XXVII Seminário Nacional de

Produção e Transmissão de Energia Elétrica

UMA VISÃO SISTEMÁTICA DA RESILIÊNCIA DAS REDES DE COMUNICAÇÃO OPERATIVA UTILIZADAS NO SEP, SUAS VULNERABILIDADES E MÉTODOS DE PROTEÇÃO E MITIGAÇÃO FRENTE A ATAQUES CIBERNÉTICOS

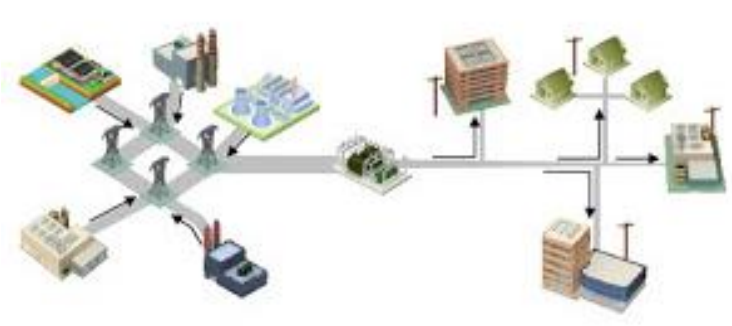
Informe Técnico GTL - 0378

Leonardo Henrique de Melo Leite

FITec
Inovações Tecnológicas

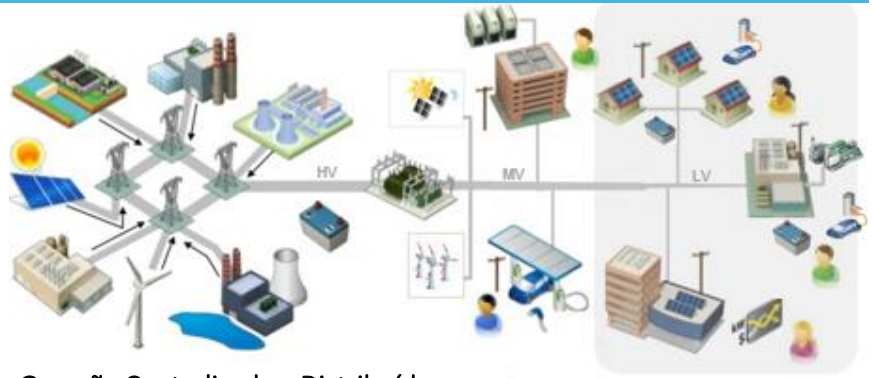
Sistema Elétrico de Potência em Transição

Do legado da grande rede…



- ✓ Geração centralizada
- ✓ Topologia Radial
- ✓ Controle de Fluxo de Energia Unidirecional
- ✓ Comunicação Unidirecional (quando existente)
- ✓ Poucos Sensores Distribuídos
- ✓ Estabilidade da rede baseada em inércia das fontes de geração
- ✓ Regulação estável
- ✓ Consumidores passivos, sem interação com o provedor de serviço de energia

… à rede em transição (*Smart Grids*)



- ✓ Geração Centralizada e Distribuída
- ✓ Topologia em Rede
- ✓ Controle de Fluxo de Energia Bidirecional
- ✓ Comunicação Bidirecional
- ✓ Múltiplos Sensores/Atuadores Distribuídos na Rede de Energia
- ✓ Fontes de Energia Variáveis e Problemas de estabilidade
- ✓ Novos agentes e interessados: agregadores, prossumidores, microrrefes, Usinas Vituais...
- ✓ Consumidores ativos e comprometidos: GD, VE, Storage, resposta à demanda, consumidor cativo x consumidor livre

Fonte: Scheider/FITec – SmartGrid Forum 13ª. Edição

Sistema Elétrico em Transição

Aumento Expressivo de Recursos Energéticos Distribuídos

- ✓ Fontes de Geração Distribuída
  - ✓ Solar
  - ✓ Eólica
  - ✓ CGH
  - ✓ Termoelétrica
- ✓ Sistemas de Armazenamento de Energia Elétrica
- ✓ Veículos Elétricos Plug in e estrutura de recarga
- ✓ Gerenciamento pelo Lado da Demanda
- ✓ Eficiência Energética

Segurança Cibernética no SEP

Maior Flexibilidade.....

Aumento da Superfície de Ataques Cibernéticos no SEP

Uso Intensivo de Infraestrutura de TIC e Digitalização

Múltiplos dispositivos IoT e Sensores Dispersos no Grid

Elevada Conectividade – Infraestrutura de Telecomunicações Pública x Privada

Protocolos de Comunicação Padronizados e Interoperabilidade

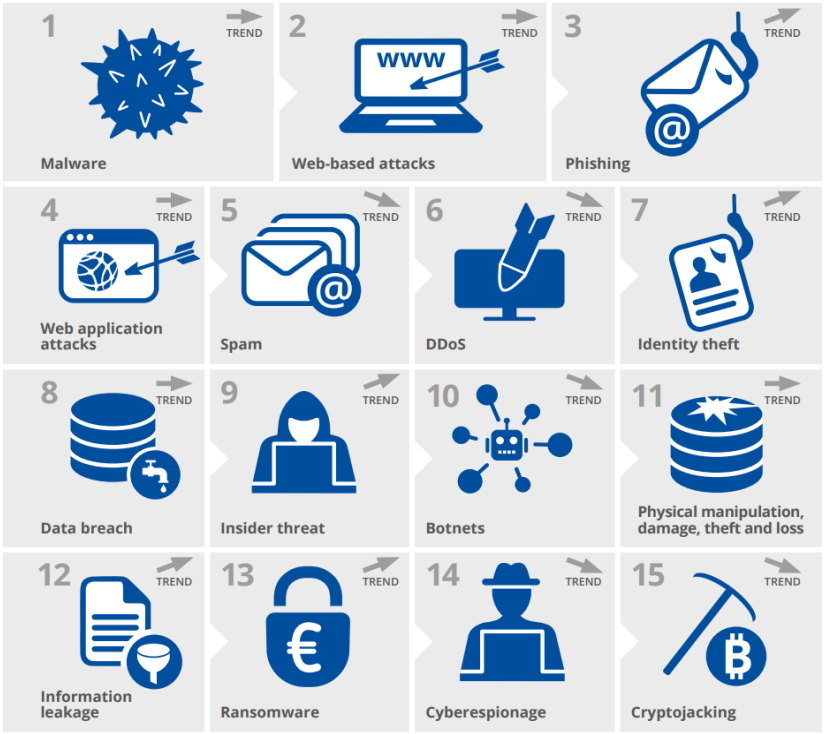
Aplicações em Nuvem

Recursos Energéticos Distribuídos on Grid

Segurança Cibernética no SEP

As principais Ciber-ameaças e Técnicas de Segurança para o SEP

Principais ameaças cibernéticas



Fonte: ENISA

Técnicas de Segurança

- Pré- Processamento
- Aprendizado de Máquina Convencional e Profundo
- Aprendizado por Esforço
- Blockchain
- Criptografia
- Grafo

Segurança Cibernética no SEP

Soluções de Segurança Cibernética frente x Tipos de Ataques Cibernéticos

Ataques Cibernéticos no SEP	Técnicas de Segurança Cibernética para o SEP						
	Pré-processamento	AM profundo	AM convencional	Aprendizado por reforço	Blockchain	Criptografia	Grafo
Ransomware	X	X					
SPAM	X	X	X				
Vulnerabilidades				X	X		
Roubo de Dados					X	X	
Botnet	X	X	X				X
Cryptojacking	X	X	X				
DDoS	X	X	X				X
Manipulação física		X	X				
Replay attack		X	X				
Data Exfiltration			X				

Segurança Cibernética no SEP

CSIS - Center for Strategic and International Studies

Incidentes de segurança cibernética na Infraestrutura de Energia Elétrica

https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

2021 - India – Hackers penetration on Grid Operators in India

2020 – Japão - Large-scale cyber-attack against Mitsubishi Electric

2019 – EUA - Hacking group with suspected Russian ties was conducting reconnaissance into the networks of electrical utilities.

2019 – EUA. Chinese hackers stole General Electric's trade secrets concerning jet engine turbine Technologies

2018 – EUA - hacking against organizations including FIFA, Westinghouse Electric Company and the U.S. and World Anti-Doping Agencies.

2018 – Reino Unido - Attack on ICS networks of electric utilities in the UK

2017 - Schneider Electric - Shut down operations of a power plant in the Middle East

Segurança Cibernética no SEP

Registros Públicos de Ataques Cibernéticos no SEP Brasileiro

• Mai/2017 • *Ransomware WannaCry* • Sites	• Mai/2020 • *Ransomware* • Site e portal do cliente	• Mai/2020 • Ransomware Maze • Dados de contratos	• Jun/2020 • Malware • SAC	• Dez/2020 • Ransomware *Kitty* • SAC, site e app
COSERN	Light	CPFL	Energisa	CEMIG

• Mar/2021 • Malware • App e arquivos	• Fev/2021 • Malware • SAC e site	• Fev/2021 • *Ransomware* • *Servidores da rede admin.*	• Jan/2023 • Ataques físicos • Linhas de transmissão
CELG	COPEL	Eletronuclear	MME*

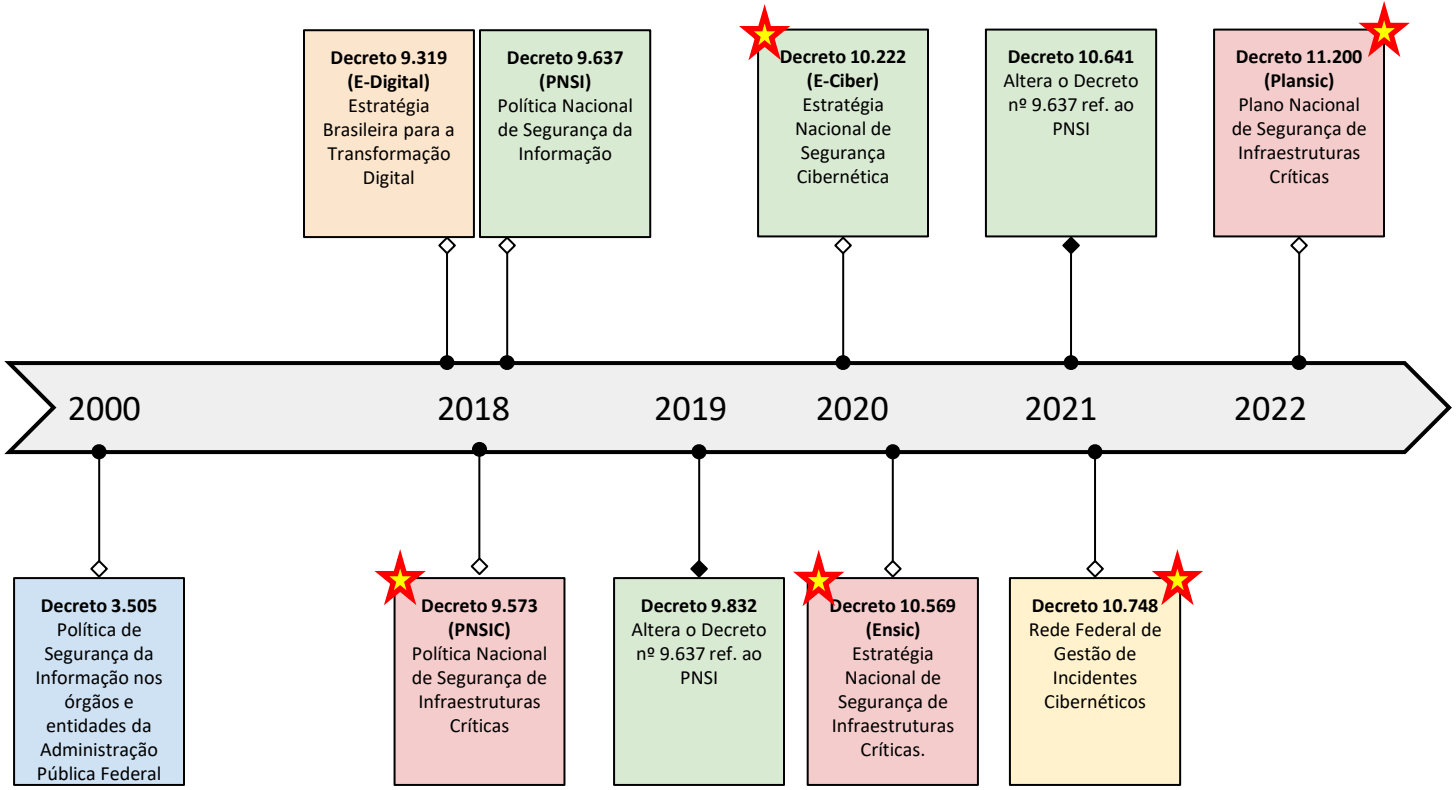
Segurança Cibernética no SEP -

Principais Frameworks, Diretrizes e Práticas Internacionais

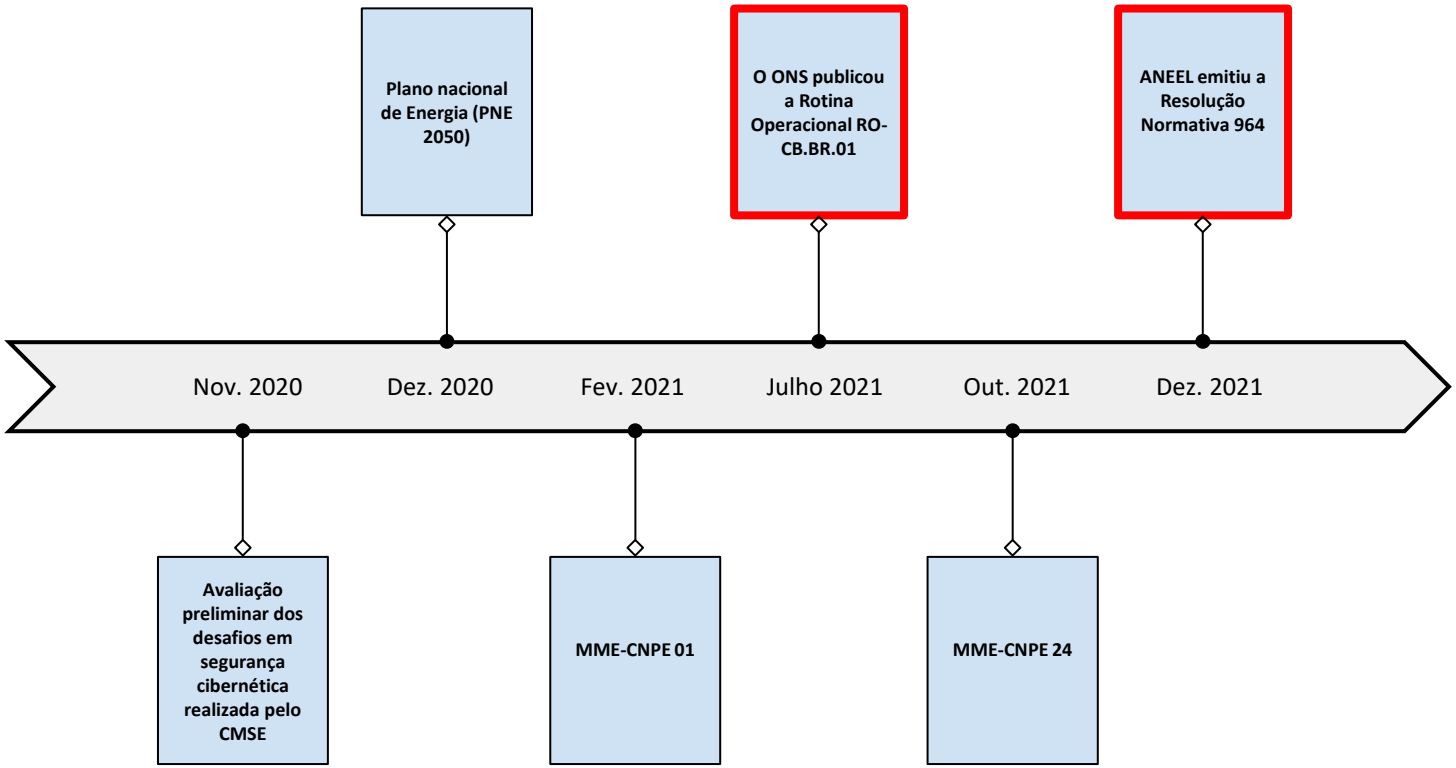
- National Institute of Standards and Technology
- North American Electric Reliability Corporation
- European Union Agency for Cybersecurity
- International Society of Automation
- US Department of Homeland Security
- International Organization for Standardization
- American National Standards Institute
- International Electrotechnical Commission
- Institute of Electrical and Electronics Engineers

Governança da Segurança Cibernética no Brasil

Decretos que instituem as políticas e estratégias sobre segurança da informação



Estruturação da Segurança Cibernética no Setor Elétrico



Estruturação da Segurança Cibernética no Setor Elétrico Brasileiro

ONS Operador Nacional do Sistema Elétrico

Manual de Procedimentos da Operação

Módulo 5 - Submódulo 5.13

Rotina Operacional
Controles mínimos de segurança cibernética para o Ambiente Regulado Cibernético

Código	Revisão	Item	Vigência
RO-CB.BR.01	01	4.1.11.	01/08/2022

MOTIVO DA REVISÃO

- Revisão textual ao longo do documento.

LISTA DE DISTRIBUIÇÃO

CNOS	COSR-SE	COSR-NE	COSR-NCO	COSR-S
Agentes de Operação	-	-	-	-

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 22/12/2021 | Edição: 240 | Seção: 1 | Página: 288

Órgão: Ministério de Minas e Energia/Agência Nacional de Energia Elétrica

RESOLUÇÃO NORMATIVA ANEEL Nº 964, DE 14 DE DEZEMBRO DE 2021

Dispõe sobre a política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica.

ABRATE

Framework de Segurança Cibernética

Força Tarefa Temporária de Segurança Cibernética

Tecnologias de Telecomunicações Aplicada às Funções Operativas do SEP

Tecnologias de Redes sem fio (Wireless)	Tecnologias de Redes com fio (Wireline)
▪ Rede Móvel Celular (GPRS, 3G, 4G/LTE, 5G) ▪ PMR – Private Mobile Radio ▪ WIMAX / WiMesh – Wireless Mesh Networks ▪ SATÉLITE ▪ LPWA (Low Power Wide Area) ○ LoRaWAN ○ NB-IoT ○ Wi-Sum ○ IEEE 802.11 ▪ WI-FI – Wireless Fidelity ▪ IEEE 802.15.4 ○ Zigbee	▪ Ethernet ▪ Rede Optica ○ PDH/SDH ○ EPON Ethernet over Passive Optical Network ○ GPON Gigabit-Ethernet Passive Optical Network ○ OTN Optical Transport Networking ○ WDM (Wave Division Multiplexing), DWDM (Dense WDM) e UDWDM (Ultra Dense WDM) PLC - Power Line Communication ○ NB-PLC ○ BB-PLC MPLS ○ MPLS-TP

Infraestruturas de Rede de Comunicação Operativa e Vulnerabilidades

Tecnologias de Telecomunicações Aplicada às Funções Operativas

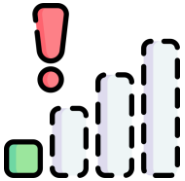
Funções de Automação	Tec. de comunicação s/ fio							Tecnologia de comunicação c/ fio			
	Rede Móvel Celular	PMR	WIMAX/ WiMesh	SATELITE	LPWA	Wi-Fi	Zigbee	Ethernet	Rede óptica	PLC	MPLS
Automação de Serviços de Campo											
Georeferenciamento de Elementos da Rede	x	x		x							
Despacho Remoto de Ordem de Serviço	x	x		x							
Envio de Arquivos (mapas, manuais, imagens)	x	x		x							
Priorização de Serviço	x	x		x							
Navegação/Roteirização	x	x		x							
Teleproteção de Linhas de Transmissão											
Proteção de Distância								x	x	x	x
Proteção Diferencial								x	x		x
Gerenciamento de Recursos Energéticos Distribuídos											
Medição de Fluxo de Potência	x	x	x					x	x		x
Comandos de Conexão e Desconexão	x	x	x					x	x		x
Parametrização de Inversores	x	x	x					x	x		x
Envio de set points de Potência Ativa e Reativa	x	x	x					x	x		x
Alteração do Fator de Potência	x	x	x					x	x		x

Funções de Automação	Tec. de comunicação s/ fio	Tecnologia de comunicação c/ fio
Automação de Rede		
Acesso remoto a IEDs (*Intelligent*		
Localização de Faltas, Isolação e F		
Análise de Contingência		
Controle de Tensão e Potência Rea		
Coordenação de Ações de Emergê		
Acesso Remoto a Oscilografia - IE		
Videomonitoramento		

Funções de Automação	Tec. de comunicação s/ fio	Tecnologia de comunicação c/ fio
Automação de Subestaç		
Bloqueio e Desbloqueio d		
Medição em Média Tens		
Controle de Tensão e Pot		
Reconfiguração de Subes		
Ajuste Remoto de Relés d		
Acesso Remoto a Oscilog		
Videomonitoramento		

Funções de Automação	Tec. de comunicação s/ fio	Tecnologia de comunicação c/ fio
Automação da Medição		
Automatic Meter Reading (A		
Automatic Meter Infrastruct		
Medição - Geração Distribu		
Informação de Perfil de Car		
Medição de Demanda de Pic		
Real Time Pricing (RTP)		
Time of Use (TOU)		
Pré-Pagamento de Energia		
Monitoração de Qualidade d		
Conexão e Desconexão Rem		
Detecção de Fraude		
Gerenciamento/Controle de Carga	x	
Detecção de Interrupção de Serviço	x	

Vulnerabilidades comuns em infraestruturas críticas em todo o mundo



Interferência e falta de proteção de sinal

Mensagens e *downlink* vulneráveis

Protocolos, funções e contadores inseguros

Autenticação falha ou fraca

Falta de proteção física

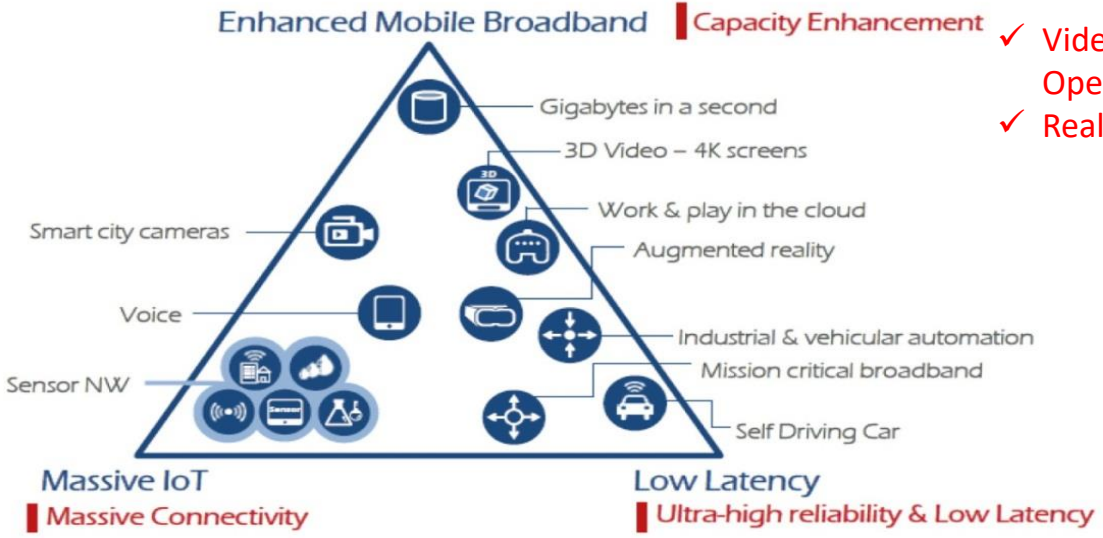
***Gateways* de acesso inseguro**

Falta de integridade

Imagens: flaticon.com

Infraestruturas de Rede de Comunicação Operativa para o SEP

Rede 5G potencialmente habilitadora para diferentes funções operativas do SEP - Medição e sensoriamento de múltiplos pontos e Serviços críticos que demandam baixa latência



- ✓ Videomonitoramento Operativo
- ✓ Realidade Aumentada

- ✓ Teleproteção Diferencial de alta confiabilidade
- ✓ Transferências de carga em situação de contingência
- ✓ PMU

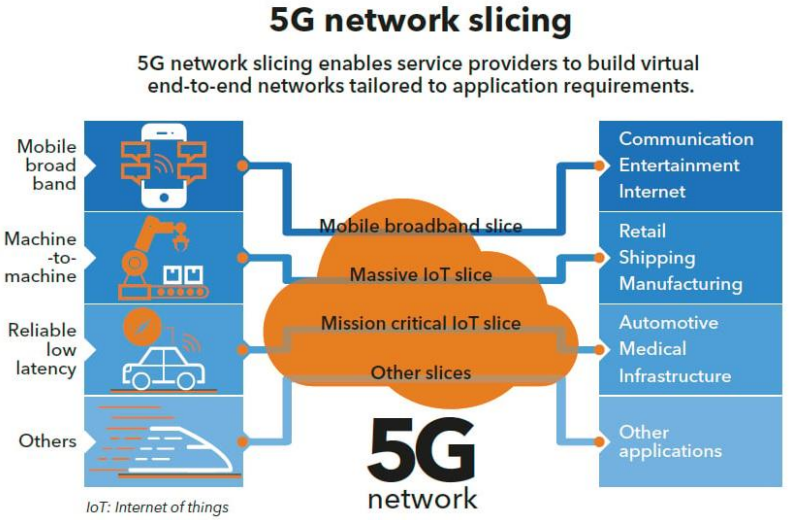
- ✓ AMI, Monitoramento de Ativos e Controle de Elementos de Rede

(Source: ETRI graphic, from ITU-R IMT 2020 requirements)

Avanços da Segurança Cibernética em Redes 5G

Isolamento de rede (*Network Slicing*)

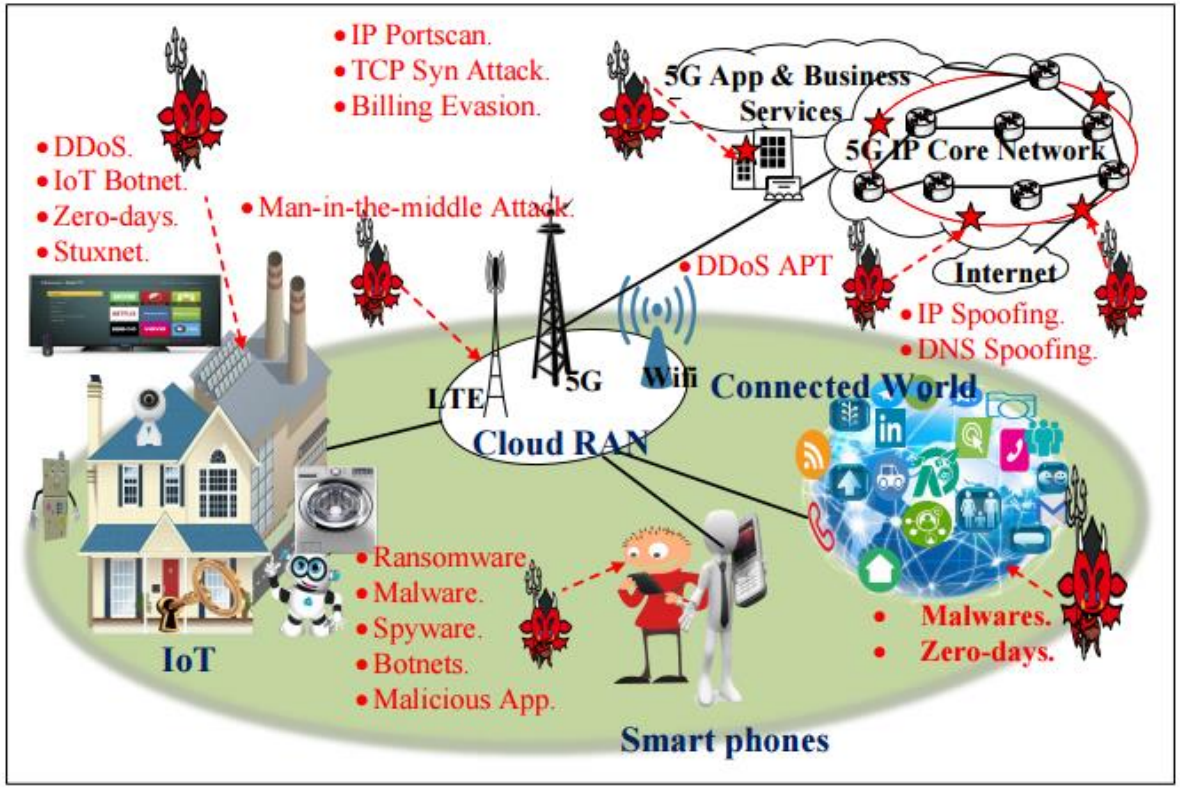
- **Isolamento Lógico**
  - ✓ Tráfego e recursos alocados por aplicação
  - ✓ Previsibilidade de desempenho por aplicação
  - ✓ Proteção contra interferências externas
- **Requisitos Personalizados**
  - ➢ Largura de banda
  - ➢ Latência
  - ➢ Confiabilidade
  - ➢ Segurança
  - ➢ Prioridade no tráfego
- **Alocação Dinâmica de Recursos**
  - ✓ Flexibilidade
  - ✓ Gerenciamento de tráfego
  - ✓ Adaptação em tempo real
  - ✓ Otimização de eficiência
  - ✓ Controle Centralizado



Fonte: https://www.sdxcentral.com/

Contudo, os dispositivos IoT conectados à rede 5G fabricados com segurança insuficiente e sem técnicas de criptografia são susceptíveis à ataques cibernéticos e podem comprometer segmentos importantes da infraestrutura

Cenário de ameaças à segurança 5G para vários ataques em IoT, smartphones, aplicaões em nuvem e mundo conectado



A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent dvancements and Future Directions, IEEE Communications Surveys & Tutorials · July 2019

Considerações Finais

- O **Sistema Elétrico de Potência** mundial encontra-se **em Transição**: **D**escarbonização, **D**escentralização, **D**igitalização e **D**emocratização. Oportunidades, novos modelos de negócios e desafios

- Aumento da **Digitalização**, **conectividade** e **interoperabilidade** no SEP. Consequentemente **aumento da superfície para ataques cibernéticos**

- **Frameworks e Normatização Internacionais** de Segurança Cibernética para infraestrutura de energia **em evolução**: NIST, NIS, C2M2, NERC CIP, ISO, ISA, IEC, IEEE...

- **Arcabouço regulatório e normativo de Segurança Cibernética no Brasil para o SEP é ainda incipiente**. Publicações recentes de controles de Segurança pelo ONS (ARCiber) e RES ANEEL 964

- **Redes de comunicação 5G podem ser habilitadoras para funções críticas no SEP**. É preciso endereçar controles de segurança fim a fim, inclusive nos dispositivos do Grid que se conectam à infraestrutura 5G

- A s**egurança cibernética é um investimento necessário** para um futuro energético seguro e confiável. Porém, **um longo caminho ainda precisa ser percorrido** para oferecer **soluções especializadas** para o contexto do setor elétrico.

Leonardo Henrique de Melo Leite

Obrigado !

(31) 98851-4215
lleite@fitec.org.br
www.fitec.org.br

FITec Inovações Tecnológicas

HUAWEI

UFMG UNIVERSIDADE FEDERAL DE MINAS GERAIS

Promoção

cigre Brasil

Coordenação

Eletrobras Eletronorte