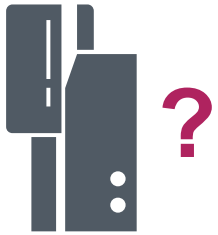
Os desafios de proteção em sistemas digitalizados



Quais são os ativos da minha rede?

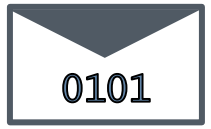
Posso confiar no software e firmware do ambiente de TO?





Quem e o quê tem acesso à TO?

Posso depender dos dados de processo?



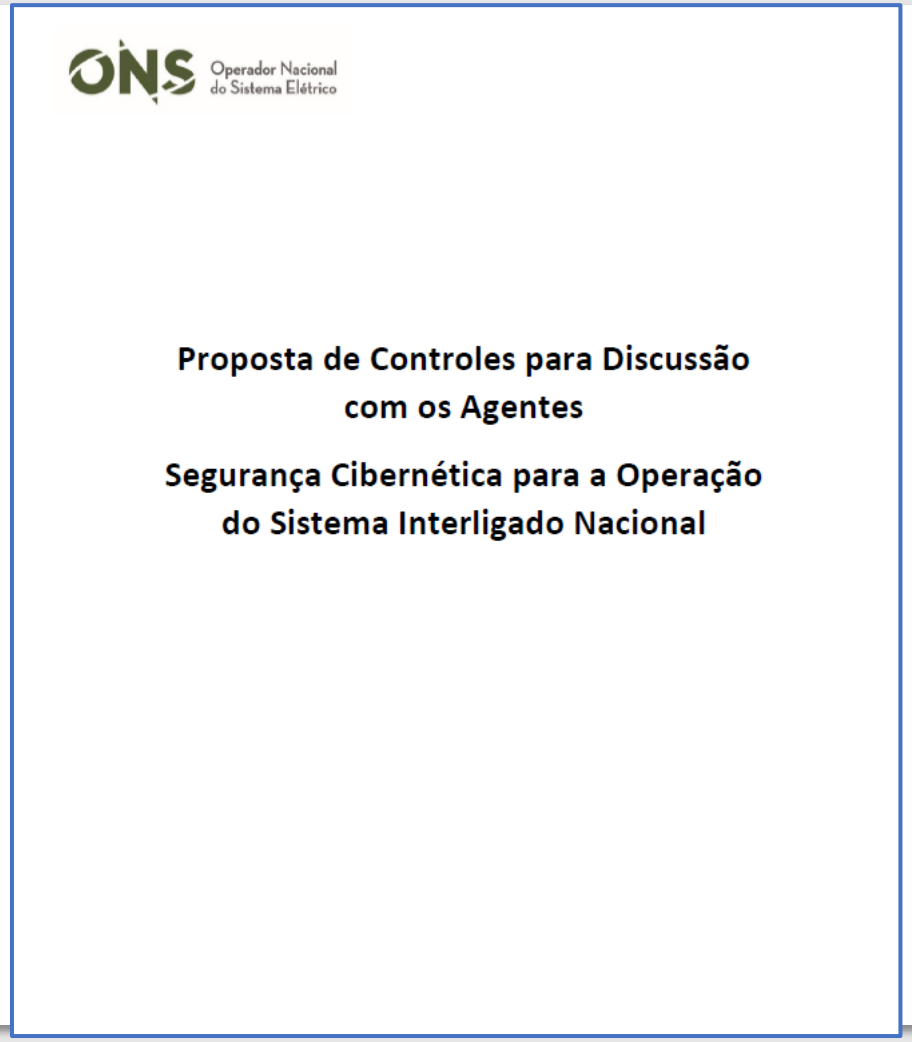
Posso confiar na minha rede de processos e no acesso remoto ao sistema?

Os parâmetros da minha rede de operação estão intactos e configurados corretamente?

© 2007-2021 – TI Safe Segurança Cibernética Industrial
Todos os direitos reservados

O novo procedimento de rede do ONS

- Objetivo: Estabelecer os controles de segurança cibernética a serem implementados pelos agentes de operação conectados à rede de supervisão e pelo ONS em seus ambientes operativos.
- Plano de 3 anos com 3 ondas de implantação (18, 24 e 36 meses).
- O tempo de implantação passa a contar da sua data de publicação.
- Este procedimento vai obrigar as empresas de energia a implantar segurança cibernética em suas redes de OT em tempo recorde.


ONS Operador Nacional do Sistema Elétrico

Proposta de Controles para Discussão com os Agentes

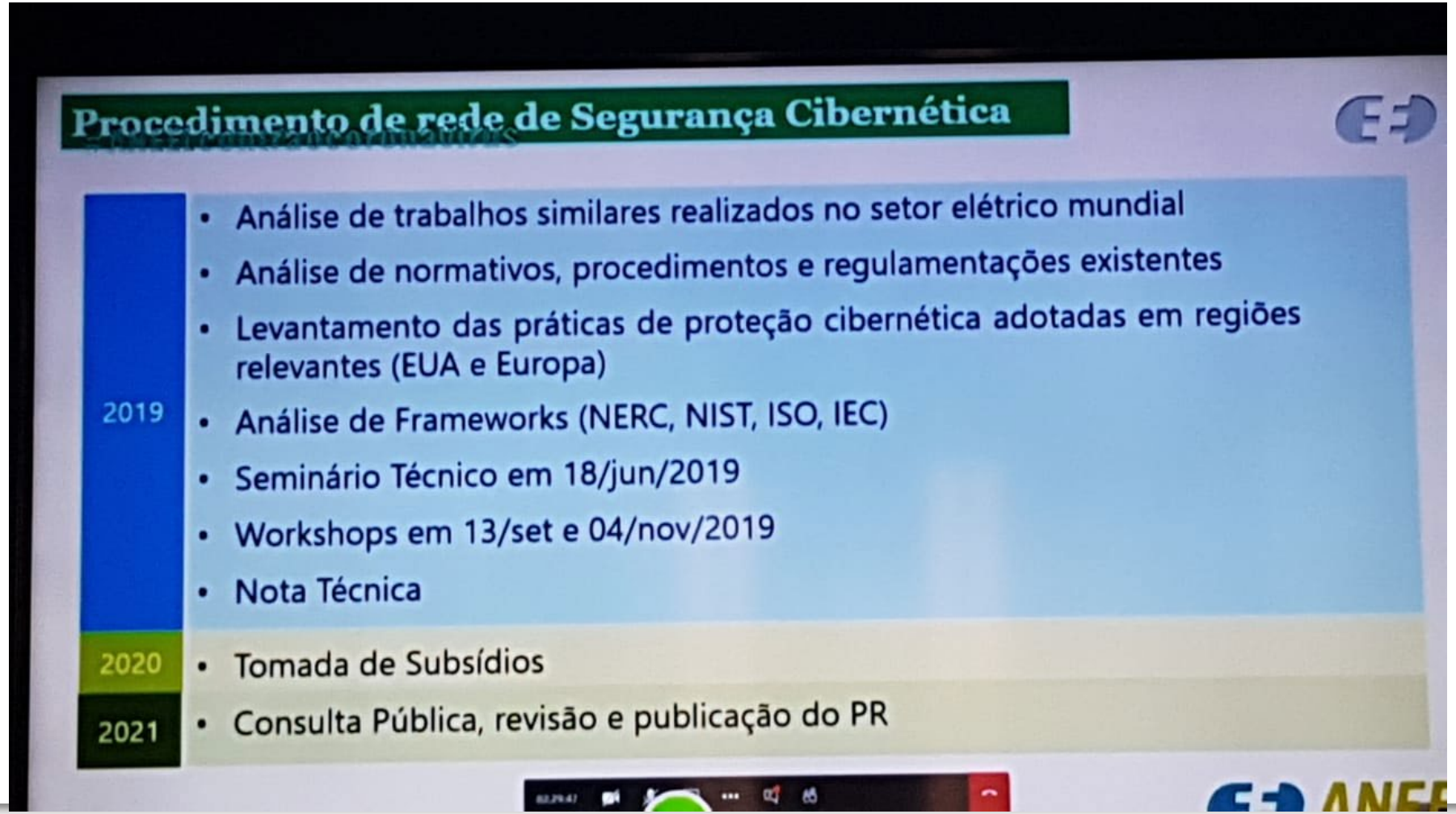
Segurança Cibernética para a Operação do Sistema Interligado Nacional

© 2007-2021 – TI Safe Segurança Cibernética Industrial
Todos os direitos reservados

Visão geral do Procedimento de Rede proposto pelo ONS

© 2007-2021 – TI Safe Segurança Cibernética Industrial
Todos os direitos reservados

Quando deve ser publicado?



© 2007-2021 – TI Safe Segurança Cibernética Industrial
Todos os direitos reservados

Chamada para consulta pública da ANEEL

ANEEL
AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA

Acesso à Informação | Sala de imprensa | Fale conosco

A ANEEL | SERVIÇOS | ESPAÇO DO CONSUMIDOR | INFORMAÇÕES TÉCNICAS | PARTICIPAÇÃO SOCIAL | TARIFAS

Agência Nacional de Energia Elétrica / Sala de Imprensa / Segurança cibernética no setor elétrico é tema de consulta pública

Imprimir

Segurança cibernética no setor elétrico é tema de consulta pública

Autor: AID
Publicação: 09/03/2021 | 12:49
Última modificação: 09/03/2021 | 12:55

Tweetar
Recomendar 0

A Agência Nacional de Energia Elétrica – ANEEL abrirá nesta quinta-feira (11/3) a Consulta Pública nº 007/2021, que visa a estabelecer um diálogo com a sociedade a respeito da Análise de Impacto Regulatório (AIR) sobre segurança cibernética no setor elétrico, de modo a minimizar os impactos de incidentes do gênero no funcionamento do setor elétrico.

© 2007-2021 – TI Safe Segurança Cibernética Industrial
Todos os direitos reservados

Notem que:

Durante a deliberação acerca da consulta, a Diretora da ANEEL também determinou que as áreas de fiscalização da Agência realizem uma verificação nos centros de operação dos agentes da rede de operação do ONS, para verificação do cumprimento do requisito de segurança cibernética estabelecido nos Procedimentos de Rede, e apresentem um panorama do resultado em até 120 dias. Também foi recomendado que o ONS estabeleça um documento operativo com as orientações ou critérios para definir a política de segurança e os recursos tecnológicos para proteção contra ataques cibernéticos na rede de supervisão e controle dos centros de operação. “Nos colocamos à disposição, por meio de nossas áreas técnicas, para construir com o ONS essa nova rotina para uma melhor segurança cibernética”, ofereceu o diretor Sandoval Feitosa, que incentivou ainda a realização, por parte da fiscalização da ANEEL, de uma campanha de verificação das providências que estão sendo tomadas pelos agentes para assegurar a proteção de seus sistemas e instalações contra ataques cibernéticos.

O estudo da ANEEL sobre segurança cibernética foi iniciado quando o Operador Nacional do Sistema (ONS) encaminhou à ANEEL, no final de 2019, uma proposta de submódulo dos Procedimentos de Rede que abrange os agentes do Ambiente Regulado Cibernético (ARCiber). A partir dessa interlocução, foram empreendidas em 2020 as providências para o tratamento desse risco regulatório, com base no Decreto nº 9.637/2018, que instituiu a Política Nacional de Segurança da Informação, e no Decreto nº 10.222/2020, que aprovou a Estratégia Nacional de Segurança Cibernética. A ANEEL promoveu a Tomada de Subsídio nº 007/2020 e, em seguida, um estudo interno para análise da questão por meio da abordagem inovadora de Design Thinking. Também foram pesquisadas as melhores práticas aplicadas por instituições públicas no Brasil e no exterior.

A Consulta Pública nº 007/2021 estará disponível para contribuições entre 11/3 e 26/4/2021, por meio de formulário eletrônico na página da ANEEL na internet (www.aneel.gov.br/consultas-publicas), no espaço da Consulta Pública nº 007/2021. O relatório da AIR e demais documentos também estarão na mesma página.

© 2007-2021 – TI Safe Segurança Cibernética Industrial
Todos os direitos reservados

Marcelo Branquinho

marcelo@tisafe.com

© 2007-2021 – TI Safe Segurança Cibernética Industrial
Todos os direitos reservados