Segurança Cibernética no Setor Elétrico

EDUARDO FAGUNDES

Segurança cibernética no setor elétrico

Autor: Prof. MSc. Eduardo Fagundes

O ataque hacker que a Eletronuclear sofreu em 7 de fevereiro de 2021, atingindo o seu sistema administrativo segundo fontes da empresa, abre novamente a discussão sobre a segurança cibernética – *Cyber Security* – no setor elétrico.

Ataques hackers planejados por organizações criminosas, terrorismo ou missões de guerra cibernética passam a ser cada vez mais frequentes. Um exemplo é o Stuxnet, um worm de computador (tipo de malware mais perigoso que um vírus comum, pois sua propagação é rápida e ocorre sem controle da vítima) projetado especificamente para atacar o sistema operacional SCADA desenvolvido pela Siemens, usado para controlar as centrífugas de enriquecimento de urânio iranianas, através da reprogramação dos Controladores Lógico Programáveis (CLP) do sistema. O Stuxnet pode estar camuflado em milhares de computadores, sendo inofensivo nos sistemas operacionais utilizados para funções comuns pessoais e comerciais. Entretanto, potencialmente perigoso se encontrar brechas na rede de comunicação para acesso a sistemas industriais e sistemas SCADA das empresas, incluindo as do setor elétrico.

Este artigo procura oferecer uma visão do momento atual da segurança da informação do setor elétrico no Brasil e frameworks de governança de segurança cibernética para monitoração, controle e respostas a incidentes.

Sistema Integrado Nacional (SIN)

O SIN (Sistema Integrado Nacional) é um ecossistema de geração e transmissão de energia elétrica no Brasil, constituído por geração hidro-termo-eólico de grande porte, de múltiplos proprietários, dividido em quatro subsistemas: Sul, Sudeste/Centro-Oeste, Nordeste e a maior parte da região Norte.

A interconexão das usinas de geração de energia é feita por uma malha de transmissão nacional, onde o despacho de energia de cada usina é definido pelo ONS (Operador Nacional do Sistema), buscando ganhos sinérgicos e explorando a diversidade entre os regimes hidrológicos das bacias. Por exemplo, em períodos secos, o sistema aciona as termelétricas, de custo maior, para suprir a parte da demanda de energia, preservando os níveis dos reservatórios das hidrelétricas e garantindo água para consumo humano.

O cálculo de despacho de energia é realizado através de complexos modelos matemáticos para assegurar o atendimento ao mercado com segurança e economicidade. Podemos observar a complexidade do SIN na figura 1.

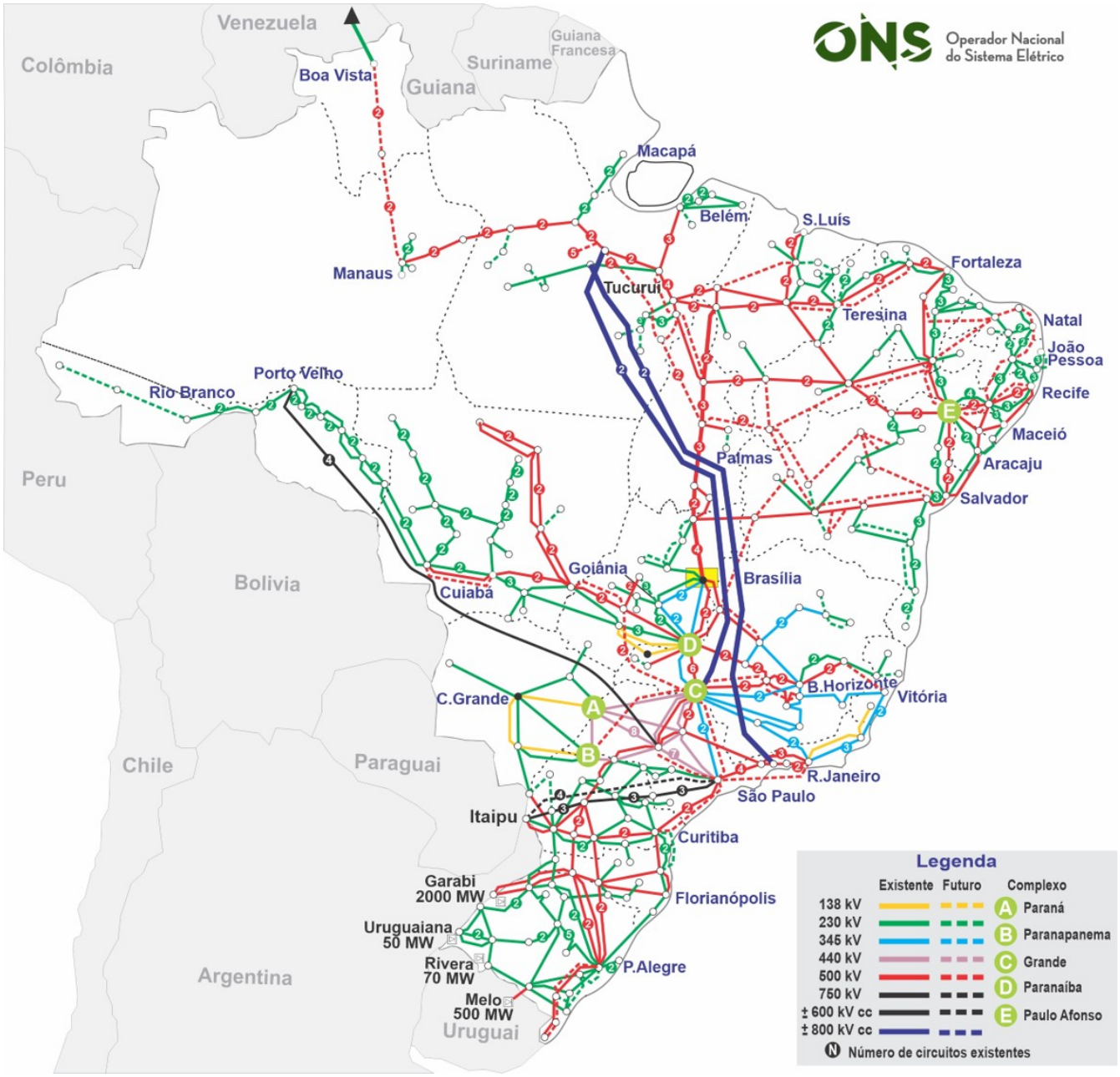
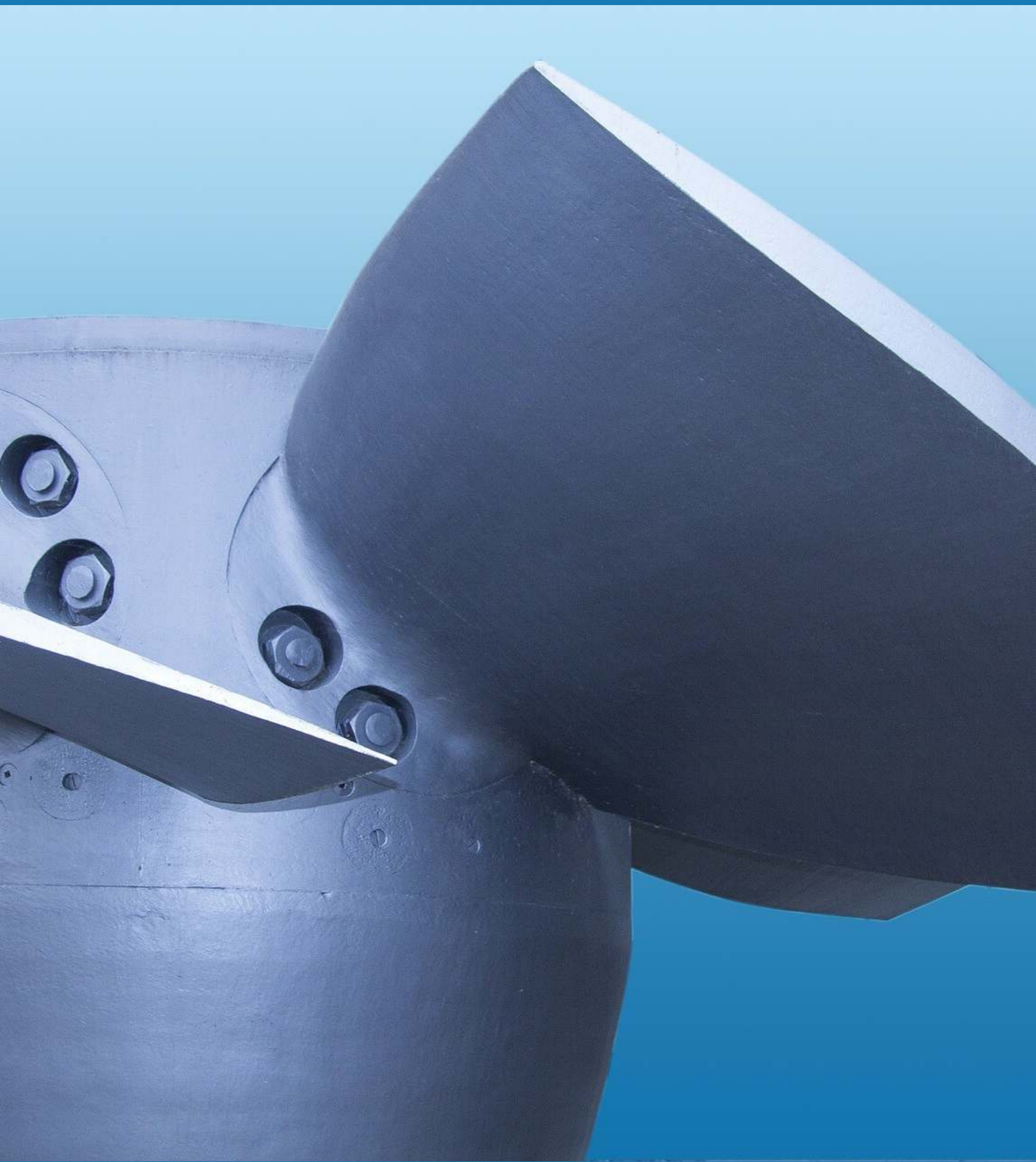


Figura 1. SIN - Sistema Integrado Nacional

Segurança Cibernética no Setor Elétrico



Eduardo Fagundes

O modelo do setor elétrico brasileiro

O modelo adotado pelo Brasil para o setor de energia tem vários atores, entre eles: usinas de geração de energia; sistemas de transmissão de alta tensão; distribuidoras de energia; permissionários; comercializadores de energia no mercado livre; Ministério das Minas e Energia; Agência Nacional de Energia Elétrica (Aneel); Operador Nacional do Sistema (ONS); consumidores livres; consumidores cativos; Câmara Comercialização de Energia Elétrica (CCEE); Empresa de Pesquisa Energética (EPE); e, autoprodutores de energia.

O mercado de energia no Brasil é regulado. A Aneel através de licitações públicas celebra contratos de concessão e outorga autorizações para o funcionamento das empresas de geração, transmissão e distribuição de energia. O ONS orquestra o funcionamento do SIN. A CCEE é uma operadora do mercado de energia, contabilizando operações de compra e venda de energia elétrica, determinando os débitos e créditos dos agentes do setor e calculando o Preço de Liquidação das Diferenças (PLD). A EPE faze estudos e pesquisas para subsidiar o planejamento do setor energético (energia elétrica, petróleo e gás natural e biocombustíveis). Leis especificas criaram a Aneel, ONS, CCEE e EPE.

Governança e gestão de segurança cibernética no setor elétrico brasileiro

Existe um arcabouço legal para apoiar a governança e gestão de segurança cibernética de infraestruturas críticas, como telecomunicações, transporte, energia, água e financeiro.

O Decreto nº 9.573, de 22 de novembro de 2018, aprovou a **Política Nacional de Segurança das Infraestruturas Críticas Nacionais**. Essa Política visa garantir a segurança e a resiliência das infraestruturas críticas do País e a continuidade da prestação de seus serviços. Nesse sentido, estabelece o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas, a Estratégia Nacional de Segurança de Infraestruturas Críticas e o Plano Nacional de Segurança de Infraestruturas Críticas.

Em dezembro de 2019, o Operador Nacional do Sistema (ONS) enviou à ANEEL sua proposta de Procedimento de Rede de segurança cibernética, cujo objetivo é estabelecer os controles de segurança cibernética a serem implementados no Ambiente Regulado Cibernético (ARCiber), composto pelos centros de operação dos agentes; pelos equipamentos que participam da infraestrutura de envio ou recebimento de dados e voz para ambientes operativos do ONS ou para centros de operação de outros agentes; e pelo ambiente operativo do ONS.

Decreto nº 10.222, de 5 de fevereiro de 2020, aprovou a **Estratégia Nacional de Segurança Cibernética** com o objetivo de elevar o nível de proteção das infraestruturas críticas nacionais, por meio das seguintes ações:

- Promover a interação entre as agências reguladoras de infraestruturas críticas para tratar de temas relativos à segurança cibernética;
- Estimular a adoção de ações de segurança cibernética pelas infraestruturas críticas;
- Incentivar que essas organizações implementem políticas de segurança cibernética, que contemplem, dentre outros aspectos, métricas, mecanismos de avaliação, e de revisão periódica.
- Incentivar a constituição de equipe de tratamento e resposta aos incidentes cibernéticos;
- Estimular que as infraestruturas críticas notifiquem o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) dos incidentes cibernéticos;
- Incentivar a participação das infraestruturas críticas em exercícios cibernéticos.

As organizações, públicas ou privadas, devem possuir uma equipe de tratamento e resposta aos incidentes cibernéticos (ETIR), em inglês *Computer Security Incident Response Team* (CSIRT). Essa equipe deve ser capacitada, dispor de ferramentas computacionais adequadas às suas necessidades, possuir sistemas baseados em tecnologias emergentes, condizentes com os padrões internacionais. O único CSIRT listado no site do cert.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) é o CSIRT Cemig. Embora, a organização que preenche os requisitos deve solicitar sua inclusão. O que pode significar que podem existir outros não catalogados.

Em 18 de maio de 2020, a Aneel emitiu a Nota Técnica nº 50/2020-SRT-SGI-SRD-SRG/ANEEL com o objetivo de propor a abertura de Tomada de Subsídios para coletar contribuições para avaliar a necessidade de intervenção regulatória para a segurança cibernética do Sistema Elétrico Brasileiro.

A Nota Técnica menciona a norma ISO/IEC 27000:2018 fornece a visão geral dos sistemas de gerenciamento de segurança da informação e os termos e definições comumente usados na família de normas ISO/IEC 27001. A norma ISO/IEC 27.001, detalha os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gerenciamento de segurança da informação, exigindo o exame sistemático dos riscos de segurança das informações e ações de mitigação, além de um processo de gerenciamento abrangente para garantir a continuidade da organização. A norma ISO/IEC 27.002 trata das boas práticas de segurança da informação, estabelecendo diretrizes e princípios gerais para a implantação da gestão de segurança da informação. A norma ISO/IEC 27.017, adiciona controles de segurança para a computação em nuvem que não foram tratados na ISO/IEC 27.002. Ainda, a norma ISO/IEC 27.005 fornece diretrizes e técnicas para o gerenciamento de riscos de segurança.

A Nota Técnica, também, comenta a existência de um framework de segurança cibernética com foco em redes operacionais da Associação Brasileira das Empresas de Transmissão de Energia Elétrica (Abrate) que define práticas para instalações de transmissão de energia elétrica, para os sistemas de telecomunicações, sistemas SCADA (*Supervisory Control and Data Acquisition*) e demais recursos relacionados às redes de automação.

As principais referências internacionais em segurança cibernética para o setor elétrico são os padrões CIP (*Critical Infrastructure Protection*) da Nerc (*North American Electric Reliability Corporation*) e o framework do Nist (*National Institute of Standards and Technology*).

As práticas de segurança cibernética são mais maduras nos Estados Unidos, Austrália e Europa, enquanto são incipientes na América Latina. No Brasil, existem leis e decretos que definem o modelo de governança, porém o desafio está na gestão para a implantação do modelo.

Segurança Cibernética no Setor Elétrico

Eduardo Fagundes

Modelo de Maturidade de Segurança Cibernética para Redes Inteligentes de Energia Elétrica

Smart Grid Cybersecurity Capability Maturity Model

No contexto de redes inteligentes de energia elétrica, Smart Grid, a segurança cibernética tem uma forte relevância. A análise do risco e as ações para mitigá-los determinam a confiabilidade do sistema. Para comparar diferentes redes e sistemas de energia é necessária a adoção de um modelo de referência com critérios padronizados.

A partir de uma iniciativa da Casa Branca americana, liderada pelo Departamento de Energia (DOE) em parceria com o Departamento de Segurança Nacional (DHS) e com a colaboração da indústria e especialistas do setor público e privado foi desenvolvido o *Electricity Subsector Cybersecurity Capability Maturity Model* (ES-C2M2).

O objetivo do modelo é apoiar o desenvolvimento e medir os níveis de segurança no setor elétrico através de quatro objetivos:

1. Reforçar as medidas de segurança cibernética do setor de eletricidade;
2. Permitir que os concessionários avaliem de forma eficaz e consistente suas ações de segurança e compará-las com outras empresas do setor;
3. Compartilhar conhecimentos, melhorar as práticas e obter referências relevantes para melhorar a segurança cibernética;
4. Permitir que as concessionárias priorizem suas ações e investimentos para melhorar a segurança cibernética.

A figura 2 mostra uma abstração da topologia da rede do sistema elétrico. Através do modelo, a “função” é usada para descrever o conjunto de atividades que devem ser analisadas pelas concessionárias ou empresas que integram a rede de geração, transmissão, distribuição e mercados.

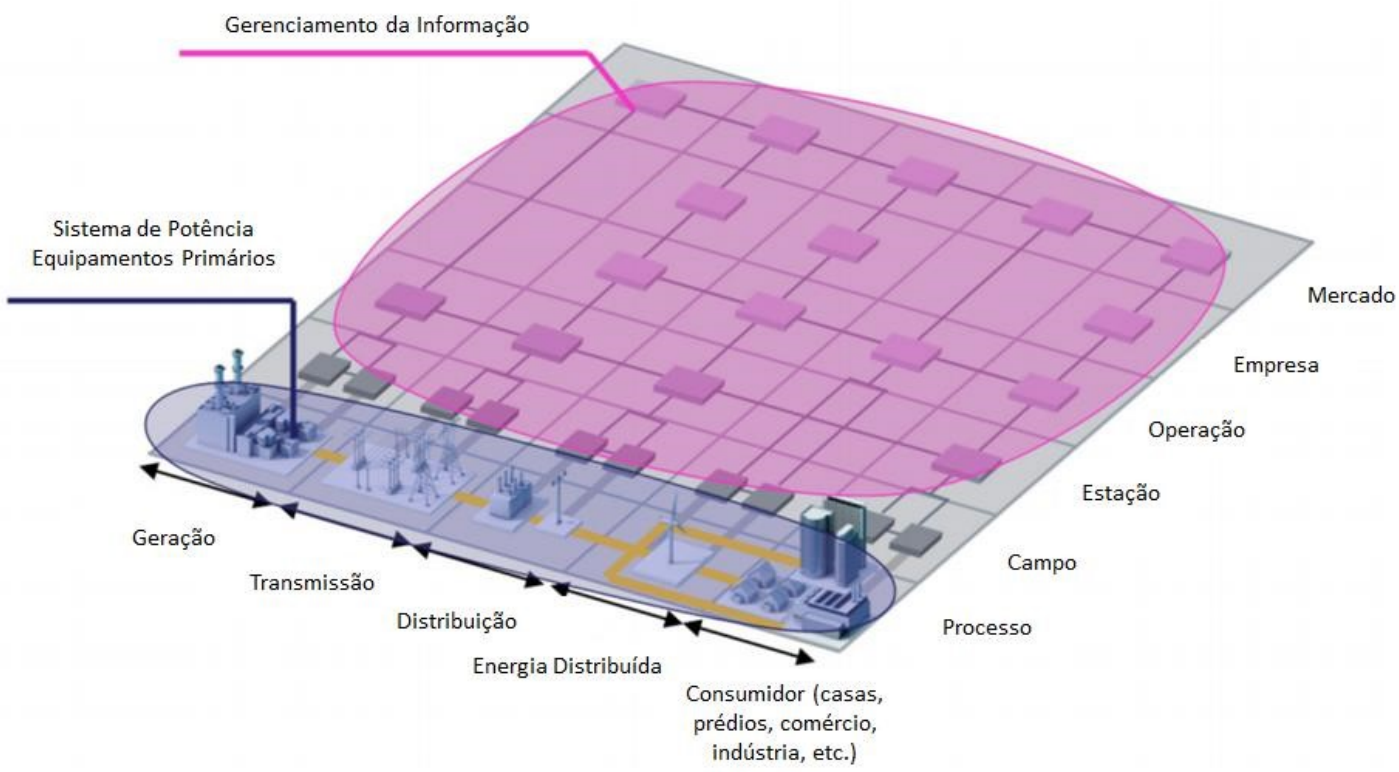


Figura 2. Abstração da topologia da rede do sistema elétrico

Arquitetura do Modelo

O modelo é organizado dentro de dez domínios e quatro indicadores de níveis de maturidade (MILs). A figura abaixo mostra a estrutura básica do modelo como uma matriz, os domínios como colunas e o MILs como linhas.

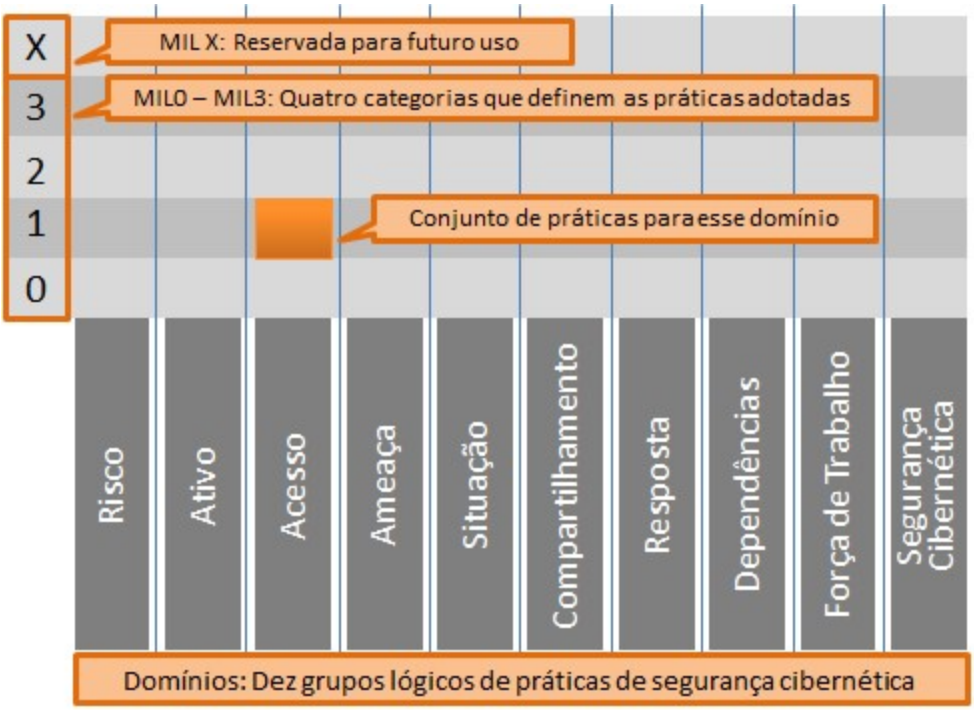


Figura 3. Arquitetura do modelo com os 10 domínios

Gestão de Risco (RISCO)

Estabelecer, operar e manter um programa de gerenciamento de riscos de segurança cibernética da empresa para identificar, analisar e mitigar os riscos da organização, incluindo o seu próprio negócio, sua infraestrutura e outras partes interessadas. O domínio RISCO compreende três objetivos:

1. Estabelecer a estratégia de gestão de riscos de segurança cibernética
2. Gerenciar os riscos de segurança cibernética
3. Gerenciar as atividades de risco

Ativo, Mudança, Configuração e Gerenciamento (ATIVO)

Gerenciar as operações de tecnologia (OT) e tecnologia da informação (TI) dos ativos da organização (hardware e software) para compatibilizar os riscos da infraestrutura com os objetivos organizacionais. O domínio ATIVO é composto por quatro objetivos:

1. Gerenciar o inventário de ativos
2. Gerenciar a configuração dos ativos
3. Gerenciar as mudanças nos ativos
4. Gerenciar as atividades

Gerenciamento de Identidade e Acesso (ACESSO)

Criar e gerenciar as identidades das entidades que podem ter acesso físico ou lógico aos ativos da organização. O domínio ACESSO compreende três objetivos:

1. Estabelecer e manter as identidades das entidades
2. Controlar os acessos
3. Gerenciar as atividades

Gerenciamento das ameaças e vulnerabilidades (AMEAÇA)

Estabelecer e manter planos, procedimentos e tecnologias para detectar, identificar, analisar, gerenciar e responder as ameaças e vulnerabilidades de segurança cibernética. O domínio AMEAÇA compreende três objetivos:

1. Identificar e responder às ameaças
2. Reduzir as vulnerabilidades de segurança cibernética
3. Gerenciar as atividades

Consciência Situacional (SITUAÇÃO)

Estabelecer e manter atividades e tecnologias para coletar, analisar, detectar, usar o sistema de energia e as informações sobre segurança cibernética, incluindo a situação e as informações dos outros domínios do modelo, para formar um quadro operacional comum, compatível com o risco da infraestrutura crítica e objetivos organizacionais. O domínio SITUAÇÃO compreende quatro objetivos:

1. Fazer o registro
2. Monitorar as funções
3. Estabelecer e manter um quadro operacional comum
4. Gerenciar as atividades

Compartilhamento de Informações e Comunicações (COMPARTILHAMENTO)

Estabelecer e manter o relacionamento com entidades internas e externas para coletar e fornecer informações sobre segurança cibernética, incluindo as ameaças e vulnerabilidades, para reduzir os riscos e aumentar a resiliência operacional, compatível com o risco da infraestrutura crítica e os objetivos organizacionais. O domínio COMPARTILHAMENTO compreende dois objetivos:

1. Compartilhar as informações de segurança cibernética
2. Gerenciar as atividades

Evento e Resposta aos Incidentes, Continuidade de Operações (RESPOSTA)

Estabelecer e manter planos, procedimentos e tecnologias para detectar, analisar e

responder aos eventos de segurança cibernética para apoiar as operações ao longo de um evento de segurança cibernética, proporcional ao risco da infraestrutura crítica e dos objetivos organizacionais. O domínio RESPOSTA é composto por cinco objetivos:

1. Detectar os eventos cibernéticos
2. Escalar os eventos cibernéticos
3. Responder aos eventos cibernéticos escalados
4. Plano de Continuidade
5. Gerenciar as atividades

Cadeia de fornecedores e gerenciamento das dependências externas (DEPENDÊNCIA)

Estabelecer e manter controles para gerenciar os riscos associados aos serviços de segurança cibernética e dos ativos que são dependentes de entidades externas, compatível com o risco da infraestrutura crítica e dos objetivos organizacionais. O domínio DEPENDÊNCIA compreende três objetivos:

1. Identificar as dependências
2. Gerenciar os riscos das dependências
3. Gerenciar as atividades

Gerenciamento da força de trabalho (FORÇA DE TRABALHO)

Estabelecer e manter planos, procedimento, tecnologias e controles para criar uma cultura de segurança cibernética para assegurar a adequação permanente e competência do pessoal, proporcional ao risco da infraestrutura crítica e dos objetivos organizacionais. O domínio FORÇA DE TRABALHO compreende cinco objetivos:

1. Atribuir responsabilidades à segurança cibernética
2. Controlar o ciclo de vida da força de trabalho
3. Desenvolver a força de trabalho
4. Aumentar a consciência sobre segurança cibernética
5. Gerenciar as atividades

Programa de Gestão de Segurança Cibernética (SEGURANÇA CIBERNÉTICA)

Estabelecer e manter um programa de segurança cibernética na empresa que forneça a governança, planejamento estratégico, e o patrocínio das atividades de segurança cibernética da organização de forma a alinha os objetivos de segurança cibernética com os objetivos estratégicos da organização e do risco da infraestrutura crítica. O domínio SEGURANÇA CIBERNÉTICA compreende cinco objetivos:

1. Estabelecer estratégia do programa de segurança cibernética
2. Eleger um patrocinador do programa de segurança cibernética
3. Estabelecer e manter a arquitetura de segurança cibernética
4. Desenvolver e utilizar um software seguro
5. Gerenciar as atividades

O modelo define quatro indicadores de níveis de maturidade: MIL0, incompleto; MIL1, inicial; MIL2, implantado; e, MIL3, gerenciado.

Os indicadores de níveis de maturidade são importantes para a ANEEL conhecer os riscos das infraestruturas das concessionárias e exigir iniciativas de mitigação. Para os investidores é importante conhecê-los para reduzir o risco dos seus investimentos.

Segurança Cibernética no Setor Elétrico

Eduardo Fagundes

Gestão de Risco em Infraestruturas de Smart Grid

Um incidente é resultado de uma sequência de falhas. Incidentes geram perdas financeiras e desgastam a imagem das organizações. Em ambientes Smart Grid que envolvem milhões de dispositivos físicos e componentes de softwares, é necessária uma nova abordagem de gestão de risco. A monitoração e a análise de risco devem ser em tempo real.

O primeiro grande desafio em sistemas complexos de Smart Grid é determinar dentro da infraestrutura quais os componentes devem ser monitorados e seu grau de criticidade, que é composto pelo tipo de ameaça, condições para iniciar uma ameaça, a probabilidade de ocorrência e o impacto nos negócios. Essa análise em sistemas complexos deve ter o apoio de softwares especializados.

Essa análise considera os processos para o restabelecimento do serviço do componente e ações de contorno, além do tempo entre falhas e seus tempos de recuperação. Os softwares de análise não conseguem identificar processos ineficientes, sendo necessários outros estudos para determinar o processo ótimo de operação.

Todo o processo envolve risco, cabe aos gestores tornar transparente o impacto gerado por uma falha e buscar o equilíbrio financeiro para os investimentos de mitigação.

Dentro de um processo de gestão de risco temos que considerar os seguintes pontos:

- **Ambiente interno**. A cultura de risco de uma organização define como o risco será visto e tratado. Isso incluir a filosofia de gestão de risco, o apetite pelo risco, à integridade e valores éticos e o ambiente em que são operados.
- **Definição de objetivos**. Sem objetivos claramente definidos é impossível identificar os eventos que podem afetar os negócios e impedir que os objetivos organizacionais sejam alcançados.
- **Identificação de eventos**. É possível definir oportunidades e ameaças identificando eventos interno e externos que influenciam na realização de um objetivo organizacional.
- **Avaliação de risco**. Os riscos são analisados e considerados a probabilidade de ocorrência e o impacto que isso causará na organização.
- **Resposta ao risco**. Várias ações podem ser tomadas quando da ocorrência de um risco. Os riscos podem ser evitados, aceitos, reduzidos ou compartilhados. Os gestores devem selecionar que a melhor opção para a organização.
- **Controle de atividades**. Procedimentos devem ser estabelecidos e implementados para auxiliar nas respostas aos riscos. Devem existir controles para avaliar a mitigação dos riscos, as visões dos gestores, relatórios, controles físicos e controles de desempenho.
- **Monitoração**. Todos os processos e componentes devem ser monitorados para assegurar sua execução e para coletar informações para ações de melhoria contínua.

- **Informação e comunicação**. Informações relevantes devem ser identificadas e comunicadas para forma apropriada e no tempo correto para que as pessoas responsáveis possam tomar ações dentro de suas competências para evitar a ocorrência de incidentes.

A figura 4 apresenta o fluxo de definição do processo e as etapas de avaliação de risco, avaliação interna e monitoração. A partir desse fluxo é possível definir responsáveis, alocação de recursos e ferramentas para a governança dos processos.

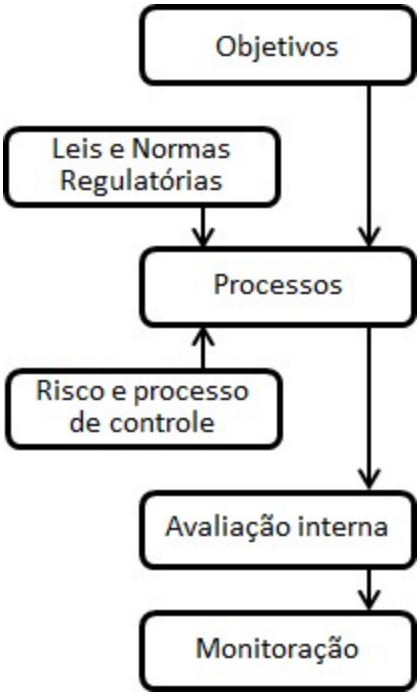


Figura 4. Fluxo de definição do processo e as etapas de avaliação de risco

A definição dos objetivos está ligada as metas de negócio da organização e das unidades de negócios. As leis e normas regulatórias devem ser consideradas para a definição do processo.

As metas geram os indicadores de desempenho dos processos. Para atingir as metas estabelecidas é necessário conhecer os riscos e tomar ações para gerenciá-los (evitar, reduzir, aceitar ou compartilhar). Frequentemente, os processos devem ser submetidos a uma avaliação interna e monitorados para assegurar sua execução e coletar informações para melhoria contínua.

Uma boa prática é incluir os objetivos no modelo BSC (*Balanced Scorecard*) de gestão da estratégia.

Para desenvolvimento e gestão de processos para Smart Grid várias ferramentas e metodologias devem ser utilizadas buscando excelência operacional.

- Software de desenho e simulação de processos.
- Software de governança, gestão de risco e conformidade.
- Software de gestão de ativos.
- Software de gestão de eventos do ambiente de Smart Grid.
- Software de gestão de portfólio de projetos.
- Metodologia de melhoria contínua para processos e mitigação de riscos operacionais.
- Software de Business Intelligence e Big Data.

Resumindo, o novo ambiente de Smart Grid exige um novo modelo de gestão risco com monitoração e análises em tempo real, detectando e avaliando mudanças do comportamento do sistema para evitar ataques cibernéticos e se antecipar a incidentes que podem paralisar alguns serviços. Essa nova abordagem exige novos desenhos de processos, softwares, metodologias de desenho de processos e novas tecnologias de análise de grandes volumes de dados em tempo real (Big Data).

A complexidade da troca de dados no setor elétrico gera um risco operacional

A gestão de um sistema elétrico é complexa em função da necessidade da troca intensa de dados entre os atores do sistema. Essa complexidade aumentará com a introdução de novos projetos de Smart Grid na distribuição e o aumento do micro e mini geração de energia pelos clientes. O aumento da complexidade do sistema gera um maior risco operacional. A quebra de confidencialidade e integridade dos dados ou a indisponibilidade de uma informação no momento certo pode comprometer todo o sistema e prejudicar milhões de consumidores.

O sistema elétrico é composto, basicamente, por sete domínios: geração, transmissão, distribuição, operação, provedores de serviços, mercado e clientes. Uma operação integrada requer a troca intensa de dados entre sistemas que geram ações automáticas ou manuais para o gerenciamento do sistema elétrico.

A figura 5 mostra uma visão simplificada dos principais componentes do sistema elétrico, os softwares e a integração necessária para operar o sistema. Esse modelo se aplica a todas as empresas que compõem o sistema elétrico integrado.

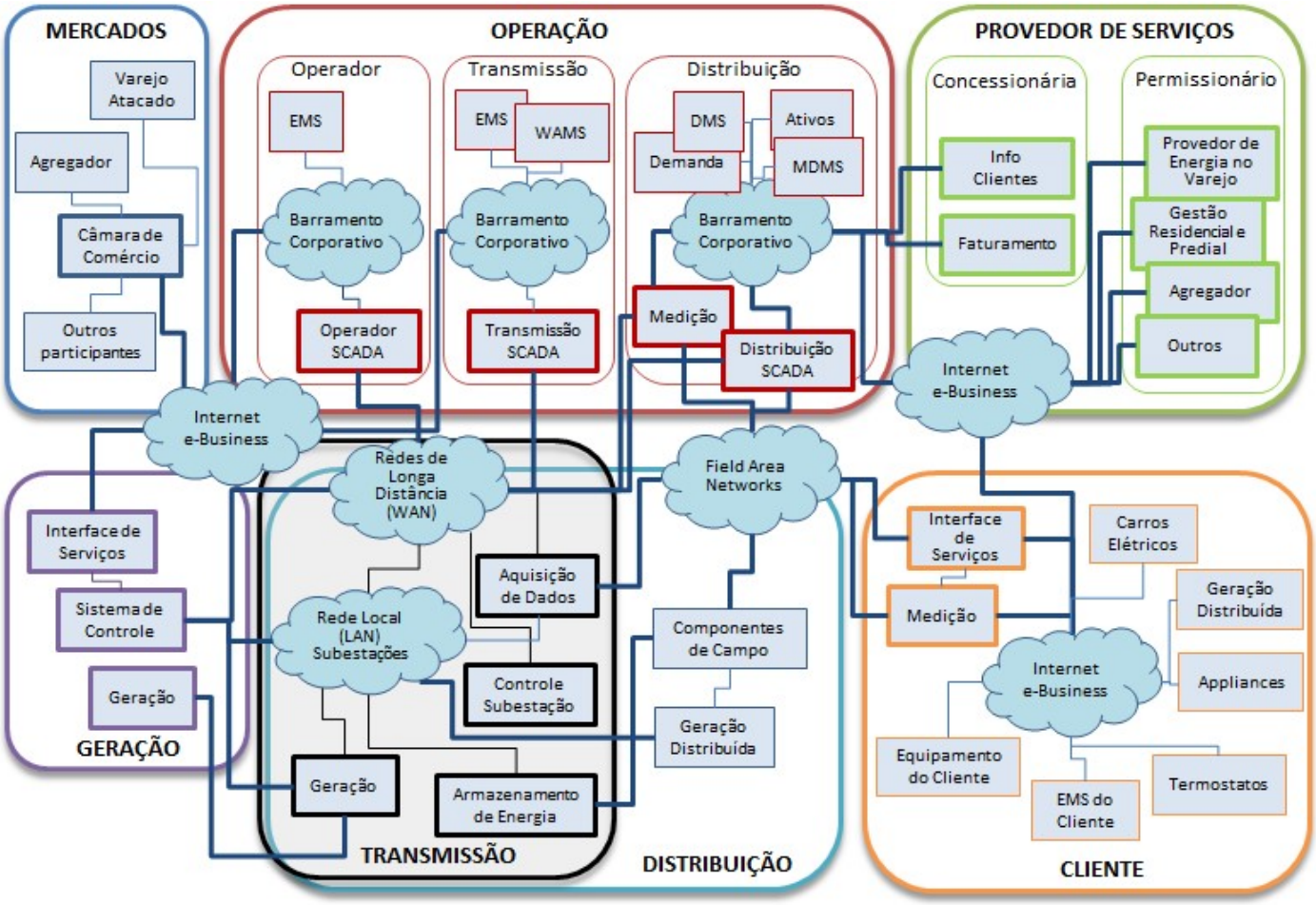


Figura 5. Visão simplificada dos principais componentes do sistema elétrico

O sistema envolve vários softwares e tecnologias de transmissão de dados e são definidos pelas empresas participantes do sistema. O único requisito é a padronização do formato de dados trocados e o tempo necessário de atualização. Isso requer das empresas a transformação dos formatos internos para o formato padrão, os chamados gateways.

A troca de dados entre a geração, transmissão, distribuição e operação são criticas e podem comprometer a confiabilidade do sistema. Basta um ator gerar informações falsas que todo o sistema será afetado. Se um hacker encontrar um único ponto vulnerável todo o sistema poderá ser comprometido.

A figura 6 mostra a complexidade das interfaces de troca de dados entre os principais sistemas do setor elétrico. Cada interface deve ser padronizada, por tanto de domínio público, para garantir a confiabilidade do sistema como um todo.

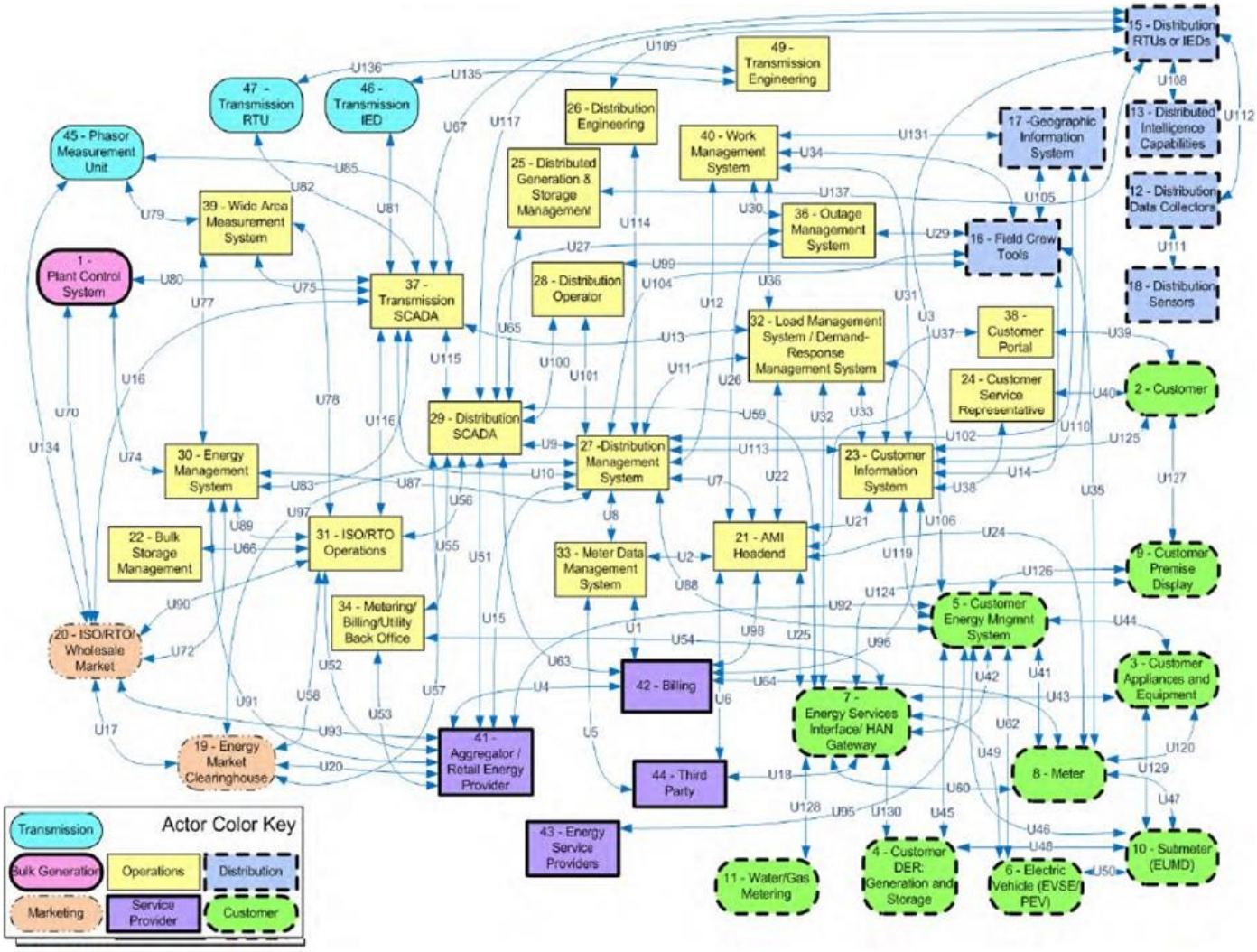


Figura 6. Interfaces de troca de dados entre os principais sistemas do setor elétrico

É necessário garantir que todas as empresas tenham um nível de proteção e monitoração da segurança da informação que evite a ação de hackers. O desafio é grande, pois os investimentos em segurança competem com projetos de expansão e melhoria no sistema físico da rede.

Um projeto de segurança para o setor elétrico começa com a necessidade de alta disponibilidade dos computadores do Data Center da empresa. A infraestrutura do Data Center (computadores, sistema de refrigeração e energia) deve ser redundante e ter a capacidade de operar em pouquíssimo tempo em outra localidade em caso de falha do data center principal.

Os sistemas de comunicação devem dispor de no mínimo duas conexões com fornecedores, infraestrutura independente e rota física distinta entre um ponto e outro. Isso garante, por exemplo, que se um cabo de fibra em um trecho for rompido exista uma rota alternativa para o encaminhamento dos dados.

Periodicamente, o sistema deve ser submetido a um teste integrado para identificar possíveis pontos de falha. Esses testes devem ser realizados primeiro nas empresas e depois no sistema como um todo, coordenado por algum órgão regulador. Isso é necessário, pois as mudanças nos sistemas são frequentes para corrigir falhar, atualização de versão de software ou para atender a requerimentos regulatórios.

Um ponto importante nesse contexto é o gerenciamento e a proteção das interfaces de troca de dados. O gerenciamento é necessário para garantir e monitorar se os sistemas estão enviando os dados dentro dos prazos estabelecidos e a proteção é vital para evitar a quebra de confidencialidade e integridade dos dados.

No mercado livre de energia a troca de informações entre as câmaras de comércio (CCEE, Câmara de Comercialização de Energia Elétrica e o BBCE, Balcão Brasileiro de Comercialização de Energia) e os consumidores deve ser segura e ter alta disponibilidade. Por envolver leilões de energia e trafegar informações financeiras, a confidencialidade dos dados é crítica para a confiabilidade do sistema. Por exemplo, o BBCE operar com um sistema nativo de certificado digital para garantir o não repúdio das operações, ou seja, é possível comprovar legalmente que um agente executou uma transação.

Alguns estudos indicam que o volume de dados das concessionárias de distribuição aumentará quase 3.000 vezes com a implantação de projetos de Smart Grid. Esse aumento é em função da coleta de dados frequente dos medidores eletrônicos dos consumidores. O gerenciamento desse grande volume de dados só será possível com o uso de novas tecnologias de banco de dados, como Big Data.

Resumindo, o avanço da automação no setor elétrico trará vantagens enormes para o setor, porém os gestores deverão investir em segurança da informação para manter os sistemas seguros, íntegros e disponíveis.

Segurança Cibernética no Setor Elétrico

Eduardo Fagundes

Segurança nas Redes Elétricas Inteligentes

Não há dúvidas dos grandes benefícios das redes inteligentes de energia elétrica. A automação do sistema elétrico não é novidade, há anos as concessionárias de energia elétrica e grandes fábricas utilizam sistemas de gerenciamento e controle dos dispositivos de proteção, geração e transmissão. A novidade é a massificação do uso da automação na distribuição de energia elétrica chegando à casa do assinante.

Em ambientes fechados e controlados a maior preocupação era a excelência operacional do sistema SCADA (Sistema de Supervisão e Aquisição de Dados). As redes de comunicação eram fechadas com links dedicados. A segurança do sistema era entendida como adequada pela complexidade do sistema, pouquíssimas pessoas qualificadas na área e difícil acesso ao sistema.

Com a implantação do Smart Grid na distribuição cobrindo, literalmente milhões de assinantes, é necessário utilizar redes de comunicação públicas e instalar os dispositivos remotos (sensores, controladores, disjuntores e medidores eletrônicos) em postes e na casa dos assinantes. O rápido desenvolvimento da Internet criou uma legião de programadores e, infelizmente, pessoas e organizações com o objetivo de roubar informações e destruir os sistemas por várias motivações, o chamado cyber terrorismo.

O grande desafio das concessionárias de distribuição e da indústria de equipamentos para Smart Grid é adequar a tecnologia e as questões de segurança da informação, mantendo o desempenho dos sistemas críticos com a melhor relação custo/benefício possível.

Para tornar viável projetos de Smart Grid, tanto do ponto de vista financeiro como técnico, é fundamental o uso de padrões de mercado para software e processos de gestão. A utilização de padrões permite a implantação de projetos com diferentes equipamentos de fornecedores com a interoperabilidade dos seus componentes assegurada pelas normas.

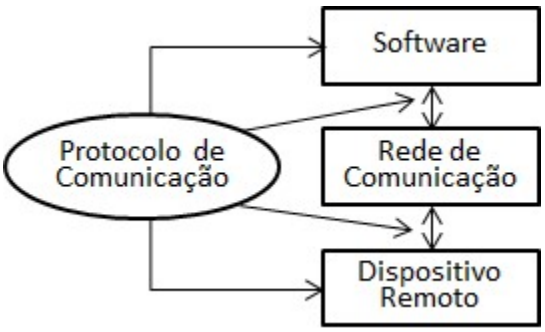


Figura 7. Visão simplificada de protocolos de redes de comunicação e computadores

Uma visão simplificada de protocolos de redes de comunicação e computadores é apresentada na figura 7. A troca de mensagens entre o software de gerenciamento e o software no dispositivo remoto é realizada com o uso de diversos protocolos que dividem uma mensagem em pequenos pacotes de dados para transmiti-los. Usa o conceito de camadas de protocolo, cada camada tem uma parte da responsabilidade da transmissão de dados. O número de camadas e responsabilidades é idêntico do lado do transmissor e do receptor.

Uma rede complexa pode ter várias camadas de software com diferentes especializações dentro do conceito de hierarquia, como mostra a figura 8.

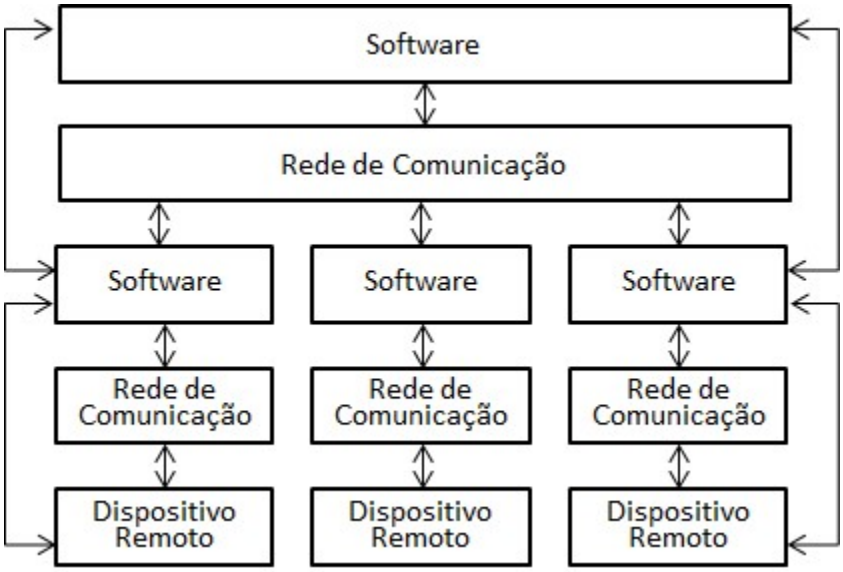


Figura 8. Camadas de software com diferentes especializações dentro do conceito de hierarquia

Uma das normas que apoia o desenho de projetos de Smart Grid é a IEC 61.850 para automação das subestações. Para a conexão de medidores eletrônicos e sensores massivamente dispersos geograficamente uma alternativa é o padrão aberto IPv6 (evolução do endereçamento IPv4 com regras de segurança), padrão de pacote seguro IPsec e a norma X.509 para segurança de mensagens.

A figura 9 mostra uma rede de comunicação para a automação do controle de uma subestação e medidores eletrônicos, remotamente.

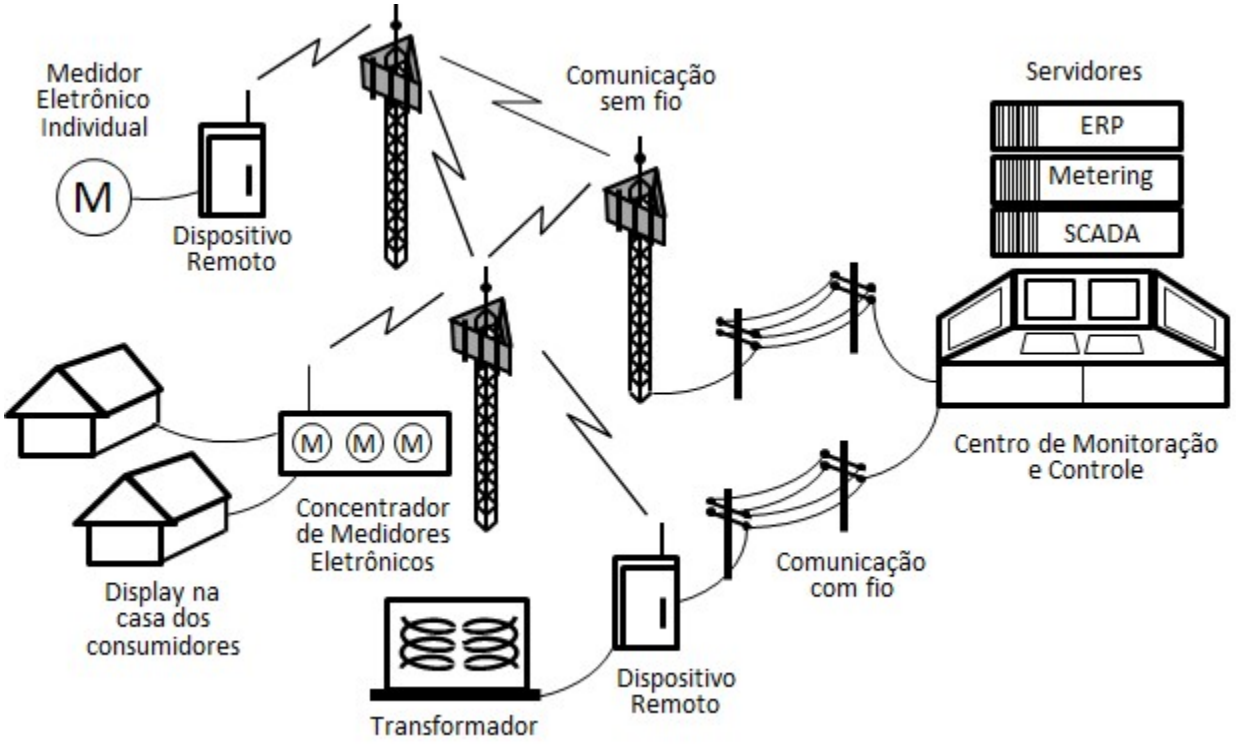


Figura 9. Rede de comunicação para a automação do controle de uma subestação e medidores eletrônicos

No exemplo, o dispositivo remoto para controle do transformador da subestação tem duas conexões de rede, com e sem fio. Essa redundância é importante para não interromper o serviço em caso de falha de uma das conexões.

A comunicação sem fio utiliza o conceito de mesh, onde cada estação base (ERB) pode se comunicar com sua adjacente de forma independente, aumentando a disponibilidade e confiabilidade da rede. Usando a rede sem fio são conectados os concentradores de medidores eletrônicos e medidores individuais.

Os displays que mostram o consumo de energia para o consumidor, exigido pela regulamentação, é feito usando comunicação de dados através da linha de energia, via PLC (*Power Line Communication*).

O sistema todo é controlado a partir de um Centro de Monitoração e Controle apoiado por sistemas de medição bidirecional (AMI – *Advanced Metering Infrastructure*), sistemas de supervisão e aquisição de dados (SCADA) e o sistema de gestão integrado (ERP) da empresa.

A configuração dos dispositivos é realizada por uma linguagem padronizada pela IEC 61.850 com base no XML (*Extensible Markup Language*) que define as regras de formato de um documento.

Veja na figura 10, um exemplo de configuração de dispositivos de controle de subestações.

```
<?xml version="1.0"?>
<SCL xmlns:sxy="http://www.iec.ch/61850/sclcoordinates001" xmlns="http://www.iec.ch/61850/2003/SCL">
<Header id="svc" toolID="SSI-Tool" nameStructure="IEDName" />
<Substation name="AA1" desc="Substation">
<VoltageLevel name="A1" desc="Voltage Level">
<Bay name="A01" desc="Bay" sxy:dir="horizontal">
<LNode iedName="AA1TH1" ldInst="LD0" lnClass="LPHD" lnInst="1" />
<LNode iedName="AA1TH1" ldInst="LD0" lnClass="ITCI" lnInst="1" />
<LNode iedName="AA1TH1" ldInst="LD0" lnClass="LLN0" lnInst="" />
</Bay>
</VoltageLevel>
<VoltageLevel name="C1" desc="Voltage Level">
<Voltage multiplier="k" unit="V">380</Voltage>
</VoltageLevel>
<VoltageLevel name="H1" desc="Voltage Level">
<Voltage multiplier="k" unit="V">33</Voltage>
<Bay name="Q03" desc="Trafo LV" sxy:x="54" sxy:y="33" sxy:dir="vertical">
<ConductingEquipment name="QA1" desc="Circuit Breaker" type="CBR" sxy:x="7" sxy:y="8" sxy:dir="vertical">
<Terminal connectivityNode="AA1/H1/Q03/N1" substationName="AA1" voltageLevelName="H1" bayName="Q03" cNodeName="N1" />
<Terminal connectivityNode="AA1/H1/Q03/N5" substationName="AA1" voltageLevelName="H1" bayName="Q03" cNodeName="N5" />
</ConductingEquipment>
<ConductingEquipment name="BU1" desc="Voltage Transformer 2 Sec. 3 Phase" type="VTR" sxy:x="4" sxy:y="24">
<Terminal connectivityNode="AA1/H1/Q03/N6" substationName="AA1" voltageLevelName="H1" bayName="Q03" cNodeName="N6" />
</ConductingEquipment>
<ConductingEquipment name="TrafoLV" desc="Line In/Out" type="IFL" sxy:x="7" sxy:y="26" sxy:dir="vertical">
<Terminal connectivityNode="AA1/H1/Q03/N6" substationName="AA1" voltageLevelName="H1" bayName="Q03" cNodeName="N6" />
</ConductingEquipment>
<ConductingEquipment name="BI1.2" desc="Current Transformer" type="CTR" sxy:x="7" sxy:y="12" sxy:dir="vertical">
<Terminal connectivityNode="AA1/H1/Q03/N3" substationName="AA1" voltageLevelName="H1" bayName="Q03" cNodeName="N3" />
<Terminal connectivityNode="AA1/H1/Q03/N4" substationName="AA1" voltageLevelName="H1" bayName="Q03" cNodeName="N4" />
</ConductingEquipment>
```

Figura 10. Exemplo de configuração de dispositivos de controle de subestações

Como podemos observar a padronização traz grandes vantagens para a implementação de sistemas Smart Grid. Entretanto, a exposição do modelo para o público em geral cria um risco potencial de segurança.

Por exemplo, a ANATEL licenciou a frequência de 3.590MHz para o uso da tecnologia de transmissão de dados WiMax. A faixa de frequência licenciada tem largura de banda 10 MHz e potência de 2 Watts em cada antena xPol com 14 dBi de ganho e tilt típico de 4 graus. Conhecendo essas características que são públicas, um hacker pode construir um transmissor de alta potência usando um chipset de WiMax para interferir no sinal da rede em uma localidade. Se esse transmissor estiver em um veículo em movimento será quase impossível sua detecção e apreensão.

Outro exemplo é o acesso de um hacker aos parâmetros de configuração dos dispositivos de controle para alterar seu comportamento. O envio de comandos e a inibição de alertas de controle podem danificar um transformador e tirá-lo de operação por um longo período, comprometendo o serviço para milhares de consumidores.

Outra situação grave é a quebra de integridade dos dados de bilhetagem dos medidores eletrônicos. Se um hacker tiver acesso aos registradores (memória) do medidor, ele poderá alterar os valores de medição. Para menos, se ele quiser se beneficiar pagando valores menores. Para mais, se ele quiser comprometer a confiança da concessionária entre os órgãos públicos e consumidores.

Seja por interferência física ou lógica, os sistemas de Smart Grid são inseguros.

A alternativa para tornar o sistema mais confiável é realizar um projeto levando em conta a segurança da informação, realizar verificações de conformidade frequentes e utilizar softwares especialistas de análise de comportamento do sistema em tempo real.

Conclusão

A energia elétrica é parte da infraestrutura crítica nacionais, requerendo ações que garantam a resiliência e disponibilidade dos serviços. Entre estas ações está a segurança cibernética. Frequentes ataques hackers têm sido registrados no mundo, incluindo no Brasil, que mostram a importância de adoção de modelos de governança e gestão da segurança cibernética. Em fevereiro de 2021, um ataque hacker na Usina de Angra obrigou a empresa a desligar seus sistemas administrativos. Felizmente, segundo a empresa, o sistema de operação da empresa é apartado do sistema corporativo que tem acesso à Internet.

O Brasil tem um arcabouço de leis e decretos que definem muito bem a política e estratégia de segurança cibernética. A Aneel e ONS tem trabalhado para implantar uma estrutura de montar equipes de tratamento e resposta aos incidentes cibernéticos (ETIR), em inglês *Computer Security Incident Response Team* (CSIRT) em todos os agentes do sistema integrado nacional. O movimento mais efetivo começou com a aprovação do Decreto nº 9.573, de 22 de novembro de 2018, sobre a Política Nacional de Segurança das Infraestruturas Críticas Nacionais e o Decreto nº 10.222, de 5 de fevereiro de 2020, sobre a Estratégia Nacional de Segurança Cibernética.

Entretanto, até o presente momento, os CSIRTs não são uma realidade na maioria das empresas de geração, transmissão e distribuição de energia elétrica, onde apenas a Cemig tem registro no site do cert.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil).

Devido a falta de um modelo nacional para governança e gestão da segurança cibernética seria interessante as empresas brasileiras seguirem modelos internacionais, como os padrões CIP (*Critical Infrastructure Protection*) da Nerc (*North American Electric Reliability Corporation*) e o framework do Nist (*National Institute of Standards and Technology*), permitindo acelerar a proteção dos sistemas.

O Departamento de Energia (DOE) dos Estados Unidos em parceria com o Departamento de Segurança Nacional (DHS) e com a colaboração da indústria e especialistas do setor público e privado foi desenvolvido o *Electricity Subsector Cybersecurity Capability Maturity Model* (ES-C2M2). Este modelo permite um melhor controle das operações, análises de riscos, respostas a incidentes e colaboração entre os agentes do sistema.

A complexidade da troca de dados no setor elétrico gera um risco operacional que envolve uma quantidade muito grande de agentes com diferentes níveis de maturidade em segurança cibernética, criando pontos de vulnerabilidade no sistema.

A ausência de auditorias oficiais pelos agentes reguladores e controladores do sistema integrado nacional dificulta conhecer a real dimensão das vulnerabilidades de segurança cibernética do setor elétrico brasileiro, criando um ambiente de incerteza sobre a robustez do sistema.

Com a introdução cada vez maior dos sistemas inteligentes de gestão (*Smart Grid*) e medição inteligentes (*Smart Metering*) e o consequente aumento da digitalização das operações, cada vez mais aumenta o risco de incidentes de segurança.

O Brasil deve acelerar a implantação de CSIRTs em todos os agentes do setor elétrico, adotando frameworks já utilizados internacionalmente com ferramentas apropriadas e pessoal treinado.

Eduardo Fagundes

Engenheiro eletricista, mestre em ciência da computação, pesquisador de Inteligência Artificial (IA), professor de cursos de pós-graduação e empreendedor. Como gerente e diretor de multinacionais, desenvolveu projetos de tecnologia na Alemanha, Argentina, Brasil, Estados Unidos, Índia, Inglaterra e Itália.

Lidera equipes de pesquisa e desenvolvimento (P&D) para a solução de problemas complexos com ferramentas analíticas e inteligência artificial. Apoia startups com mentoria para empreendedores. Desenvolve projetos de eficiência energética usando modelos avançados de análise de dados e tecnologias de monitoramento remoto. Professor de tecnologia, governança e segurança da informação.