DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Uma arquitetura de automação adaptada para Smart Grids contra ataques cibernéticos

Alexandro de Oliveira Paula

Programa de Pós-Graduação Profissional em Engenharia Elétrica
DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

AN ADAPTED AUTOMATION ARCHITECTURE TO SMART GRIDS AGAINST CYBERATTACKS

UMA ARQUITETURA DE AUTOMAÇÃO ADAPTADA PARA SMART GRIDS CONTRA ATAQUES CIBERNÉTICOS

ALEXANDRO DE OLIVEIRA PAULA

ORIENTADOR: GERALDO PEREIRA ROCHA FILHO, PhD

DISSERTAÇÃO DE MESTRADO PROFISSIONAL EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: PPEE.MP.015

BRASÍLIA/DF, MAIO - 2022

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Uma arquitetura de automação adaptada para Smart Grids contra ataques cibernéticos

Alexandro de Oliveira Paula

Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Engenharia Elétrica

Banca Examinadora

Prof. Geraldo Pereira Rocha Filho, Ph.D, FT/UnB _____
Orientador

Prof. Vinícius Pereira Gonçalves, Ph.D, FT/UnB _____
Examinador Interno

Prof. José Rodrigues Torres Neto, Ph.D, DC/UFPI _____
Examinador Externo

FICHA CATALOGRÁFICA

PAULA, ALEXANDRO DE OLIVEIRA
Uma arquitetura de automação adaptada para Smart Grids contra ataques cibernéticos [Distrito Federal] 2022.
xvi, 78 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2022).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Segurança em Smart Grids
2. Sistema de Automação de Subestações
3. Segurança Cibernética
4. Proteção de Sistemas Elétricos
I. ENE/FT/UnB
II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

DE PAULA, A. O. (2022). *Uma arquitetura de automação adaptada para Smart Grids contra ataques cibernéticos* . Dissertação de Mestrado Profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 78 p.

Alexandro de Oliveira Paula
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

À Deus, meu Pai e minha Mãe, minha esposa Aldenira e meus irmãos, Alessandro e Anderson. Desde o início, sempre depositaram fé nessa empreitada.

AGRADECIMENTOS

Agradeço à Universidade de Brasília, renomada instituição que me confiou a chance de construir uma solução técnica que sirva de legado. À CEB Distribuição, Neoenergia Brasília e Sinapsis, por acreditarem no trabalho com fomentação incondicionada e que abasteceram a pesquisa com o conhecimento de seus profissionais. Ao meu orientador, professor Geraldo Filho, que insistentemente me manteve na linha coerente e coesa da pesquisa técnica, visando sempre a padronização e objetivando a perfeição do trabalho. À toda comunidade acadêmica e profissional, que se mantém firme e forte, em prol dos avanços tecnológicos, independente da época.

RESUMO

Desde sua concepção, as *Smart Grids* ainda se encontram em fase de evolução constante, principalmente no setor de energia. Um fator ainda em evolução concerne à segurança cibernética de seus sistemas de automação e proteção, que mesmo com recomendações padronizadas das normas IEC 61850, estão vulneráveis a ataques em seus equipamentos. Isso prova que ainda é necessário investigar esse problema através de mais pesquisas. Tendo essa visão, este trabalho propõe o STRAYER: ***S**mar**T** a**R**chitecture **A**gainst c**Y**b**ER**attacks*, que reduz a vulnerabilidade dos dispositivos eletrônicos inteligentes (IED's) de automação em *Smart Grids*. O STRAYER integra segurança cibernética para monitoramento e blindagem de acesso, interoperabilidade para manter a comunicação entre equipamentos/dispositivos e gerenciamento de risco para manter a confiabilidade e prevenir ataques cibernéticos em tempo real. Para validar o STRAYER, foi construído um protótipo de arquitetura de automação em *Smart Grid*. Os resultados mostraram que o STRAYER aumenta a eficiência de segurança em relação a uma arquitetura tradicional, reduzindo a quantidade de equipamentos infectados e o tempo de acesso indevido às mesmas. Além das reduções na quantidade de IED's afetados por invasões, também foi possível perceber que o STRAYER evitou o colapso no fornecimento de energia elétrica, tendo apenas perdas mínimas e reversíveis, diferentemente da arquitetura tradicional.

ABSTRACT

Since their conception, Smart Grids are still in a constant evolution phase, mainly in the energy sector. A factor that is still evolving concerns the cybersecurity of its automation and protection systems, which, even with standardized recommendations from the IEC 61850 standards, are vulnerable to attacks on their equipment. This proves that it is still necessary to investigate this problem through further research. With this vision in mind, this work proposes the STRAYER: a **S**mar**T** a**R**chitecture **A**gainst c**Y**b**ER**attacks, which reduces the vulnerability of automation Intelligent Electronic Devices (IED's) in Smart Grids. STRAYER integrates cybersecurity for monitoring and access shielding, interoperability for maintaining communication between equipment/devices, and risk management for maintaining reliability and preventing cyberattacks in real time. To validate STRAYER, an automation architecture prototype was built for Smart Grids. The results showed that STRAYER increases security efficiency in relation to a traditional architecture, reducing the amount of infected equipment and the time of undue access to them. In addition to the reductions in the number of IED's affected by intrusions, it was also possible to notice that the STRAYER avoided the collapse in the electrical energy supply, having only minimal and reversible losses, unlike the traditional architecture.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SÍMBOLOS

Siglas

ANSI	*American National Standards Institute*
CID	*Configured IED Description*
COI	Centro de Operações Integrada
DNP3	*Distributed Network Protocol 3*
DoS	*Denial of Service*
GOOSE	*Generic Object Oriented Substation Event*
GPS	*Global Position System*
GSSE	*Generic Substation State Event*
HMI	*Human Machine Interface* (Interface Homem-Máquina)
ICD	*IED Capability Description*
ICMP	*Internet Control Message Protocol*
ICS	*Industrial Control System*
IDS/IPS	*Intrusion Detection System/Intrusion Protection System*
IEC	*Internationl Electrotechnical Commission*
IED	*Intelligent Electronic Device*
IoT	*Internet of Things*
IRIG-B	*Inter-Range Instrumentation Group - code B*
ISO	*International Organization for Standardization*
MMS	*Manufacturing Message Specification*
MU	*Merging unit*
NIST	*National Institute of Standards and Technology*
ONS	Operador Nacional do Sistema Elétrico
PENTEST	*Penetration Test*
SAMU	*Stand Alone Merging Unit*
SAS	Sistema de Automação em Subestações
SCADA	*Supervisory Control And Data Acquisition*
SCD	*Substation Configuration Description*
SCL	*Substation Configuration Language*
SSD	*System Specification Description*
STRAYER	*Smart architecture Against cyberattacks*
SV	*Sampled Values*
TC	Transformador de Corrente
TI	Tecnologia da Informação
TO	Tecnologia da Operação
TP	Transformador de Potencial

1 INTRODUÇÃO

Smart Grids permitem maior eficiência na operação e manutenção dos ativos das subestações de energia elétrica para melhor gerenciar suas cargas, reduzindo custos e potencializando as respostas a possíveis problemas nessas estruturas, em tempo real [2]. O modelo mais atual de Smart Grid idealizado pela norma IEC 61850 e complementado pelo *National Institute of Standards and Technology* (NIST) consiste em um sistema de comunicação para interligar todas as áreas inerentes aos processos de energia elétrica (geração, transmissão, distribuição), além da inclusão de subáreas de operação e mercado. A intenção é manter um domínio de gestão inteligente no setor elétrico [10]. Além disso, todas as áreas têm seus recursos tecnológicos aprimorados para manter a automação no estado da arte, incluindo os preceitos de segurança cibernética [11].

O avanço tecnológico em *Smart Grids*, que visa digitalizar as subestações elétricas existentes, também trouxe os problemas de ataques cibernéticos aos meios e protocolos de comunicação do Sistema de Automação de Subestações (SAS), conceituado pela norma IEC 61850. Esses ataques comumente ocorrem por meio de redes de computadores de empresas de gestão de energia, como as redes de Tecnologia da Informação (TI), Tecnologia Operacional (TO) e até mesmo por acesso remoto [12]. Esses problemas vêm sendo relatados atualmente na história de invasões nessas estruturas. Sobre os eventos mais impactantes e recentes, há aqueles em 2017 e 2020 na Ucrânia [13, 14], em 2010 e 2015 no Irã e em 2020 no Brasil [15]. Referente ao atual contexto mundial, ataques semelhantes podem vir a acontecer durante a guerra entre Rússia e Ucrânia (2022).

Várias soluções para segurança em *Smart Grids* foram propostas para tentar resolver os problemas de ataques cibernéticos [16, 17, 18, 19]. Recentemente, formas de mitigar o problema foram demonstradas, como as melhorias no sistema de telecomunicações [16], uso de soluções de segurança de TI padronizadas [17], e até mesmo, padronização do monitoramento e automação em *Smart Grids* [18]. Todos em comum, não mencionam adaptações na arquitetura SAS. Outra proposta [19] trabalhou no projeto físico de uma subestação elétrica totalmente digital para monitorar a comunicação e automação, mas os dados apresentados não focam na segurança efetiva da *Smart Grid*, e sim, no processo de digitalização. Sobre a robustez dos trabalhos citados, percebe-se que falta o fator dinâmico em suas soluções. Tal dinamismo se faz necessário devido justamente à diversidade de tipos de ataques cibernéticos.

1.1 OBJETIVO DA DISSERTAÇÃO

Este trabalho propõe o STRAYER, uma nova arquitetura que objetiva mitigar problemas de ataques cibernéticos em *Smart Grids* no que diz respeito à proteção do SAS e seus equipamentos. O STRAYER integra segurança cibernética para monitorar e proteger o acesso, interoperabilidade para manter a comunicação entre Dispositivos Eletrônicos Inteligentes (IED) e gerenciamento de risco para manter a confiabilidade e prevenir ataques cibernéticos em tempo real nas *Smart Grids*. Para a modelagem do STRAYER, foram utilizadas adaptações em redes de comunicação e arquitetura de automação conceitualizadas pelas

normas IEC 61850[1] além de redundâncias e separação de redes de operação e informação. Portanto, a arquitetura proposta mantém a integridade do sistema de automação e comunicação para *Smart Grids* e, consequentemente, a continuidade dos serviços essenciais para a população de uma determinada região. A continuidade no fornecimento de energia elétrica é primordial para manutenção de serviços de saúde, educação, segurança e demais objetivos de políticas públicas gerais.

1.2 ALCANCE DA PESQUISA

Como prova de conceito, um protótipo comumente utilizado em *Smart Grids* foi construído para validar o STRAYER, projetado para operar em um SAS. Quando comparado à arquitetura tradicional, o STRAYER alcançou os seguintes aspectos:

- Redução de 87,5 % dos IED's afetados por ataques através de acesso remoto e da rede TI;
- Redução de ataques a disjuntores de *Smart Grids* em 88,9 % por acesso remoto indevido;
- Atraso no tempo de invasão ao sistema supervisório da *Smart Grid* por acesso remoto em *16min27seg* em relação à uma arquitetura tradicional orientada pela IEC 61850, e;
- Atraso de *01h11min23seg* no tempo máximo de intrusão em um IED via acesso remoto.

1.3 ESTRUTURA DA DISSERTAÇÃO

O restante desta dissertação está organizado da seguinte forma. O Capítulo 2 apresenta a aplicabilidade das normas IEC 61850 e fundamentação teórica do conceito de *Smart Grid* e demais parâmetros que o STRAYER usará em sua proposta. O Capítulo 3 apresenta os trabalhos relacionados e suas limitações que esta pesquisa explora. O Capítulo 4 apresenta como o STRAYER foi modelado e sua principal contribuição. O Capítulo 5 apresenta a validação do STRAYER em comparação com uma arquitetura tradicional conceitualizada pela IEC 61850. Finalmente, o Capítulo 6 apresenta as conclusões e as linhas de pesquisa futuras.

[1] Série de normas que versam sobre os padrões de Dispositivos Eletrônicos Inteligentes - IED's - e demais requisitos do Sistema de Automação em Subestações

2 FUNDAMENTAÇÃO TEÓRICA

Para um melhor entendimento sobre a concepção da arquitetura proposta, é necessário explicar sobre os fatores teóricos que fundamentam o funcionamento do STRAYER. Além dos requisitos gerais, das mudanças e do conceito de Interoperabilidade que o rol de normas IEC 61850 trouxeram, a explicação prática e técnica sobre *Smart Grids* e seu referido sistema de automação e comunicação também se faz presente neste capítulo.

A principal adaptação que o STRAYER traz é em relação à arquitetura do Sistema de Automação em Subestações (SAS). É necessário que sejam apresentado os conceitos teóricos e aplicações práticas que a IEC 61850 determinou para o SAS tradicional, antes de verificarmos a sua alteração pelo STRAYER.

Além disso, os conceitos de Segurança Cibernética e Gestão de Riscos, que são parte dos elementos integrantes que compõem o STRAYER, serão abordados e analisados sob influência da aplicação em *Smart Grids*. Ambos são fundamentais para construção da nova arquitetura adaptada.

2.1 UMA ABORDAGEM DA NORMAS IEC 61850

Em 1994, um grupo de trabalho nomeado de *Substation Control and Protection Interfaces*, pertencente ao Comitê Técnico 57 da IEC elaborou propostas para uma padronização da comunicação em sistemas de automação de subestações [20]. Desde então as recomendações da norma IEC 61850 estão cada vez mais presentes em projetos de *Smart Grids* [21]. Não se trata apenas da troca de equipamentos de pátio antigos por novos, mas sim, na modernização de todos os elementos inerentes à comunicação e automação de uma subestação elétrica.

Desde sua criação, já passou por várias modificações e inclusões de normas complementares. Salienta-se que a 61850 é um conjunto de normas, e não um "protocolo" como alguns fabricantes costumam referir-se no *datasheet* de seus produtos. Foi conceituada inicialmente com 14 partes principais, dispostas conforme Tabela 5.1. Cada parte ainda possui subpartes que foram revisadas ao longo dos anos até o presente momento.

Tabela 2.1: Primeiras revisões de normas IEC 61850 [8]

Parte	**Descrição da Norma**
Parte 1	Introdução e Visão Geral.
Parte 2	Glossário.
Parte 3	Requisitos Gerais.
Parte 4	Gerenciamento de Sistemas e Projetos.
Parte 5	Requisitos de Comunicação para Funções e Modelos de Dispositivos.
Parte 6	Linguagem de descrição de configuração para comunicação em subestações elétricas relacionadas a IED's.

Parte 7-1	Estrutura Básica de Comunicação para Subestações – Princípios e Modelos.
Parte 7-2	Estrutura Básica de Comunicação para Subestações – Interface de Serviço de Comunicação Abstrata (ACSI).
Parte 7-3	Estrutura Básica de Comunicação para Subestações – Classes de Dados Comum (CDC).
Parte 7-4	Estrutura Básica de Comunicação para Subestações – Classes de Nós Lógicos Compatíveis e Classes de Dados.
Parte 8-1	Mapeamento de Serviços de Comunicação Específica – Mapeamento para MMS ISO/IEC 9506 (Parte 1 e 2) e para ISO/IEC 8802-3.
Parte 9-1	Mapeamento de Serviços de Comunicação Específica – Valores Amostrados Sobre Enlace Serial Ponto a Ponto Unidirecional.
Parte 9-2	Mapeamento de Serviços de Comunicação Específica – Valores Amostrados sobre ISO/IEC 8802-3.
Parte 10	Teste de Conformidade.

A princípio, a primeira norma IEC 61850 surgiu da necessidade de padronização da comunicação entre os recém criados IED's (Dispositivos Eletrônicos Inteligentes) [22] que traziam uma inovação no sistema de automação das subestações digitais como objetivo principal [20]. A possibilidade de construir um sistema de automação inovador foi devido aos grandes avanços na tecnologia dos circuitos integrados à época. O resultado foi uma evolução dos equipamentos secundários eletromecânicos das subestações elétricas para dispositivos digitais.

Com o passar dos anos, os IED's assumiram mais e mais funções, além da proteção e automação. O monitoramento e supervisão remota através do SCADA foi um dos resultados da implantação das normas IEC 61850, além de evolução no sistema de comunicação entre os mesmos [20].

Adicionalmente, o conjunto de normas tentou trazer o sistema de redes e de automação das *Smart Grids* próximo ao Estado da Arte, individualizando o conjunto de tecnologias já existentes, como a Tecnologia da Informação (TI) e Tecnologia de Operação (TO).

É de salientar que as normas IEC 61850, apesar de requisitar avanços na área de segurança da informação para os IED's, não aborda de maneira mais precisa sobre a gestão de segurança em *Smart Grids* como um todo. Para tanto, é necessário aliar os fundamentos da IEC 61850 com *frameworks* já consolidados, como as instruções do NIST, por exemplo.

2.1.1 Requisitos da IEC 61850

O conjunto de normas são regidos por uma série de requisitos gerais delineados na IEC 61850-3 [23] que de certa maneira, trazem uma ênfase na qualidade do sistema de comunicação [9] entre IED's. Esses requisitos gerais de qualidade exigem Confiabilidade, Disponibilidade, Manutenção, Segurança, Integridade dos dados, e, entre outros elementos que devem estar implantados no projeto e construção de de IED's [23] ou outros dispositivos que compõem o sistema de comunicação utilizado para supervisão das *Smart Grids*.

No requisito de Confiabilidade, a norma define que uma subestação elétrica digital deverá continuar operando, de forma adequada, mesmo se algum componente de comunicação do SAS vier a falhar, evitando a descontinuidade dos serviços de fornecimento de energia elétrica. Ou seja, determinada falha de qualquer componente não deve resultar em perda indetectável de funções nem falhas em cascata [23].

A Disponibilidade trata da recuperação automática e geração de backup. De maneira geral, segundo a IEC 61850-3, é definida com a razão entre o tempo de atividade do SAS e o tempo total [23, 4]. Logo, a Disponibilidade avalia o tempo disponível dos dispositivos de automação e comunicação, como os IED's e HMI, e determina que, depois de detectada a falha, seja realizada recuperação rápida, automática e de backup.

Conforme comentado anteriormente, as normas IEC 61850 tratam indiretamente dos requisitos de Segurança, sendo esses, recomendadas por outras normas pela própria IEC 61850-3 [23], como a IEC 60870-4, por exemplo. O mesmo acontece com os requisitos de Manutenção e Integridade de Dados. Essas normas complementares tratam apenas da classificação e requisitos de desempenho.

Adicionalmente, existem alguns requisitos determinados pela IEC 61850-3 que se referem à questões gerais de redes de computadores, tais como: Quantidade de equipamentos, disposição geográfica dos dispositivos inteligentes, classe de tensão, tipo de barramento de rede, entre outros. A mesma norma pede para que, para tal definição, as normas IEC 61850-1 e 61850-5 sejam consultadas na ocasião.

Por fim, quando um IED, ou qualquer dispositivo de rede, com um *switch* ou roteador apresentar a descrição da IEC 61850-3 em seu corpo ou *datasheet*, significa que seu respectivo fabricante aderiu às condições de projeto da norma, significando maior robustez de comunicabilidade e automação.

2.1.2 Mudanças com aplicação das normas IEC 61850

A aplicação direta de todas as normas trouxe avanço tecnológico às *Smart Grids* através dos dispositivos inteligentes de automação e comunicação. Evolução nos projetos de relés eletromecânicos para os IED's digitais, sensibilidade dos medidores de tensão e corrente, e, precisão dos *logs* de eventos em oscilografias são apenas alguns dos exemplos de melhorias identificadas desde a concepção da IEC 61850.

Além disso, houve também mudança na aplicação de redes de computadores na comunicações, dentro e fora das *Smart Grids*. O uso de Redes Locais (LAN's), a separação das redes de TI e TO no interior das *Smart Grids* e a melhoria significativa dos sistemas de supervisão e monitoramento também são requisitos das normas. Isso denota mudança tanto em *hardware* quanto em *software*. O desenvolvimento dos sistemas e dos dispositivos inteligentes, sob ótica da IEC 61850, tiveram alterações nas fases de projetos, implantação, construção e comissionamento, conforme descritas na Tabela 5.2.

Tabela 2.2: Benefícios nas fase de desenvolvimento de um sistema inteligente pela IEC 61850 [9]

Fase	**Evolução tecnológica da IEC 61850**
Projeto	Desenvolvimento do Sistema de Automação em Subestações (SAS), com uso de ferramentas de especificação integrada e padrões de projetos nos IED's ou outro dispositivo inteligente.
Implantação	Geração automática dos arquivos de configuração nos IED's para os equipamentos de campo das *Smart Grids*. Além disso, é possível verificar essas configurações a partir de outros IED's.
Construção	Na construção dos dispositivos e na instalação dos mesmos nas *Smart Grids*, há a minimização de problemas decorrentes da Camada Física de redes. O uso de cabos e fibras ótica no lugar dos cabos de par trançado, a redução do uso de cabo elétricos em relés eletromecânicos e conexões são exemplos de avanço nessa fase.
Comissionamento e Documentação	Testes de comissionamento e geração de documentação do ensaios de forma mais rápida, pois as simulações do funcionamento das *Smart Grids* já estão pré-determinadas nos IED's. Isso resulta em redução de erros de informação nas bases de dados

2.1.3 Interoperabilidade entre dispositivos

Uma contribuição significativa com a aplicação da IEC 61850, foi a padronização da troca de informações de configuração e interoperabilidade entre sistemas, ferramentas e dispositivos de diferentes fabricantes em *Smart Grids*.

Um exemplo dessa padronização foi a concepção da *Substation Configuration Language* (SCL), descrito na norma IEC 61850-6 [24]. Trata-se de uma linguagem de configuração baseada em XML que é utilizada para intercambiar os dados de configuração do banco de dados entre dispositivos distintos e de diferente projeto de construção [9]. Atualmente, o projeto de arquitetura deve conter os seguintes arquivos SCL:

- ***System Specification Description*** **(SSD)** - função dedicada ao sistema de potência da subestação da Smart Grid;
- ***Substation Configuration Description*** **(SCD)** - define a arquitetura de comunicação da Smart Grid;
- ***IED Capability Description*** **(ICD)** - determina os objetos do banco de dados de determinado IED;
- ***Configured IED Description*** **(CID)** - determina a configuração final de uma IED. Talvez a linguagem mais importante em termos de proteção.

As informações desses arquivos representam os dados do produto de forma padronizada, e, em um ambiente de sistemas de informação integrada, é necessário que todos os dispositivos consigam ler esse conteúdo. Assim sendo, pode-se dizer que os dispositivos estão em integração e interoperáveis [25].

Enfim, por determinação da IEC 61850-6, os fabricantes devem implantar e manter os arquivos SCL padronizados no momento da montagem da arquitetura do dispositivo. Isso permite obter o máximo de comunicação possível entre os equipamentos.

A interoperabilidade diferenciada em conjunto com mais dois elementos, a Segurança Cibernética e a Gestão de Riscos compõem a lógica de fluxo da arquitetura adaptada do STRAYER. O conceito teórico dos demais elementos serão apresentados mais adiante, ao passo que, a lógica de fluxo, no capítulo de apresentação da arquitetura adaptada.

2.2 A HISTÓRIA POR TRÁS DAS *SMARTS GRIDS*

As *Smart Grids* permitem maior eficiência na operação e manutenção dos ativos de fornecimento de energia elétrica para melhor gerenciar suas cargas, reduzindo custos e potencializando as respostas a possíveis problemas nessas estruturas, em tempo real [2]. O modelo complementado pelo *National Institute of Standards and Technology* (NIST) consiste em um sistema de comunicação para interligar todas as áreas inerentes aos processos de energia elétrica (geração, transmissão, distribuição), além da inclusão de subáreas de operação e mercado. A intenção é manter um domínio de gestão inteligente no setor elétrico [10]. Além disso, todas as áreas têm seus recursos tecnológicos aprimorados para manter a automação no estado da arte, incluindo os preceitos de segurança cibernética [11].

2.2.1 Subestações e o Sistema elétrico

Uma Subestação elétrica é um complexo estrutural que contém uma série de equipamentos específicos que atuam em conjunto com a finalidade de elevar ou reduzir uma faixa específica de tensão elétrica. Esse processo é chamado de transformação. A depender do contexto, as subestações podem ser elevadoras ou abaixadoras, de acordo com a posição em que encontram no caminho do fornecimento de energia elétrica. Esse caminho é composto, basicamente por três etapas: Geração, Transmissão e Distribuição.

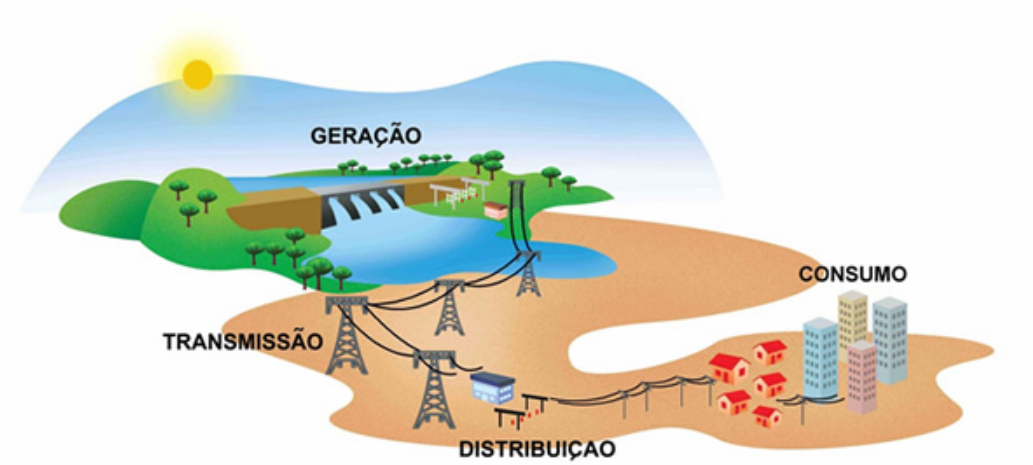


Figura 2.1: Caminho da energia elétrica. Retirado de [1].

- **Geração de energia elétrica** - A energia elétrica pode ser gerada de várias maneiras. Apesar de que no Brasil a sua grande maioria são de Usinas Hidrelétricas (UHE) justamente por seu potencial fluvial hidráulico, existem ainda outras alternativas, mais nocivas e mais sustentáveis. As usinas termelétricas movidas a carvão mineral, óleo combustível, gás natural ou nucleares, consumindo neste último caso o urânio enriquecido, são exemplos de usinas geradoras de energia com fontes nocivas ou não sustentáveis, e tendem a sumir do cenário energético. Atualmente em voga e ganhando cada vez mais espaço, estão as usinas sustentáveis, tais como as de energia solar fotovoltaica, usinas eólicas, usinas utilizando-se da queima da biomassa (como a madeira, cana de açúcar) e de biogás. Nesse caminho inicial, como a tensão gerada é baixa, as subestações elétricas são elevadoras. A frequência padrão de geração no Brasil é de 60 Hz.

- **Transmissão de energia elétrica** - A transmissão é um conjunto de várias subestações, abaixadoras e elevadoras (dependendo do fluxo de potência) que têm finalidade especifica de transporte de energia. As tensões usuais de transmissão adotadas no Brasil, em corrente alternada, podem variar de 138 kV até 765 kV incluindo neste intervalo as tensões de 230 kV, 345 kV, 440 kV e 500 kV.

- **Distribuição de energia elétrica** - A etapa de Distribuição, por sua vez, é aquela que recebe grande quantidade de energia do sistema de transmissão e a distribui para consumidores médios e pequenos. Os consumidores, individualmente, requerem potências inferiores às transmitidas. Portanto, são previstas estações de transformação abaixadoras nas quais as tensões permanecem em níveis compatíveis com as cargas regionais.

As subestações ainda suporta diversos equipamentos e dispositivos, tais como: Equipamentos de Automação (*switches*, roteadores, *gateways*, GPS's, computadores, cabos de fibra ótica), Proteção (relés de proteção, disjuntores, comandos elétricos), Telecomunicações (torres de comunicação, rádios, antenas, multiplexadores), Medição (Transformadores de corrente ou potencial) e Transformação (transformadores de potência ou serviços auxiliares). Em uma Subestação Digital, muitos desses dispositivos são totalmente digitais e interligados, facilitando a instalação elétrica.

o transformador de potência é de longe o ativo mais importante de uma subestação, afinal, é ele quem executa a tarefa originária. Todos os outros equipamentos existem para proteger o transformador de potência, inclusive, a filosofia de proteção de uma subestação segue o rito de deixar esse equipamento como o último e ser desligado, em caso de faltas (curto-circuito) indevidas.

2.2.2 Elementos de *Smart Grids*

As Redes Inteligentes, ou *Smart Grids* são estruturas complexas que se utilizam do conceito de IoT (*Internet of Things*) que otimizam o uso dos ativos e reduzem o consumo de energia com processos de operação e manutenção eficientes e dinâmicas. Sua principal característica é o sistema de resposta às demandas de equilíbrio de carga, fazendo com que haja uma eficiência no uso de energia de forma aprimorada [2].

Com a concepção de aplicações de *Smart Grids*, é possível que haja um fluxo de dados dinâmico e bidirecional em tempo real de informações como fluxo de carga e consumo por região ou cidade, tanto

para o COI quanto para os consumidores. Geradoras e consumidores terão relação mais próxima devido a maior disposição de informações do processo como um todo. Este conceito é apresentado na Figura 2.2 que trata do caminho do setor elétrico, agora com adventos de *Smart Grid*.

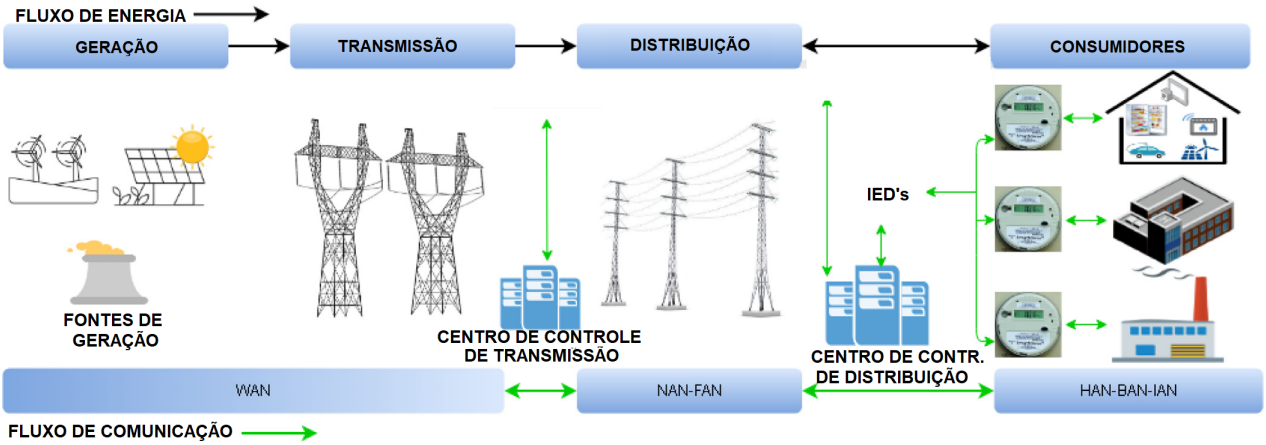


Figura 2.2: Processo de transmissão de eletricidade de *Smart Grid* da geração ao consumidor. Adaptado de [2].

Agora, os IED's têm todo o seu potencial explorado e se torna o elemento chave para consecução das necessidades das Smart Grids. Outros elementos também tiveram impacto na evolução, com os sensores e interfaces de visualização de operação. Este último representado pelo HMI, que mostra a situação em tempo rela da estrutura através do Controle Supervisório e Aquisição de Dados (SCADA), tanto local quanto remotamente. Através da gestão descentralizada da automação e de controle remoto em subestações de média tensão, o SCADA ajuda a garantir a confiabilidade do fornecimento de energia e reduz os custos de manutenção e operação da rede junto com sistemas de gestão de distribuição e de energia [2].

2.2.3 A evolução para as *Smart Grids*

No início, as subestações elétricas eram totalmente analógicas. Isso concernia em equipamentos que não se comunicavam entre si, tão pouco com outras subestações. Não havia sequer um Centro de Operações Integrado. Ao invés disso, era necessária a presença humana dentro de uma subestação para dirimir eventuais emergências. Os relés de proteção eram eletromecânicos e não existiam equipamento de automação.

Aos poucos, as subestações elétricas foram evoluindo, principalmente sobre os equipamentos de automação, proteção e comunicação. havia agora a comunicação de uma subestação com um Centro de Operações e elementos de automação, como as Unidades Terminais Remotas (UTR's). Filosofias de proteção começaram a ser implantas com o advento dos IED's, mas ainda sem qualquer pretensão de aplicação de normas de segurança, interoperabilidade interna ou externa.

A criação da IEC 61850, a renovação dos equipamentos analógicos para digitais, a implantação rígida do dinamismo de comunicação e de *smart metering* fez surgir a concepção das *Smart Grids*. Esta tem uma regra bem simples de interconexão dinâmica. Agora, as subestações passaram a comunicar-se entre si, não penas para simplesmente passar informações, mas as informações agora são tratadas de forma a otimizar todo um sistema inteligente de subestações elétricas digitais.

Basicamente, para tornar uma subestação analógica em digital, é necessário executar um dos dois caminhos a seguir: i) substituir todos os componentes analógicos por equipamentos digitais ou ópticos (o que leva muito tempo e é relativamente caro), ou; ii) inserir mecanismos de conversão Analógico/Digital (A/D) entre o equipamento e a comunicação (operação da subestação). Foi pensando nesta última opção, mais acessível, que os fabricantes criaram dispositivos de "digitalização", como IED's e os SAMU's.

É bem verdade que existem várias lacunas que impossibilitam uma total interligação entre *Smart Grids*. Além das deficiências tecnológicas entre diferentes regiões, ainda há o problema da segurança cibernética. Invasores entendem que é bastante conveniente essa "interligação máxima". E por esse motivo, é possível pensar sobre uma solução de pesos e contramedidas, que permita a expansão da intercomunicação de estruturas elétricas, sem deixar vulnerabilidades.

2.3 O SISTEMA DE AUTOMAÇÃO DE SUBESTAÇÕES - SAS

As *Smart Grids* possuem segmentações internas para melhor organizar seu bom funcionamento. Não existe uma definição final da disposição desses segmentos, porém, de maneira geral, comumente se dividem em: Equipamentos mecânicos de manobra, Transformadores, Comandos elétricos, Proteção, Comunicação, e por fim, a Automação. Apesar da importância de todo o conjunto mencionado, as partes de Comunicação e Automação possuem parcela significativa no gerenciamento e monitoramento das *Smart Grids* e serão estudadas de maneira mais aprofundada, pois são objetos fundamentais na proposta do STRAYER.

A automação trata do controle de dispositivos inteligentes que comandam os equipamentos de campo, de forma automática, mantendo o pleno funcionamento do sistema elétrico. Para isso, utilizam-se lógicas de automação que são implantadas nesses dispositivos. São exemplos de dispositivos de automação: os Controladores de Automação, os Sincronizadores de Tempo (GPS), as Interfaces Homem-Máquina (HMI), as *Merging Units* (MU), além de sensores variados e os já mencionados IED's. Este último recebe a maior quantidade de lógicas de automação.

Sobre as lógicas, é importante salientar que para sua determinação, os estudos envolvem análise não só da rede de automação da *Smart Grid*, mas também, dos parâmetros de proteção. o segmento de proteção determina os valores de técnicos dos equipamentos de campo, como, por exemplo, nível de sobrecorrente dos disjuntores para sua correta atuação. Percebe-se então, que as lógicas de automação podem abarcar parâmetros de vários segmentos de *Smart Grid* (não só automação e comunicação).

Já na comunicação, há a "conversa" entre os mesmos dispositivos de automação, além de passagem de informação entre os equipamentos de campo e o centro de gestão dos ativos, como por exemplo, o Centro de Operações Integrado (COI). Os dispositivos de comunicação existentes em *Smart Grids* não são diferentes dos elementos de rede de computadores, como os roteadores, *switches* de nível 2 e 3 e meios físicos conhecidos, como os cabos de par trançado e óticos.

A conexão entre os barramentos de rede de uma *Smart Grid* é realizada por alguns protocolos de comunicação determinadas pela IEC 61850. Dentre os mais conhecidos estão os Eventos de Subestação Orientados a Objetos Genéricos (GOOSE), as Especificação de Mensagem de Fabricação (MMS) e as mensagens *Sampled Values* (SV), que serão objeto de análise mais adiante.

Sendo assim, a norma IEC 61850 trata a comunicação e a automação como um processo global e as designa como um sistema unificado, chamado de Sistema de Automação em Subestações - SAS [8]. Logo, todo o conjunto de dispositivos inteligentes e protocolos de comunicação de uma *Smart Grid* fazem parte do SAS, e, são essenciais para manter sua integridade operacional, tanto local quanto remotamente.

2.3.1 Níveis do SAS

Segundo a norma IEC 61850-1, dentro de uma subestação elétrica ou *Smart Grid*, o SAS pode ser dividido, de forma resumida, em três níveis que são interligados por barramentos [20, 3] conforme apresentado na Figura 2.3. Os níveis são descritos a seguir.

- **Nível de Estação:** Aqui se encontram os dispositivos de monitoramento, supervisão indireta da *Smart Grid*, para melhor gestão por parte do Centro de operações. É composto pela HMI (interface homem-máquina), sistema supervisório (SCADA), *switch* Ethernet e sincronismo de tempo via protocolo de comunicação.
- **Nível de Bay:** Nível de grande importância em quesito de comissionamento. É nesse nível onde se encontram os IED's e suas lógicas de controle e proteção implementadas e forma a realizar operações de comando nos equipamentos de campo.
- **Nível de Processos:** Por fim, os equipamentos de campo que realizam manobras, com os disjuntores e chaves seccionadoras motorizadas, estão nesse nível. Lembrando que é considerado apenas nesse nível, equipamentos que são controlado pelas IED's. Ou seja, equipamentos com possibilidade de acesso por rede, e na falta desse, que aceitem a digitalização através das *Merging Units*. Sensores e atuadores também se encontram nesse nível.

Os dois Barramentos interligam os três níveis e também possuem tráfego de protocolos de comunicação. Dividem-se em Barramento de Estação e Barramento de Processo. O Barramento de Estação interliga os níveis de estação e de *bay*. Por não haver comunicação direta entre os equipamentos de estação, o Barramento de Estação é responsável por essa tarefa. Isso é determinado pela IEC 61850, para evitar acesso indevido às interfaces desses equipamentos, mesmo quando um possível invasor adentre as instalações da *Smart Grid*.

Já o Barramento de Processo, interliga os níveis de *Bay* e de Processos. Sua função é mais complexa, já que a restrição de comunicação horizontal (de mesma hierarquia) do barramento anterior não existe. Porém, mesmo havendo comunicação horizontal entre equipamentos desses dois níveis, o Barramento de Processo prevê a comunicação vertical. Essa redundância é necessária, pois é nesse barramento que se encontram os dispositivos de conversão A/D, como as *Merging Units*. Colocando em termos gerais, só há a existência do Barramento de Processo se houver a MU. Senão, considera-se uma ligação analógica padrão das subestações elétricas.

Existe ainda uma subdivisão dentro dos níveis e barramentos do SAS, chamados de Nós Lógicos. Esse nós estão particionados em vários pontos dos níveis, entre cada equipamento ou dispositivo (que são os nós físicos). Esse nós lógicos possuem função de sincronização e chaveamento da automação, além de

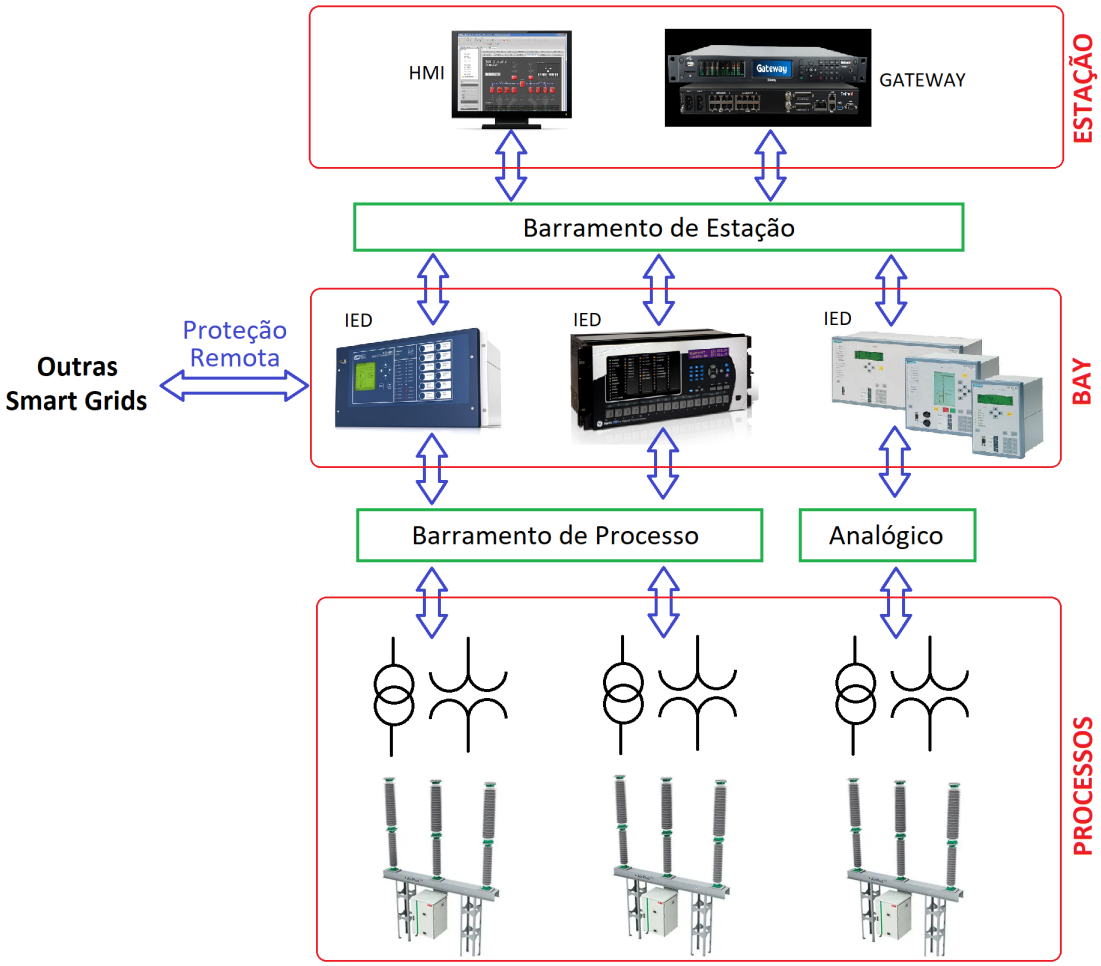


Figura 2.3: Níveis e Barramentos dos SAS. Adaptada de [3].

proteções básicas, como a de distância e de sobrecorrente [20]. Quando há a execução simultânea de duas ou mais funções em dois ou mais dispositivos, teremos uma função distribuída. A partir desse ponto, como há a comunicação entre várias funções distribuídas, não há mais uma definição individual, até que seja implementada propositalmente (*e.g.*, por um gestor de redes).

A comunicação entre os dispositivos e equipamentos se dá por meio de protocolos de mensagem, específicas par Subestações elétricas e *Smart Grids*. A subseção mais à frente tratará do funcionamento e responsabilidade dos tipos de mensagens.

2.3.2 Protocolos de comunicação do SAS, segundo a IEC 61850

Em relação à troca de informações entre equipamentos, existem dois tipos de mensagens principais: as GOOSE e as SV (*Sampled Values*). As mensagens GOOSE são utilizadas para troca de sinais de comando entre os IED's enquanto que as mensagens SV consistem na amostragem digital de uma grandeza analógica obtida de um transformador para instrumentos (tensão ou corrente) e sua transmissão para os dispositivos inteligentes. Existem ainda as mensagens MMS trocadas entre os IED's e os sistemas supervisórios através do Barramento de Estação [3].

- **Mensagens GOOSE**. Por recomendação da norma, as mensagens GOOSE são utilizadas para troca de sinais de comando entre IED's [26], independente se foram de mesmo fabricante ou não. Seu método de transmissão dar-se por *multicast*, e às vezes, *broadcast*, com limitação de pacotes. Encarregam-se do transporte das descrições SCD, com informações sobre eventos de atuação de proteção de subestações. As mensagens GOOSE utilizam protocolos UDP, para que haja transmissão rápida, porém, sem a verificação cíclica típica de protocolos TCP.

- **Mensagens MMS**. O processo das mensagens MMS é bem diferente do GOOSE. Justamente por esse motivo, que os dois protocolos devem se complementar. No MMS, é possível realizar a transmissão apenas por *unicast*. Além disso, ele trata apenas de informações dos IED's e demais dispositivos de automação. Ele alimenta as medições do supervisório SCADA e para clientes (se estiver configurado esse tipo de função).

- **Mensagens SV**. É possível citar que as mensagens SV possuem uma caráter mais operacional que os dois anteriores. Ele trata da reciclagem de informações analógicas, oriundas dos equipamentos de campo. Os equipamentos de campo de maior robustez, como transformadores e disjuntores, emitem sinais analógicos apenas pelos transformadores de instrumentação, no caso, os TC's e TP's. As mensagens SV simplesmente convertem essas informações analógicas (e de preciosa informação) para um formato digital no IED.

2.3.3 Engenharia de comunicação do SAS

A IEC 61850-4 exige que o SAS tenha alguns requisitos mais técnicos relacionados aos dispositivos que o compõe. Essa engenharia inclui as definições de *hardware* dos dispositivos e sua documentação, parametrização de configuração e operação, além da determinação das ferramentas de engenharia, previsão de flexibilidade e expansão, e, padronização da documentação de comissionamento.

2.3.3.1 *Hardware* necessário

A Figura 2.4 representa a estrutura de *hardware* exigida pela 61850-4. Ela define uma configuração de *hardware* dos IED's e suas interfaces, necessária para o SAS. Um outro ponto é a adaptação da funcionalidade e dos requisitos operacionais específicos para uso de parâmetros dos IED's, além de documentação de todas as definições específicas [4].

A norma sugere que, para os IED's sejam necessárias as existências de três ambientes de *hardware*: de telecomunicações, de HMI e de Processos. O ambiente de Telecomunicações envolve a adicção de *gateways*, conversores, unidade terminal remota (RTU) e os relés de proteção, propriamente ditos. O ambiente HMI detém tudo que concerne à visualização de parâmetros. Computadores, pessoais ou não, e estações de trabalho, fazem parte do rol desse ambiente. Finalmente, o ambiente de Processos contempla os controladores da *Smart Grid*, transdutores, medidores de grandezas elétricas, TC's e TP's digitais.

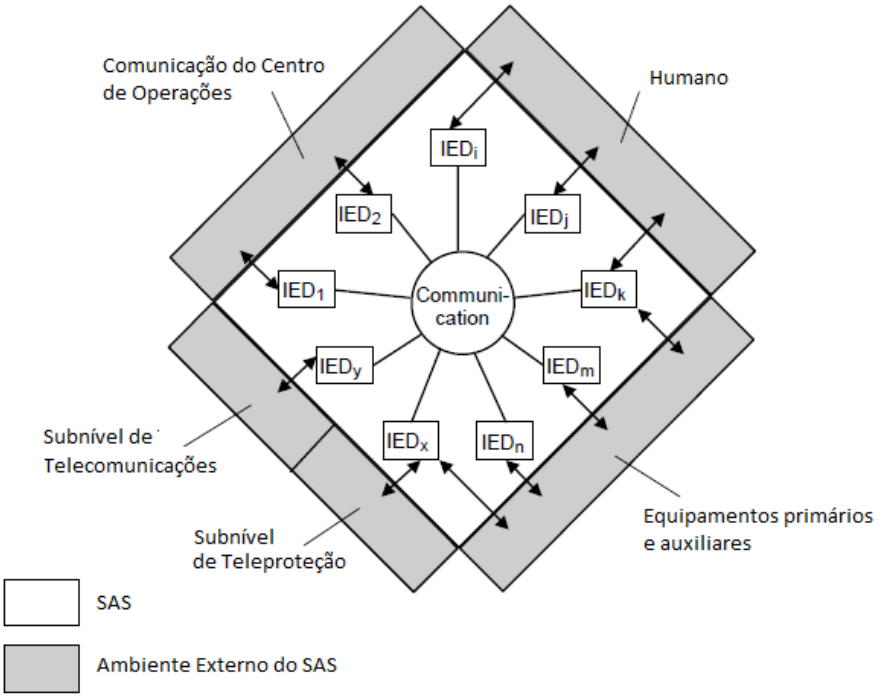


Figura 2.4: Estrutura inicial de engenharia do SAS. Adaptada de [4].

2.3.3.2 Parâmetros

Segunda a norma, os dados operacionais são considerados os parâmetros. Dados inerentes à configuração dos IED's e seus respectivos *softwares*, além das ferramentas de suporte do SCADA e do HMI. O conjunto total de parâmetros de um SAS é denominado Conjunto de parâmetros do SAS [4]. Trata-se do parcelamento dos parâmetros dos IED's.

Os parâmetros se classificam, segundo os precedimentos de manuseio e procedimentos, em: i) parâmetros de Configuração, e; ii) parâmetros de Operação. Os parâmetros de Configuração definem o comportamento global de todo o SAS e seus IED's. Como um regra, eles só recebem um valor durante a parametrização inicial, porém, deve ser atualizado se houver alteração no funcionamento do SAS. Esse processo deve ser realizado com o sistema desligado, de forma segregada. Durante a entrada dos parâmetros de configuração, a operação do SAS deve ser suspensa, por motivos de segurança. Os parâmetros Operacionais definem o comportamento das funções parciais do SAS. Ao contrário dos parâmetros de Configuração, podem ser alterados de forma *online* no que concerne ao funcionamento do SAS, mantendo seus requisitos operacionais.

Ainda há a categorização em relação à origem e função dos parâmetros. Estes podem ser divididos em: i) parâmetros de Sistema; ii) parâmetros de Processos, e; iii) parâmetros Funcionais.

Os parâmetros de Sistema determinam a cooperação entre os IED's, incluindo as estruturas internas e procedimentos de um SAS em relação aos seus limites tecnológicos e componentes disponíveis. Por exemplo, os parâmetros do sistema determinam a configuração dos componentes de *hardware* do SAS, (*eg.*, placas e IED's), o procedimento de comunicação entre os próprios IED's (*eg.*, protocolos e taxa de transmissão), e, o escopo das funções necessárias e disponíveis no *software* dos IED's no nível da estação

[4]. Além disso, os parâmetros do sistema descrevem as relações entre os dados de diferentes IED's.

Já os parâmetros de Processo determinam a troca de informações entre o SAS e o ambiente de Processos de Sistema. Se há uma dupla saída, como no caso das redundâncias dos IED's, há então uma relação de parâmetros de Processo. Eventos que indicam dupla saída de dados pertencem ao rol. Ele também é responsável pelos recursos qualitativos, como o tempo de saída/chegada de determinado comando remoto, supressão de eventos transitórios dentro do IED (eventos espúrios), entre outros. Além disso, os parâmetros do processo incluem a atribuição de textos a eventos para visualização no IED.

Por fim, os parâmetros Funcionais descrevem as características qualitativas e quantitativas que serão utilizadas na ponta da comunicação. Determinam as condições de *trip* dos relés de proteção, sequências automáticas de operações dos comandos, entre outros. Esse tipo de parâmetro também define o intertravamento entre os IED's e os ajustes de lógica e de proteção do SAS.

2.3.3.3 Ferramentas

As ferramentas são basicamente as condições do SAS para adaptação da filosofia de proteção em *Smart Grid*. Uma das ferramentas é o Projeto que contém *checklist* a funcionalidade do *hardware* dos IED's. O projeto é o processo inicial que determina tanto a ferramenta de Parametrização, quanto a de Documentação.

A ferramenta de parametrização suporta a criação do conjunto de parâmetros de origem consistente para todos IED's de um SAS. A ferramenta de parametrização pode ser dividida em ferramenta de parametrização geral, que gerencia os parâmetros do sistema no nível SAS, e, parametrização específica do IED, que tem a finalidade de gerenciamento dos conjuntos de parâmetros de IED autônomos. As principais tarefas da ferramenta de parametrização são a geração de listas de dados de processo com base em um conjunto de parâmetros de origem e o gerenciamento seguro das listas de dados do processo para o SAS e seus IED's [4].

Existem dois documentos para a parte de ferramentas: a Documentação de *hardware* e a de parâmetros. A documentação de *hardware* representa todas as conexões externas entre o SAS e o ambiente de Processos que são definidos no processo de concepção do projeto. A documentação de parâmetros apresenta todos os dados internos que são definidos no processo de parametrização.

2.3.3.4 Flexibilidade e Expansibilidade

Segundo a IEC 61850-4, a flexibilidade e Expansibilidade do SAS requerem a capacidade de expansão da configuração de *hardware* do SAS. A extensão flexível da configuração de *hardware* com os IED's adicionais ou com IED's de diferentes funcionalidades é o primeiro requisito para atender a flexibilidade e expansibilidade do SAS. Ambos também dependem das ferramentas de engenharia, como os *softwares* proprietários dos IED's.

2.3.3.5 Escalabilidade e Documentação de projeto

Para que haja Escalabilidade, a ferramenta de parametrização deve estar apta a ser utilizada por todos os *softwares* de um SAS. Geralmente, o SAS deve ser projetado para atender demandas de fabricantes, níveis elevados de *softwares*, complexidade e funções de telecomunicações, essencialmente.

Quanto à documentação de projeto, deve conter, no mínimo: diagramas unifilares e conexões externas, lista de lógicas de automação, arquitetura do SAS, configurações e ajustes, além da documentação relacionada ao *hardware* utilizado e a documentação de parâmetros.

2.4 INTEGRAÇÃO DE PARÂMETROS DO STRAYER

A união entre Segurança cibernética e Interoperabilidade já está consolidada pelas normas IEC 61850, desde sua concepção. Apesar de ser uma integração, a norma não trata como tal, sugerindo apenas a implantação de interoperabilidade entre sistemas no momento de criação de arquitetura de automação segurança em *Smart Grids*. Além disso, essa aliança não é imparcial, pois há sobreposição da interoperabilidade em detrimento da segurança. Não é determinado, por exemplo, sobre impacto negativo de segurança em detrimento de um aumento exponencial da interoperabilidade. A troca de informações de diferentes *hardwares* pode gerar corrompimento de dados a ajustes do SAS, deixando-os inutilizados.

Entretanto, a proposta do STRAYER consiste em adicionar o fator original de Gestão de Riscos à essa união já existente, dando valor assim ao termo “Integração”. Adicionalmente, tende a manter equilíbrio entre os três parâmetros unidos, de forma a manter a imparcialidade no processo de análise de ajustes e dados iniciais.

Semelhante ao processo de exposição do conceito de interoperabilidade, apresentado na seção 2.1.3, é necessário discorrer sobre a real função dos fatores de Segurança Cibernética e Gestão de Riscos, para melhor entender o conceito do STRAYER.

2.5 SEGURANÇA DE REDES E SEGURANÇA CIBERNÉTICA

A Segurança de redes é um ramo da segurança da informação que trata sobre comunicação segura entre dois pontos. Em sua forma mais simplificada, segundo Tenenbaum [27], a segurança de redes visa o impedimento de um terceiro mal-intencionado em verificar, ler ou modificar informações referentes à uma comunicação ponto a ponto. Isso pode ser dar diretamente à conexão da comunicação ou de forma remota. O mesmo autor divide os problemas de segurança de redes em áreas interligadas, sendo elas:

- ***Sigilo ou Confidencialidade*** - relaciona-se com o fato de manter as informações protegidas contra usuários sem autorização [27];
- ***Autenticação*** - é o processo de determinação e identificação de usuários, antes da comunicação entre ambos [27];

- ***Não repúdio*** - esse segmento trata da veracidade das informações, ou da prova das requisições de informações [27];
- ***Integridade*** - uma vez que a comunicação já está estabelecida, deve-se verificar a integridade das mensagens recebidas [27].

Jim Kurose, autor bastante conhecido, em sua obra, adiciona que a segurança de redes é um mecanismo sistêmico, o que é chamado de Segurança Operacional [28]. Funciona da seguinte forma: se todas as organizações, sejam empresas ou universidades, que detém informações precisam se comunicar pela Internet pública, invariavelmente, suas respectivas redes podem ser comprometidas por atacantes por meio desse mesmo caminho. E que a solução mais prática, seria a imposição de "portas grossas" na entrada da Internet para cada organização [28]. Hoje, sabemos que essas tais portas se tratam dos *firewalls* e sistemas de detecção de intrusão das empresas. Tendo isso em vista, o autor adicionou esse conceito em sua divisão de problemas de comunicação segura. Para Kurose, divide-se em:

- ***Confidencialidade*** - apenas o remetente e o destinatário devem entender o conteúdo da mensagem transmitida [28];
- ***Integridade de mensagem*** - semelhante ao conceito de Tenenbaum, é a manutenção da integridade da mensagem transmitida, sem interferência de terceiros [28];
- ***Autenticação do ponto final*** - é a imposição de mecanismos para a identificação das partes comunicantes, inclusive, para terceiros, sejam bem ou mal intencionados [28];
- ***Segurança Operacional*** - Trata da unificação das três divisões anteriormente mencionadas, com a adição de soluções tecnológicas para as organizações, protegendo suas bordas de rede [28]. Instalação de filosofias de segurança cibernética faz parte dessas soluções.

Já Goodrich, de maneira mais técnica, prediz que Internet já estava projetada de forma que a comunicação seria de forma gradual e finita, no formato de pacotes de dados (e não de mensagens) [5]. Esse pacote de dados divide-se em *header* (cabeçalho) e o *payload* (corpo da mensagem com os dados da aplicação). Na comunicação entre dois pontos pela Internet é necessário que os usuários devam emitir suas mensagens em pacotes, anexando um cabeçalho (que contém informações de endereçamento de cada usuário) na frente de cada outro existente, a medida que a mensagem vai passando pelas camadas do modelo TCP/IP, e depois deixar que esses pacotes encontrem o seu caminho pela Internet para chegar ate seus respectivos destinos [5]. A Figura 2.5 apresenta o encapsulamento de pacotes.

O autor ainda adiciona mais elementos à divisão preconizada por Kurose. Segundo Goodrich, os problemas causados por vulnerabilidades da Internet afetam os objetivos da segurança de redes. Sendo assim, o autor dividiu os objetivos conforme abaixo:

- ***Confidencialidade*** - trata-se da manutenção dos pacotes de dados transmitidos. Os cabeçalhos são o cartão de visitas de toda a carga, e por isso, devem se manter confidenciais, para cada usuário [5]. Esse processo é realizado por encriptação;

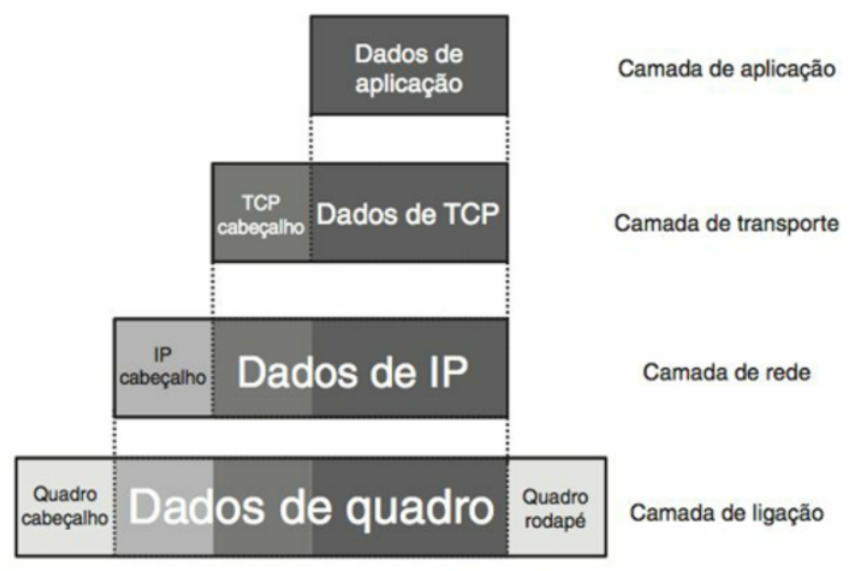


Figura 2.5: Encapsulamento de pacotes nas camadas da pilha de protocolos TCP/IP [5].

- ***Integridade*** - para que se mantenha a integridade dos pacotes de dados, é necessário manter a verificação de soma (*checksum*), existente na estrutura do cabeçalho [5];
- ***Disponibilidade*** - Mesmo com a robustez da Internet, essa não consegue suprir toda a necessidade de disponibilidade de forma contínua [5]. Evitar ataques que visam o comprometimento de servidores é essencial para a disponibilidade da rede. Junto com a Confidencialidade e a Integridade, foram a tão famosa sigla "CID", conhecido no meio da segurança da informação;
- ***Garantia*** - A garantia trata do acesso privilegiado dos administradores de rede. Se houver uma filosofia de restrição perfeita, como os gestores de rede poderiam ditar as regras de acesso? Deve-se manter o privilégio restrito com auxílio da Autenticidade [5];
- ***Autenticidade*** - Goodrich expôs um problema na troca de mensagens de baixo nível: a impossibilidade de autenticação nas camadas mais baixas da pilha de protocolos. A autenticação deve ser realizada ainda nas camadas mais altas, com a de Aplicação [5];
- ***Anonimato*** - O Anonimato é comum na Internet [5]. Porém, para este caso, é necessário ter o cuidado para não permitir acesso anônimo à certas aplicações sensíveis, pois pode-se atacar uma rede, informando ser outro usuário.

O amplo conceito de segurança de redes, independente do autor, é abarcado por seu meio de execução mais comum: a Criptografia. Técnicas criptográficas permitem que um usuário disfarce os dados de uma mensagem de forma que um intruso, mesmo tendo sucesso na abordagem indevida, não consiga obter a informação nela contida [28]. Apenas o destinatários, dependo da técnica empregada, poderá revelar a informação e determinar sua veracidade. Sem fazer uma extensão das técnicas, a saber, as mais comuns são as de: criptografia de Chave Simétrica, criptografia de Chaves Públicas (ou Assimétricas), funções *hash* criptográficas e assinaturas digitais.

Sendo assim, com a evolução das técnicas de criptografia e ampliação da gama de quesitos de segurança de redes, percebe-se então que era necessário a criação de técnica e políticas de segurança mais robustas para atendimento de sistema interligados e distribuído. A segurança Cibernética foi conceituada a partir desse ponto, pois essa evolução foi necessária devido à complexidade dos ataques cibernéticos, que estavam cada vez mai adaptados à contramedidas.

Portanto, Segurança Cibernética é um braço da segurança de redes, que visa a determinação de políticas, modelos e gerenciamento das informações por meio de *framework* ou outras especificações técnicas para mitigação de ataques e revisão das vulnerabilidades. Os *frameworks* sugerem uma série de ações que vislumbram o modelo de controles de acesso, padrões de segurança e de avaliação de vulnerabilidades de *software* e *hardware*, além de administração e auditorias.

Talvez o *framework* de Segurança Cibernética mais conhecido e o mais seguido por administradores de rede é o divulgado guia de infraestrutura crítica do NIST [7]. O documento apresenta uma Estrutura Básica, que é uma lista de Funções, Categorias, Subcategorias e Referências Informativas que descrevem atividades específicas de segurança cibernética, comuns em todos os setores com infraestrutura crítica [7]. Trata-se de um grande compilado de referências normativas que auxilia na normatização das funções pré definidas de ações de segurança cibernética. Uma referência normatiza é determinada de acordo com cada função, categoria e subcategoria utilizada.

As funções do *framework* do NIST estão apresentadas abaixo, conforme descrito explicitamente no próprio documento:

- ***Identificar* (ID)** - Essa função tem a finalidade de compreender os riscos de segurança cibernética nas peças organizacionais de uma empresa, tais como os seus recursos e colaboradores. Entendendo a sua área de atuação, a organização tem a capacidade de direcionar o seu esforço de segurança nos seus ativo mais críticos. Segundo o *framework*, a função Identificar abarca a avaliação e gestão de risco e ambiente da empresa com sua governança.

- ***Proteger* (PR)** - A função de Proteger garante a continuidade dos serviços executados por determinada organização por meio de mitigação de possíveis ameaças à segurança da cibernética. Ela determina as regras de controle de acesso nas empresas, além procedimento para melhor proteção dos dados. Também faz parte do escopo da função, o devido treinamento das pessoas sobre segurança cibernética.

- ***Detectar ou Diagnosticar* (DE)** - Como o próprio nome já revela, trata da identificação de possíveis ameaças à segurança cibernética, diferente da função Proteger, que visa a mitigação do próprio ataque. Processos de detecção e monitoramento dos sistemas fazem parte dessa função.

- ***Responder* (RS)** - A função Responder visa a minimização dos efeitos de uma ataque bem sucedido. Os incidentes de segurança cibernética devem ser avaliados e deverá ser realizado um plano de ação com análises e aperfeiçoamentos das contramedidas.

- ***Recuperar* (RC)** - Essa função trata do restabelecimento rápido dos sistemas de uma organização, após um evento de segurança cibernética. Envolve um planejamento de recuperação de dados e retorno das redes e seus referidos recursos, em um menor tempo possível.

São várias as referências Normativas determinadas pelo NIST. No Anexo VI do Apêndice, é apresentado todo o rol determinado pelo guia, com suas respectivas funções, Categorias e Subcategorias que ligam às Referências técnicas.

2.5.1 Políticas de Segurança da Informação

A segurança da informação é um assunto delicado que deve ter suas regras bem definidas em documentos oficiais que irão nortear a sua gestão de forma ideal. A seção 5 da norma IEC 27002 induz que deve ser criado um documento que trata sobre a política de segurança da informação em empresas que detenham informações sigilosas e essenciais. A documentação deve conter os conceitos de segurança da informação, uma estrutura para estabelecer os objetivos e as formas de controle e mitigação de riscos, além de compromisso oficial da alta direção das empresas com as políticas de segurança da informação [29].

Os objetivos que se encontrarem nessa documentação, devem ser seguidos estritamente, por todas as pessoas envolvidas na segurança da informação, com atribuição de responsabilidades. Vale ressaltar que essas regras também deve seguir as normas oficiais de tratamento e *compliance* de dados de cada país. No caso do Brasil, a norma oficial é Lei Geral de Proteção de Dados (LGPD).

Uma vez definida a política de segurança, em sequência, deve-se atender aos requisitos organizacionais de segurança das empresas. A seção 6 da IEC 27002 sugere que para a implementação da segurança da informação, é necessário estabelecer uma estrutura de gerenciamento, com coordenação e responsabilização direta por representantes das empresas.

2.5.2 Controle de Acesso e uso da Autenticação

Tanto o acesso à informação quanto aos recursos das empresas, devem ser controlados com regras de controle, através de Autenticação. Deve ser permitido o acesso de usuário com a devida autorização e negada o acesso não autorizado e prevenido o acesso não autorizado a sistemas de informação. A finalidade central da Seção 11 da IEC 27002 é de proteção dos dados, enquanto que para o contexto das *Smart Grids*, é a prevenção de ataques cibernéticos e invasões aos COI's.

É possível realizar esse controle através de técnicas de Autenticação (que faz parte do conceito de Segurança cibernética). Para o caso de prevenção de ataques, pode-se utilizar a Autenticação do Ponto Final [28]. Este é um processo de prova de identidade entre entidades de determinadas redes de computadores ou sistema inteligentes. Ele visa a verificação,não só ´de dados pessoais do usuários, mas identificação por dados sensíveis, tais como: biometria, identificação facial e até mesmo por voz.

2.6 GERENCIAMENTO DE RISCOS

Parte fundamental na governança de qualquer empresa ou grande organização, a Gestão de Riscos têm ganhado mais relevância justamente por sua aplicação no setor de segurança da informação. Segundo a norma IEC 27002, é essencial que uma organização identifique e avalie os riscos, entenda as legislações

em vigência, e, levante todos os seus ativos de negócio para manuseio e processamento correto de operação dos mesmos [29].

Entender a definição de Risco é o primeiro passo para conhecer todo o potencial de seu gerenciamento. Risco é um desvio incerto do que se é esperado de objetivos (6). Assim sendo, a Gestão de Riscos se conceitua como um conjunto de atividades ou ações, visando direção e controle dos riscos. É de salientar que os riscos sempre existirão, sendo praticamente impossível sua inteira mitigação porém, é possível seu gerenciamento.

A norma ISO 31000, um dos padrões vigentes sobre diretrizes de gestão de riscos no Brasil, sugere que as empresas devam se basear nos princípios, estrutura e processo de gestão. Trata-se de uma metodologia cíclica e contínua de melhorias com intuito de sempre manter a iteratividade do controle. O conceito é apresentado graficamente pela Figura 2.6.

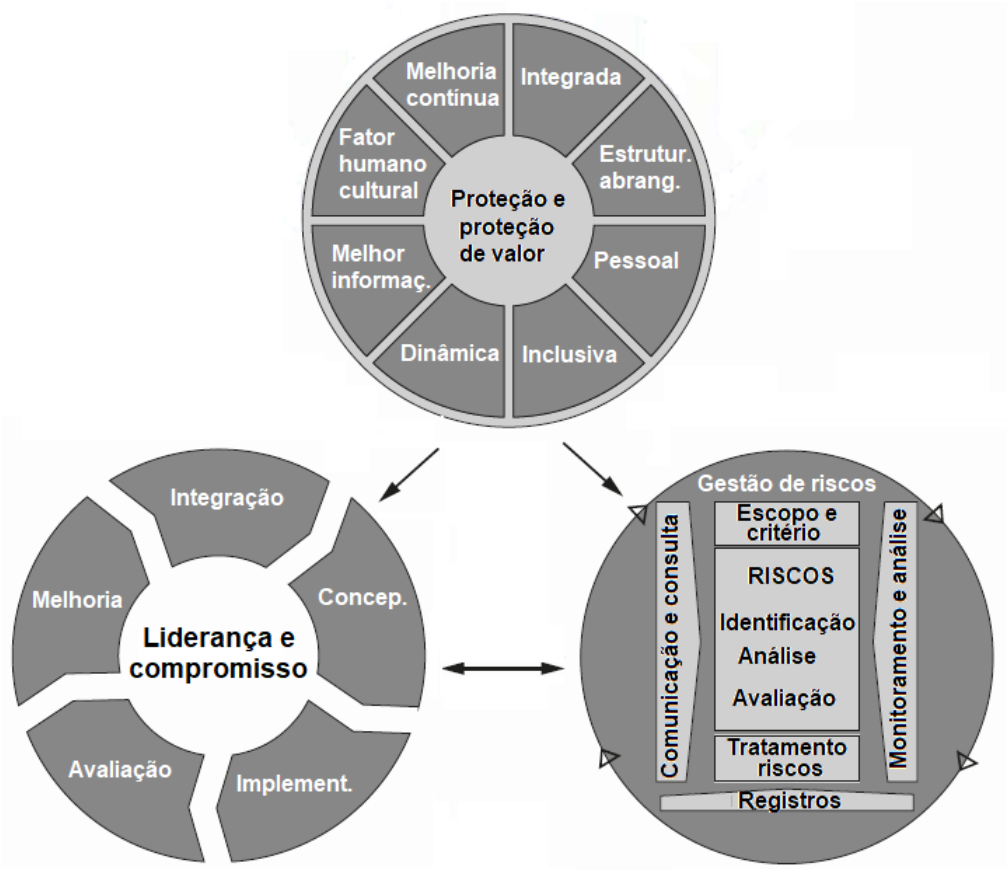


Figura 2.6: Princípios, Estrutura e Processos da gestão de riscos. Adaptada de [6].

Uma vez que há o entendimento do conceito de gestão de riscos, é possível verificar sua aplicabilidade nas instalações e redes do setor elétrico de maneira geral, fazendo uma análise preliminar dos riscos à segurança das *Smart Grids*.

2.6.1 Riscos de segurança da informação no Sistema Elétrico

À época dos subestações elétricas analógicas, as comunicações através dos rádios e unidades de terminais remotos eram os únicos dispositivos digitais, de certa forma, capazes de realizar algum processamento de dados. Eram dispositivos muito lentos, porém, pode-se dizer que eram bastante resistentes à interferências externas, justamente por seu isolamento tecnológico. A evolução para comunicação em fibra ótica e equipamentos mais robustos não, foi necessariamente, o problema de vulnerabilidade no sistema de comunicação em subestações, e sim, a interligação entre elas.

Técnicas de *smart metering* e interconexões entre subestações digitais, abriram o caminho para invasões, que de certa forma, também se fazem de maneira digital. Essa abordagem foi um dos primeiros fatores tratados como risco nas instalações de fornecimento de energia elétrica no mundo. Além disso, não havia um controle do quantitativo de ativos analógicos ou digital (nem a diferenciação dos mesmos), o que facilitava o descontrole dos processos de gestão dos equipamentos. Adicionalmente, também não existia um procedimento básico de resposta à ataques cibernéticos e de controle de acesso ao Centro de Operações de maneira eficaz. Esses riscos não tinham o devido tratamento.

Dois documentos relacionados à rotinas de boas práticas de segurança cibernética no setor elétrico trouxeram embasamento na montagem de rotinas de gestão de vulnerabilidades. O primeiro se trata do Módulo 5 - Submódulo 5.13 do Manual de Procedimentos da Operação do ONS (Operador Nacional do Sistema Elétrico). Ele discorre sobre procedimentos de elaboração de uma série de instruções padronizadas e sua implantação. Os procedimentos são: Cadastros de Informações Operacionais, Instruções de Operação, Mensagens Operativas, Rotinas Operacionais, Ajustamentos Operativos, além de Referências Técnicas sobre o assunto relacionado ao setor de energia brasileiro [30].

O manual segue o rito semelhante ao *Framework* do NIST, apontando uma série de outras normas, dependendo do perfil que determinado Centro de Operações das concessionárias adotar. Funciona como um *survey*, voltado apenas para o setor de supervisão e controle do sistema elétrico brasileiro.

O segundo documento, de caráter mais normativo, é o ANSI/ISA 95.00.01 que trata sobre levantamento de riscos voltado para área empresarial. Visa a defesa dos ativos e patrimônio das empresa concessionárias de energia ou demais setores. Tem o objetivo de aumentar a uniformidade e determinação de riscos reduzi-los, além de redução de custos e erros. A norma pode ser usada para reduzir o esforço associado à implementação de um novo produto, além de facilitar a interoperabilidade entre sistemas corporativos e sistemas de controle [31].

2.6.2 Gestão dos ativos do Setor elétrico

Gestão de riscos envolve avaliação dos recursos, e principalmente, dos ativos. A norma IEC 27002 determina as melhores práticas para apoiar a implantação do Sistema de Gestão de Segurança da Informação (SGSI), que visa a avaliação sucinta de todos os ativos de governança de empresas, entre elas, as concessionárias de energia elétrica.

Todas as seções da referida norma, têm importância especial no que se refere ao controle de ativos das *Smart Grids*, porém, é dada uma ênfase à seção 7. Esta determina sobre as práticas de identificação de

ativos. Um Ativo, é qualquer coisa que tenha valor para a organização e que precisa ser protegido [29]. Mas para isso, eles devem ser identificados e classificados para a formação de um inventário que possa ser estruturado e mantido. A formalização das regras é de extrema importância pois define qual o uso para cada tipo de ativo e a permissão para tal.

Sempre nos levamos a pensar no ativo como uma coisa material, tal como uma estrutura física, um disjuntor, um transformador ou equipamento afim. Porém, há de salientar que o principal ativo de uma empresa, até mesmo de *Smart Grids*, não são os equipamentos, e sim, as pessoas. A seção 8 da IEC 27002 preconiza que as pessoas que irão se envolver na operação de informações sigilosas ou sensíveis (*eg.*, operadores do COI), devem passar por uma análise minuciosa antes da realização de sua contratação [29]. Isso deverá acontecer não só com o ambiente interno, mas externo também, como os fornecedores e até mesmo, clientes. A intenção desta seção é mitigar o risco de roubo de recursos ou informações e ataques internos.

3 TRABALHOS CORRELATOS

Nas atuais literaturas, existem trabalhos relacionados ao aumento do desempenho de segurança de redes em *Smart Grids* relacionados aos mais variados ataques cibernéticos, tanto local quanto remotamente. Essas pesquisas utilizaram diversas técnicas para tentar chegar a uma solução robusta contra intrusões em seus sistemas de automação e comunicação. Este capítulo se dedica à exposição desses trabalhos. Serão apresentadas as referidas pesquisas mais proeminentes no campo de segurança de redes de automação e comunicação em subestações elétricas analógicas e em *Smart Grids*, reais ou virtualizadas.

3.1 SOLUÇÕES EM RECENTES PESQUISAS

De forma padronizada, Lázaro *et al* [16] apresentam uma série de soluções que visam garantir a comunicação entre *Smart Grids*, atendendo aos requisitos estabelecidos na IEC 62351-6 com ênfase na troca de mensagens entre todos os equipamentos. Mesmo com a robustez do trabalho, a pesquisa não apresenta soluções voltadas à segurança do SAS.

Faquir *et al* [17] utilizaram diversas soluções existentes para proteção de redes de TI utilizando IoT (*Internet of Things*), como os *firewalls*, IDS/IPS, acesso remoto via VPN, entre outros. Apesar de ainda ser uma prática bastante robusta de proteção na rede das concessionárias de energia elétrica, não foi possível observar uma melhoria no sistema de segurança da rede de TO nem mesmo no sistema de proteção do IED.

Os principais problemas de um sistema de monitoramento em subestações elétricas, com ênfase em comunicação e segurança cibernética foram apresentados por Yang *et al* [18]. O trabalho consistiu em padronizar, de forma estática, soluções de monitoramento. A solução baseia-se na manutenção de atualizações de dados em *Smart Grids*, apenas com o recurso de segurança (sem gerenciamento de riscos ou interoperabilidade), mantendo apenas uma arquitetura básica de automação. Como os ataques cibernéticos estão em constante evolução e estão mais dinâmicos, manter um método estático abriria brechas para problemas futuros.

Vardhan *et al* [19] projetaram uma *Smart Grid*, seguindo o "estado da arte" conceitual. O projeto consistiu na criação de uma subestação elétrica digital piloto, com comunicação entre dispositivos no barramento de processo por meio de mensagens SV [32], com o objetivo de comparar os resultados com subestações elétricas tradicionais. Apesar de promissor, o conceito criado contou com a implementação de equipamentos e sensores digitais de alto custo nos poucos equipamentos de comutação analógicos. O projeto também utiliza uma arquitetura básica, sem adaptações na topologia de automação e comunicação, não sendo possível perceber implementações eficientes de segurança cibernética.

Em seu trabalho, Fontes [21] apresentou um protótipo através de uma plataforma de testes, denominada LabProtec, para projetar uma infraestrutura para diversos testes em subestações elétricas digitais com a aplicação da norma IEC 61850. Os testes visam facilitar o processo de comissionamento de subestações digitais por meio de testes de bancada de configurações e ajustes de proteção e automação. Foram utilizadas

diversas modificações de arquiteturas e equipamentos de diferentes fabricantes, resultando em parâmetros de interoperabilidade e segurança cibernética. Como o trabalho apresentou um protótipo de plataforma, não foi possível verificar os resultados do projeto de uma plataforma física real ou menção estratégica de gerenciamento de risco. No entanto, o trabalho deixou espaço para conceituar o projeto de integração de informações (segurança + interoperabilidade).

Heinisch *et al* [33] apresentaram uma proposta em relação ao monitoramento de ameaças externas em *Smart Grids*. Na forma de projeto piloto, o trabalho realizado por uma concessionária de distribuição de energia elétrica consistiu no desenvolvimento de um aplicativo para registro de parâmetros de segurança em tempo real em uma *Smart Grid* digital virtual. No entanto, não foi apresentado no trabalho, uso prático desses registros em possíveis ataques reais, nem dados de gerenciamento de risco. A aplicação de trabalho ainda não atingiu o estágio de ambiente controlado em uma *Smart Grid* real ou apresentação de uma arquitetura digital.

Lellys *et al* [34] focaram na solução de interoperabilidade entre equipamentos de diferentes fabricantes. Apresentaram resultados de casos ao redor do mundo e arquitetura simplificada baseada na IEC 61850, a partir do barramento de processos, através do uso de dispositivos MU, digitalizando assim uma subestação elétrica comum. Embora a apresentação dos resultados seja promissora, não foram relatadas soluções práticas em testes de lógica do SAS (sobre interesse de interoperabilidade) ou identificação de formas de abordar o risco de vulnerabilidades a ataques cibernéticos inerentes a dispositivos MU de alto tráfego de dados.

Outros estudos apresentam resultados em projetos piloto, como demonstrado por Kimura *et al* [35] no Brasil. Ge Li-Qing *et al* [36], sugeriram a integração dos sistemas de monitoramento, erro e decisão de *Smart Grids* em sua plataforma. Vicente [9] propôs uma visão abrangente da interoperabilidade em seu trabalho, com foco na troca de informações sobre relés de proteção de diferentes subestações elétricas e universalização da comunicação horizontal através de mensagens GOOSE. Apesar de promissores, não apresentam correlação ou similaridade com a proposta da STRAYER em termos de gerenciamento de risco em suas plataformas ou, apresentação de dados de validação em comum com o proposto neste trabalho. O trabalho de Pandey [37] descreve uma série de possíveis problemas em estruturas de *Smart Grid* relacionados a ataques cibernéticos e outros problemas, e, sugere uma solução mais eficiente.

3.2 DISCUSSÃO SOBRE OS TRABALHOS

É perceptível que o grande foco na segurança dos sistemas de automação e comunicação nos trabalhos citados relaciona-se com emprego separado de soluções, de maneira independente. Houve uma grande evolução no sentido de detecção de ataques, especificamente aplicados nos equipamentos de subestações elétricas.

Muitos incluíram defesas até mesmo nos dispositivos de supervisão, como os HMI's e equipamentos de troca de pacotes na entrada das *Smart Grids*. Em várias soluções, foi aplicada a versão padrão de interoperabilidade exigida pela norma IEC 61850, que "obriga" a comunicação entre os IED's pelo protocolo da mesma norma.

Porém, diferentemente das referidas pesquisas, a arquitetura proposta pelo STRAYER utiliza o conceito de solução integrada, unindo parâmetros que solucionam problemas de ataques cibernéticos com gerenciamento de riscos e, ao mesmo tempo, interoperabilidade para que a arquitetura fique completa. Além disso, o STRAYER exige requisitos mínimos de configuração na arquitetura SAS, vinculando assim uma situação padrão de *Smart Grid* com parâmetros necessários de segurança e operabilidade, independentemente do tamanho da planta ou da carga elétrica da *Smart Grid*.

A Figura 3.1 representa um comparativo entre os trabalhos comentados acima, no que se refere aos fatores que estarão presentes no STRAYER. Nota-se uma ausência de aplicação direta de gestão de riscos em todas as soluções pesquisadas, sendo que apenas uma sugeriu alteração de arquitetura do SAS.

Autores	Foco de pesquisa	Aplicação			Arquitetura adaptada
		interoperabilidade	Segurança Cibernética	Gestão de Riscos	
Lázaro *et al* [16]	Comunicação entre SG	X			**Não**
Faquir *et al* [17]	Proteção da rede TO/TI		X		**Não**
Yang *et al* [18]	Segurança na Supervisão	X	X		**Não**
Vardhan *et al* [19]	Contrução de uma SG conceitual	X	X		**Não**
Fontes [21]	Protótipo de testes conceitual	X	X		**Sim**
Heinisch *et al* [33]	Ameaça externa às SG	X	X		**Não**
Lellys *et al* [34]	Interoperbilidade entre IED's	X			**Não**
Kimura *et al* [35]	Contrução de uma SG conceitual	X	X		**Não**
Ge Li-Qing *et al* [36]	Protótipo de Supervisão		X		**Não**
Vicente [9]	Comunicação segura entre IED's	X	X		**Não**
Pandey [37]	Melhoria de solução já existente em SG		X		**Não**

Figura 3.1: Comparativo entre as soluções pesquisadas.

4 UMA ARQUITETURA DE AUTOMAÇÃO ADAPTADA PARA *SMART GRIDS* CONTRA ATAQUES CIBERNÉTICOS

Este capítulo apresenta o STRAYER, uma solução adaptada para a arquitetura do SAS da *Smart Grids*. Para a modelagem do STRAYER, foram utilizadas adaptações nas redes de comunicação e automação da arquitetura delineadas pelas normas IEC 61850 além de mais dispositivos de segurança, redundância e separação das redes de operação em *Smart Grids*. É de salientar que as normas IEC 61850 não apresentam uma arquitetura propriamente dita, mas desenvolvem de como uma deve ser, de forma padronizada. O principal objetivo da STRAYER é manter a integridade do sistema de automação e comunicação dessas estruturas e, portanto, a continuidade das mesmas e o pleno funcionamento dos serviços essenciais à população que a utiliza.

Para facilitar o entendimento do STRAYER, é necessário apresentar o modelo arquitetônico de automação tradicional e suas brechas. Com isso, será possível demonstrar a cobertura das lacunas que os modelos tradicionais deixam, através da solução proposta. A seguir, serão demonstradas o funcionamento de uma arquitetura tradicional do SAS e a proposta do STRAYER.

4.1 ARQUITETURA TRADICIONAL DO SAS

Mesmo após a consolidação da IEC 61850 em 2004 [8], levou-se muito tempo para que o setor de energia elétrica percebesse a importância da segurança cibernética no contexto prioritário das subestações elétricas. O tema só foi implementado substancialmente após os ataques às plantas ao redor do mundo, que vem ocorrendo a partir de 2015. Diversas pesquisas foram realizadas para o desenvolvimento de arquiteturas para este fim. Foi um grande passo, mas as arquiteturas visavam apenas os testes de interoperabilidade de equipamentos de diferentes fabricantes e testes lógicos que compõem o SAS.

A norma IEC 61850 define parâmetros para uma arquitetura tradicional básica a fim de transformar uma subestação elétrica analógica em uma *Smart Grid* digital, conforme apresentado na Figura 4.1. Os conceitos de *Smart Grids*, via de regra e conforme definido no Capítulo 2, possuem três camadas: (i) Camada de Estação; (ii) nível da baía; e (iii) Nível de processo. Esse modelo é uma arquitetura tradicional utilizada atualmente em diversas estruturas digitais para aplicação dos conceitos básicos do padrão.

Ainda no contexto de *Smart Grid*, são compostos pelos IED's (Rótulo A, Figura 4.1). Esses dispositivos são responsáveis pelos comandos dos equipamentos do Nível de Processos, tais como Transformadores de Potência, Transformadores de Potencial e de Corrente e Disjuntores (Rótulo B). Como tal, eles se tornam os principais alvos de ataques cibernéticos, pois são os equipamentos detentores do pleno funcionamento do serviço de fornecimento de energia elétrica.

Na arquitetura do SAS tradicional, os IED's se comunicam com apenas um concentrador (Rótulo C),

sem qualquer redundância com outros *switches* da mesma ou de outra *Smart Grid*. Cada *switch* se interconecta com vários IED's através de apenas uma porta por dispositivo. Dependendo do tamanho do *frame*, podem haver mais *switches* para a mesma finalidade. A norma IEC 61850 sugere que esses vários elementos da camada dois, estejam interconectados para que um anel de comunicação seja criado entre eles. Essa comunicação é feita via fibra óptica, comumente com velocidade *Fast* Ethernet e usando mensagens GOOSE. Além disso, pelo menos um desses dispositivos se comunica com um principal (Rótulo D), que levará as informações ao COI (Centro Integrado de Operações), que detém função de supervisão geral do funcionamento das *Smart Grids*.

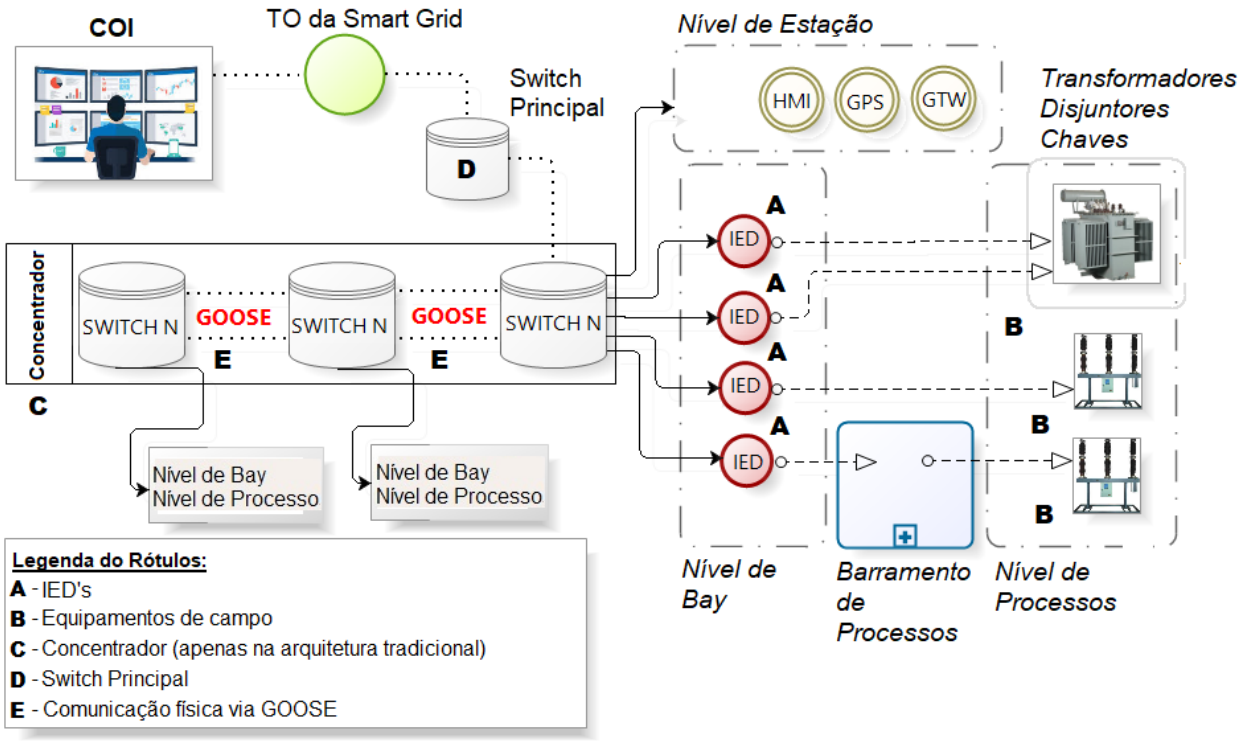


Figura 4.1: Exemplo de arquitetura de SAS tradicional.

Em relação aos protocolos de comunicação, os mais utilizados em *Smart Grids*, tradicionalmente, são o GOOSE ou GSSE (Generic Substation State Events), dispostos na cláusula 6.4 da norma IEC 61850-8-1 [38]. Esse protocolo é utilizado para comunicação horizontal (entre equipamentos de mesma hierarquia) e vertical (por subordinação), principalmente na comunicação horizontal entre *switches*, conforme mostrado no Rótulo E da Figura 4.1. É comum a comunicação estritamente vertical utilizar Modbus, DNP (*Distributed Network Protocol*), ou mesmo o protocolo legado ML7870. Além disso, para sincronismo de *timestamp*, o protocolo IRIG-B (*Inter-Range Instrumentation Group* - código B) é o mais utilizado em um barramento específico para esta finalidade. Embora as normas IEC 61850 indiquem o uso de mensagens GOOSE e SV, elas o fazem de forma padronizada por separação, sem a possibilidade de uso redundante desses mesmos protocolos.

A simples aplicação das normas IEC 61850 na arquitetura tradicional já traz diversos benefícios ao SAS das *Smart Grid*. A principal contribuição é uma linha de *switches* interligados em um anel para criar um concentrador. Isso facilita a comunicação entre IED's e equipamentos de configuração de *timestamp*, como o GPS. O problema dessa arquitetura tradicional, mesmo aplicando o padrão puro, é que existem

várias situações de vulnerabilidade, tais como:

- A perda de uma das portas do *switch* de borda;
- Perda ou queima de porta de comunicação com o IED no *switch*, ou;
- Falta de integração total entre os IED's.

Tais problemas podem culminar na perda parcial ou total da operacionalidade do supervisório (pelo COI) e deixar muitas brechas de segurança, como a fragilidade de acesso à rede operacional e abertura para interceptação de mensagens e vulnerabilidade do servidor. Estes podem causar a exposição dos IED's e, consequentemente, dos equipamentos de campo da *Smart Grid*. O desafio da pesquisa proposta é mitigar os problemas citados acima, demonstrando uma nova arquitetura que será apresentada a seguir.

4.2 ARQUITETURA ADAPTADA DO SAS PELO STRAYER

O STRAYER foi desenvolvido em uma adaptação avançada e segura do modelo básico de arquitetura SAS especificadas pela norma IEC 61850, usadas atualmente, realizando os devidos ajustes. Manter as recomendações que a norma exige, tais como i) interligação entre os barramentos de Processo da *Smart Grid*; ii) o uso de mensagens GOOSE e; iii) uso de um modelo SAS de três níveis (Estação, de *Bay* e Processos). A proposta integra elementos de segurança, com o objetivo de identificar formas de mitigar vulnerabilidades e riscos relacionados ao alto tráfego de dados em situações de emergência na troca de informações entre os diversos equipamentos de *Smart Grids* como IED's, barramentos de alta e baixa tensão e configurações de proteção, e os sistemas envolvidos (como outras estruturas interligadas externamente), o COI e as redes de TI/TO das concessionárias de energia. Portanto, o STRAYER apresenta um design de variações dinâmicas com mais redundâncias do que a arquitetura SAS tradicional.

A Figura 4.2 mostra o fluxo lógico operacional do STRAYER. O fator Gestão de Riscos está basicamente em todo o processo, porém, com ênfase na Entrada de Dados e Ajustes, no processo de Análise de Dados e Retroalimentação do Risco. A Análise de Dados é realizada nos dados fornecidos. Com isso, os dados passam por um novo processo de análise de risco e são retroalimentados no Integrador, possibilitando a mesclagem dos parâmetros em questão.

O processo do Integrador revela onde dois dos três parâmetros são unidos. Há um grande esforço computacional neste ponto, que exige equipamentos com alto fator tecnológico e de processamento. Na prática, acontece a simples união entre os fatores de Interoperabilidade e Segurança Cibernética. Ao final do fluxo, os dados estão ajustados e prontos para serem inseridos na *Smart Grid*.

A Entrada de Dados e Ajustes, o Processador de Dados, a Análise de Riscos, o Integrador, a Análise de Dados, a Retroalimentação de Risco (*feedback*) e os Resultados ajustados, são processos inerentes ao fluxo lógico do STRAYER, incluídos em seu servidores no formato de linhas de comando do Sistema Operacional Linux (CentOS e Ubuntu) e serão explicados em detalhes a seguir.

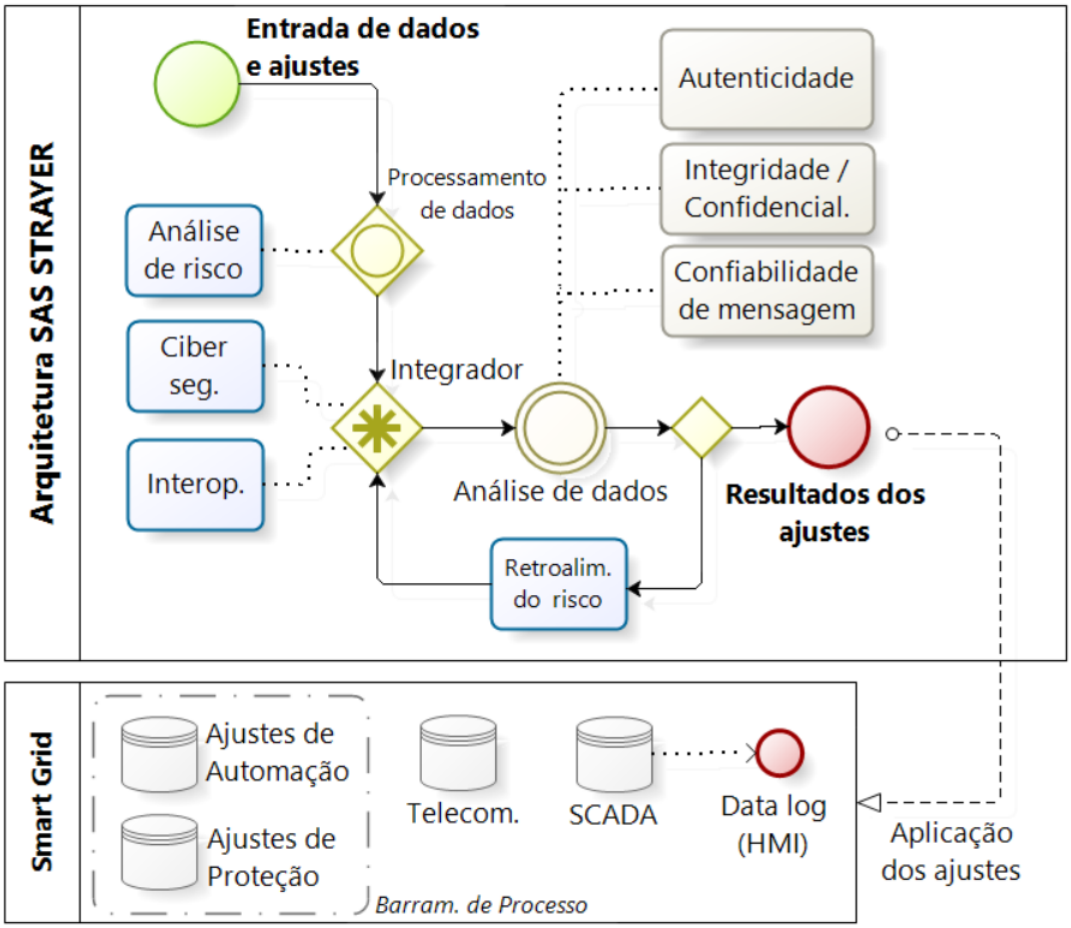


Figura 4.2: Fluxo lógico do STRAYER.

- **Entrada de Dados e Ajustes**. Trata-se da entrada dos dados e configurações originais de automação, proteção e comunicação para os IED's. É comum em uma situação de comissionamento que esses ajustes sejam inseridos em seu estudo original de projeto de subestações nos IED's, sem o devido tratamento de segurança, interoperabilidade ou gerenciamento de riscos. Os pacotes dos arquivos de ajustes podem estar corrompidos, danificados e as configurações erradas. Eles são a matéria-prima do STRAYER.

- **Processador de dados e Análise de Risco**. É o processo preliminar do STRAYER. Consiste na primeira inspeção dos dados de configuração, com simples verificação e detecção de variações na comunicação da rede. Ele desempenha o papel de um Sistema de Detecção/Prevenção de Intrusão (IDS/IPS). Da mesma forma que os dispositivos IDS e IPS, eles protegem os servidores do STRAYER. A assinatura padrão do ICMP Snort é usada no processo (comando "*icmp alert*"). O tempo necessário para a detecção é o mesmo que o TTL (*Time to Live*) das mensagens ICMP tipo 8 (TTL = 64).

- **Integrador**. Sua função é receber as configurações pré-analisadas de automação, proteção e comunicação e realizar duas funções simultaneamente: Análise de Vulnerabilidade (VA) e verificação da presença do soquete 61850 no protocolo do fabricante. Neste último, é possível realizá-lo através do arquivo de Descrição de Capacidade do IED (ICD) e do arquivo de Descrição de Configuração de

Subestação (SCD), presentes nos ajustes inspecionados. Pode-se perceber então que o Integrador é capaz de combinar uma função de segurança com análise de protocolo para interoperabilidade. Para este processo, STRAYER usou o renomado programa NESSUS CLIENT para o sistema operacional Kali Linux x86 no modo de linha de comando (CLI).

- **Análise de Dados**. O processo de análise de dados é um complemento ao Integrador, no que diz respeito ao parâmetro de segurança cibernética. Enquanto o integrador cuida da análise de vulnerabilidades, a Análise de Dados trata de outras funções de segurança da rede, a saber: i) *Autenticidade* - evitando ataques de força bruta, utilizando proatividade (modificação dinâmica de senha); ii) *Confidencialidade e Integridade de Dados* - análise de modificações de pacotes, e; iii) Confiabilidade - mantendo o administrador do STRAYER (*root*) sempre íntegro. A Análise de Dados usa outro servidor executando o Kali Linux OS com recursos NMAP.

- **Retroalimentação de Risco**. Este processo desempenha, praticamente, o mesmo papel do Processador de Dados que utiliza o Analisador de Risco. Porém, com uma diferença: ao invés de deixar passar o primeiro ajuste inspecionado, ele nega a passagem de dados caso não cumpra as regras de segurança da STRAYER. Em seguida, ele funciona com um *firewall* interno, com o mesmo intuito de lista de acesso (ACL) e esquema de políticas. Caso as configurações de automação, proteção ou comunicação ainda não estejam de acordo com as regras, elas serão devolvidas ao Integrador. Isso evita a passagem de ajustes inadequados para o *Smart Grid*. As regras utilizadas foram montadas com o sistema *iptables* do Linux. Além de algumas regras de permissão/negação para endereços IP, bits de *flag* TCP (*eg*, TCP SYN, TCP ACK) e datagramas que entram e saem da rede de TO, algumas políticas e configurações básicas foram implementadas, tais como: i) Prevenir o rastreamento de rotas na rede TO, descartando todo o tráfego ICMP de saída com TTL expirado, e; ii) Prevenir um ataque DoS *Smurf* na rede TO descartando todos os pacotes *ping* que estão indo para um endereço de *broadcast*. É nessa etapa que está o fator de dinamismo do STRAYER.

- **Resultado Ajustado e aplicação na *Smart Grid***. Estes são os dados finais de automação, proteção e comunicação devidamente ajustados em todas as etapas do fluxo lógico do STRAYER. Dados como: lógica de supervisão do IED, tempo máximo de disparo de corrente dos disjuntores (comumente chamado de "*trip*") e, verificação do tempo de retorno do SCADA, serão aplicados de forma adaptada na *Smart Grid*, diferente das configurações originais. A partir daqui, o SRAYER entrega os ajustes para o SAS adaptado.

O STRAYER foi projetado com mais de uma redundância de *switches*, ou seja, com mais de um concentrador (Principal e Secundário, conforme mostrado no Rótulo A da Figura 4.3), para manter uma arquitetura mais estruturada em termos de segurança. O número de *switches* de cada concentrador será determinado pelo número de portas de entrada/saída (I/O) dos IED's. Existem modelos de IED no mercado com um número variado de portas dependendo de cada fabricante. Porém, há unanimidade de presença modelos de IED com duas portas na maioria das Subestações elétricas. Portanto, para manter a situação de redundância nos IED's e a razoável relação custo-benefício para o STRAYER, a arquitetura foi estruturada para configuração de porta dual. Como resultado, cada IED será alimentado por dois concentradores, cada um em portas diferentes (Rótulo B, Figura 4.3).

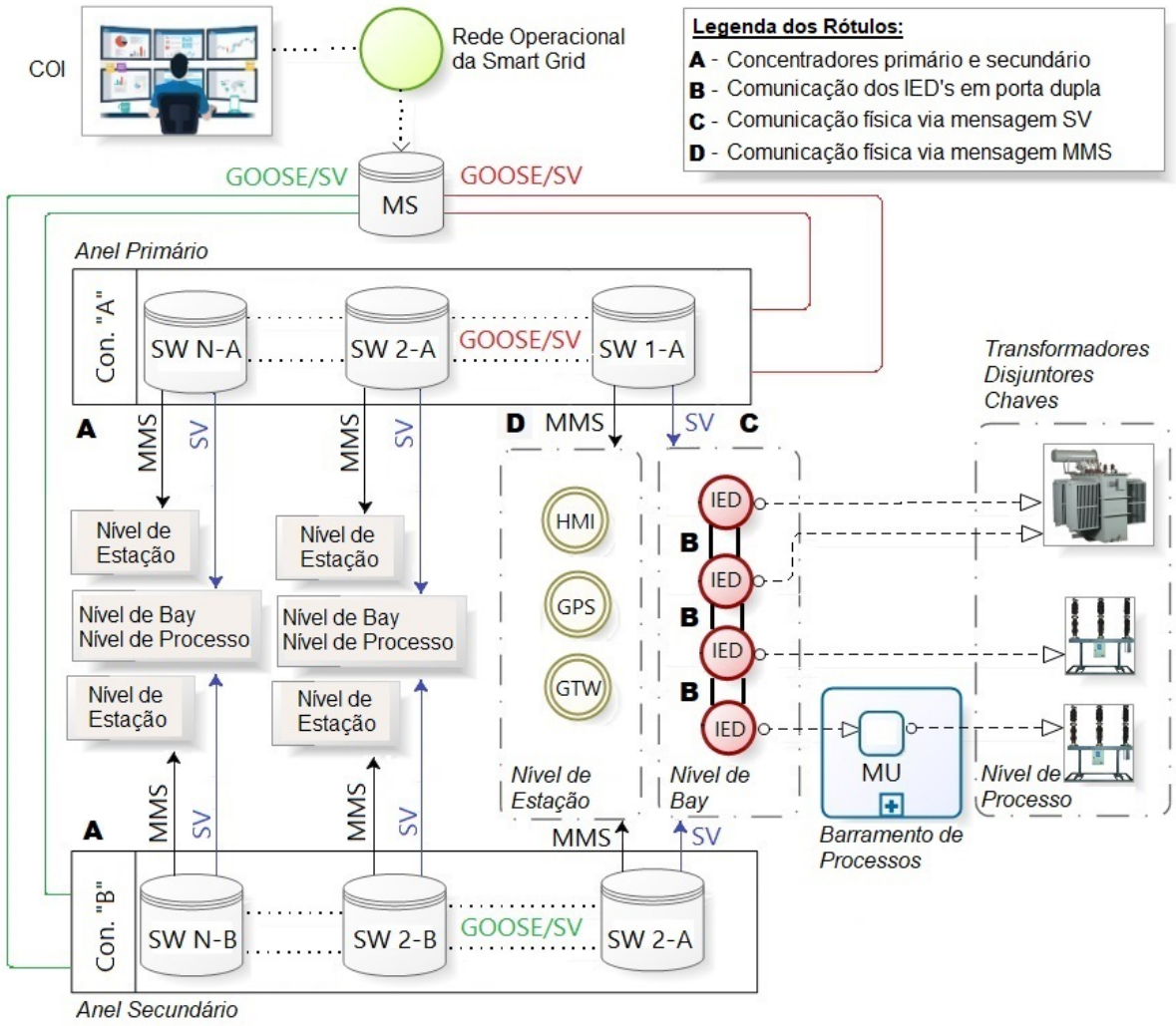


Figura 4.3: Arquitetura adaptada do SAS de *Smart Grid* para o STRAYER.

Nessa arquitetura, os concentradores são interligados por topologia em anel, via fibra óptica Gigabit Ethernet, e todos os IED's são interligados e gerenciados por protocolos de reconfiguração automática para garantir o fluxo de comunicação entre eles. Em consequência, os IED's e os equipamentos da *Smart Grid* poderão trocar informações entre si, independentemente do tipo de equipamento ao qual cada um esteja sujeito. Adicionalmente, por meio de dispositivos SAMU (ou simplesmente *Merging Units* - MU), as mensagens são digitalizadas no barramento de Processos para atender a norma IEC 61850. A MU ficará entre o IED e um possível equipamento analógico para digitalizar as informações de grandezas elétricas desses equipamentos de *Smart Grid*.

Para o requisito de comunicação adaptado ao STRAYER há o uso de mensagens SV [26, 39] na comunicação vertical e horizontal, conforme mostrado no Rótulo C da Figura 4.3, e mensagens GOOSE em comunicação estritamente horizontal, com VLANs restritas. Em comparação com a determinação de segurança dos protocolos de comunicação da norma IEC 62351-6, que visa imobilizar a forma de emissão de mensagens GOOSE e SV em procedimentos específicos (*eg*, deixando a comunicação em GOOSE tanto horizontal quanto verticalmente) [40], preferiu-se o uso mais aberto de mensagens de comunicação proposto pela IEC 61850-90-2. Dessa forma, é possível que o STRAYER tenha mais dinamismo na troca de

mensagens e não sature a comunicação com muitas mensagens GOOSE (mais pesadas que as mensagens SV) no barramento de Processos do SAS.

Outra importante implementação realizada pelo STRAYER foi a utilização de protocolos de comunicação MMS (*Manufacturing Message Specification*) como comunicação vertical entre IED's de interface de usuário, conforme apresentado no Rótulo D da Figura 4.3, diferente da arquitetura tradicional. No STRAYER, os protocolos MMS [41, 42] atendem aos critérios de interoperabilidade, pois funcionam facilmente no processamento de dados em tempo real entre dispositivos de outros fabricantes. O MMS cria um dispositivo virtual, comum em todos os equipamentos de interface (HMI - *Human Machine Interface*) ou troca de mensagens entre usuários, como o SCADA (*Supervisory Control and Data Acquisition*), mas mantendo o nível de segurança para acesso remoto, conforme solicitado na Norma IEC 61850-7-410 [43]. Quanto aos protocolos de sincronização de tempo, diferentemente da arquitetura tradicional, o STRAYER aproveita o próprio Barramento de Processos para implementar os protocolos, o que é permitido em algumas diretrizes.

A principal contribuição do STRAYER é seu fator de sucesso na redução de ataques a IED's e equipamentos de manobra, como os disjuntores, além de manter, pelo maior tempo possível, a integridade do SAS e das redes supervisórias. A contribuição secundária, é a comunicação entre equipamentos de diferentes fabricantes de forma dinâmica, segura e gerenciável. O dinamismo é necessário, pois sabe-se que é impossível praticar a aquisição de vários equipamentos por um único fabricante. Outra contribuição desta arquitetura é a capacidade de analisar situações de risco utilizando como método, teste de lógica e controle de proteção das *Smart Grids*. Isso facilita a gestão de parâmetros administrativos como KPI's da empresa (*Key Performance Indicators*), custos e melhor gestão de ativos.

Esses são os requisitos mínimos e as contribuições do STRAYER, ressaltando que cada *Smart Grid* se adaptará à sua arquitetura de acordo com a topologia da planta de fornecimento de energia elétrica, carga e visibilidade estratégica. Com a aplicação dos dados de arquitetura em novos projetos ou *retrofits* de *Smart Grids*, o resultado será a invulnerabilidade a agentes externos prejudiciais ao sistema elétrico de determinada região, dentro ou fora do administrador da concessionária de energia elétrica. No próximo capítulo, será apresentada a avaliação do STRAYER.

5 AVALIAÇÃO DO DESEMPENHO

Este capítulo apresenta a validação do STRAYER, em comparação com a arquitetura tradicional utilizada nas atuais *Smart Grids*. Para isso, o mesmo foi avaliado em três etapas: i) avaliação do desempenho de mitigação de ataques através da rede TO; ii) avaliação do desempenho de mitigação de ataques através da rede de TI da concessionária; e iii) avaliação do desempenho de mitigação de ataques através de acesso remoto. Com tais etapas, foi possível identificar os principais avanços que o STRAYER tem em relação à arquitetura tradicional, como apresentado a seguir.

5.1 CENÁRIOS

Para avaliar o STRAYER, foi construído um protótipo base de *Smart Grid* fornecedor de energia elétrica, adaptando-a ao STRAYER, conforme montagem de *hardware* apresentada na Figura 5.1. A configuração da arquitetura tradicional contemplou equipamentos do mesmo fabricante, enquanto que no STRAYER, optou-se por utilizar fabricantes diferentes, mantendo apenas a interligação em um sistema de segurança de infraestrutura distribuída e evitando uma solução *adHoc*, pois esta tende a facilitar a quebra de interoperabilidade. Embora os IED's estejam em conexão direta, estes são apenas ramificações dos nós principais (os *switches*). Para fazer uma comparação justa entre as arquiteturas, ambos utilizaram a mesma infraestrutura, composta por duas linhas de entrada, dois transformadores de potência e dois alimentadores de distribuição, contemplados por nove disjuntores de alta tensão, como mostrado na Figura 5.2. A descrição do equipamento utilizado no cenário para gerar os experimentos é apresentada na Tabela 5.1.

O fluxo lógico do protótipo alimenta os dados de ajuste do IED. Na prática, os servidores do STRAYER (*rack* de equipamentos à direita da Figura 5.1) estão localizados entre o COI e o primeiro acesso operacional à rede da *Smart Grid*, no caso o *Switch* Principal (ou de borda). Tudo que entra na *Smart Grid* deve avaliar rigorosamente os processos internos do Fluxo Lógico. Portanto, possíveis ataques serão redirecionados para o processo de Análise de Riscos. Outro ponto importante é que a arquitetura SAS adaptada da *Smart Grid* está mapeada para os servidores. Além disso, mesmo que o STRAYER faça sua análise completa, se uma determinada *Smart Grid* conter uma arquitetura diferente da filosofia de integração, haverá um conflito, e os ajustes não serão repassados. Esse é um ponto limitador para que os novos projetos sigam os critérios de Segurança Cibernética, Interoperabilidade e Gestão de Riscos.

Uma vez configurado os cenários, o objetivo é atacar os comandos elétricos e a lógica de automação dos IED's, remotamente ou localmente, acessando os privilégios das mensagens GOOSE ou SV e desabilitando o acesso remoto de autenticidade pelo COI. Para isso, foram utilizadas três técnicas de Teste de Penetração (*PENTEST*) para Sistemas de Controle Industrial (ICS): i) *SNIFFING*; ii) FORÇA BRUTA, e; iii) *ROOTKIT*. Os conceitos de ataques e os *softwares* abertos/proprietários utilizados nos testes são descritos a seguir.

- **i)** *SNIFFING*. De acordo com o banco de dados *ATT&CK for ICS* do MITRE, *Sniffing* (código MI-

Figura 5.1: Protótipo desenvolvido como prova de conceito para validar a arquitetura proposta.

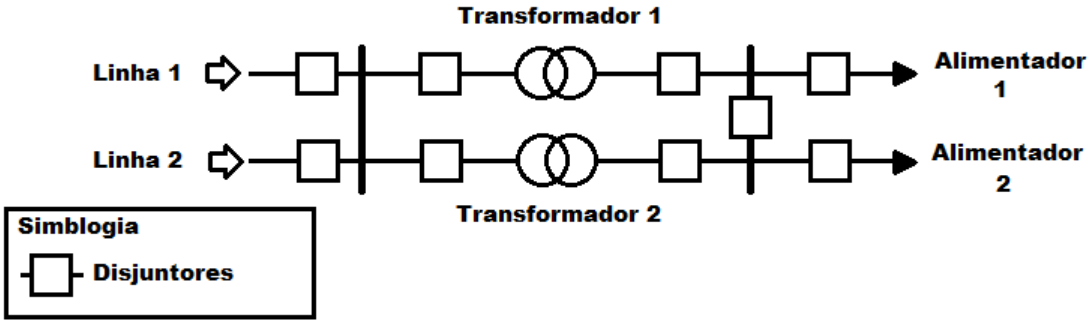


Figura 5.2: Diagrama unifilar de *Smart Grid* modelado para o protótipo.

TRE T1040) é um ataque que monitora ou captura informações de uma determinada rede, justamente por um ativo nessa mesma rede, independente do fluxo de pacotes. Essa prática geralmente explora informações essenciais para um ataque futuro mais elaborado, chamado de *exploit*. O envenenamento de protocolos ARP ou DNS pode ser usado para capturar credenciais para sites, *proxies* e sistemas internos redirecionando o tráfego para um invasor [44]. Para o teste, um *software* amplamente utilizado pelos administradores de rede *NIX foi utilizado: o "TCPDump". Para capturar a rede, foi necessário adicionar mais 18 bytes de endereçamento aos 1500 bytes máximos da rede Ethernet, ficando assim com um total de 1518 bytes. Uma vez que o *log* de atividades da rede é registrado, é possível analisá-lo com um simples comando "-*r*" do TCPDump.

- **ii)** FORÇA BRUTA. Considerado na categoria de técnica de sub-ataque pelo *ATT&CK for ICS* do MITRE, a Força Bruta, código T1110, consiste em obter acesso a redes quando as senhas são desconhecidas ou quando são obtidos seus *hashes*. Isso também pode ser feito sistematicamente

Tabela 5.1: Quantidade de dispositivos SAS e equipamentos de *Smart Grid* por cenário.

Dispositivo	Tradicional	STRAYER	Equipamento	Tradicional	STRAYER
IED	3	8	Transformadores	2	2
Switches Principais	1	2	Disjuntores	9	9
Concentradores	1	3	Linhas	2	2
Merging Units	1	7	Alimentadores	2	2
HMI	1	1	TC	8	8
GPS	1	2	TP	4	4
Gateways	None	2	Seccionalizadoras	10	10

Tabela 5.2: Etapas de acesso aos cenários.

ETAPA	DESCRIÇÃO
Acesso direto pela rede TO	Acesso ao Centro de Operações Integradas (COI) da empresa Uma vez dentro, pode-se acessar a rede TO além da rede de TI. O COI detém permissão de comando remoto para os IED's (manobras por comando remoto dos disjuntores, por exemplo).
Acesso indireto pela rede TI	Acesso ao edifício ou sede da concessionária. É possível acessar a rede corporativa (TI) da empresa. Este ataque é facilitado por invasores internos.
Acesso remoto	É o acesso não físico a qualquer estrutura elétrica, *Smart Grid* ou edificação da empresa. Neste caso, o ataque é mais difícil, mas não impossível. Driblar o firewall é essencial.

pelo invasor usando mecanismos de repetição ou iteração dos serviços de validação de credenciais. O acesso por Força Bruta aproveita o conhecimento adquirido de outros comportamentos pós-comprometimento, como despejo de credenciais do sistema operacional, descoberta de conta ou descoberta de política de senhas ou combinações desses ataques [45]. Para o *PENTEST*, os cenários foram enfatizados com o amplamente conhecido "*John The Ripper*" para Linux OS, que usa a linguagem C para varrer as *wordlists*.

- **iii)** *ROOTKIT*. O *Rootkit* é um conjunto de ações que visa limpar os rastros de um ataque principal. De acordo com o *ATT&CK for ICS* do MITRE (pelo código T1014), ele serve para ocultar a presença de programas, arquivos, conexões de rede, serviços, *drivers* e outros componentes, maliciosos ou não, do sistema [46]. Ele intercepta e modifica as interfaces do sistema operacional. A intenção final do *Rootkit* é o controle quase total do sistema, capturando o papel do administrador (a credencial de *root*). Isso pode resultar na desconsideração de comandos e na alimentação de informações falsas para o dispositivo mestre. Nos testes, esse ataque foi projetado para rodar após tentativas de *SNIFFING* e FORÇA BRUTA com um advento já existente no Linux, chamado *SetUID*. Esta função nada mais é do que a permissão que o *root* dá a outros usuários para acessar determinados arquivos. Se os ataques mencionados forem bem-sucedidos, o *Rootkit* fará com que o *host* trabalhe para que o sistema ative outros ataques, como implantações de *trojans*, outros *malwares* e ataques de *backdoor*. Este último consiste em abrir rotas alternativas de invasão uma vez dentro do sistema. No nosso caso, a intenção é apenas observar se a instalação do *backdoor* foi bem sucedida.

Após a definição dos tipos de ataques, eles foram aplicados em três etapas: i) acesso à rede de TO, ii) acesso à rede de TI e iii) acesso remoto, conforme já mencionado no Capítulo 4. Essas etapas são os caminhos para invasões em *Smart Grids*. A etapa de acesso à rede TO é a forma mais direta de invasão, pois é a rede onde o sistema SCADA está localizado. A rede de TI funciona como um segundo nível para acessar a rede TO. Finalmente, o acesso remoto é mais difícil, mas possui a maior quantidade de intrusões, historicamente. A disposição das etapas e suas descrições podem ser vistas na Tabela 5.2.

Como o objetivo é validar os problemas de ataques cibernéticos no STRAYER, foram selecionadas as seguintes métricas:

- **Taxa de IED's Afetados** - porcentagem de IED's invadidos com sucesso.

- **Taxa de disjuntores manobrados** – porcentagem de disjuntores abertos com sucesso.
- **Permanência de integridade do COI** – tempo dispendido para invadir o sistema SCADA;
- **Tempo real para acessar um IED** – tempo gasto para acessar cada IED, especificamente.

Depois de montados os cenários e as métricas de teste, foi possível obter resultados. Os mesmos são apresentados a seguir.

5.2 RESULTADOS OBTIDOS

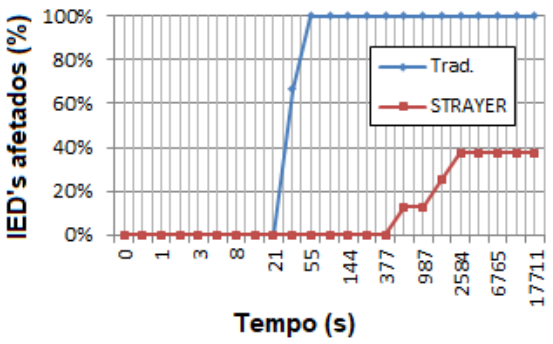
Nesta seção, os resultados obtidos são apresentados. São apresentados os dados das etapas de acesso à rede de TO, TI e por acesso Remoto. Os resultados para tais acessos foram comparados, quantificados, e finalmente, discutidos como apresentado a seguir.

5.2.1 Etapa de acesso pela rede de Tecnologia de Operação - TO

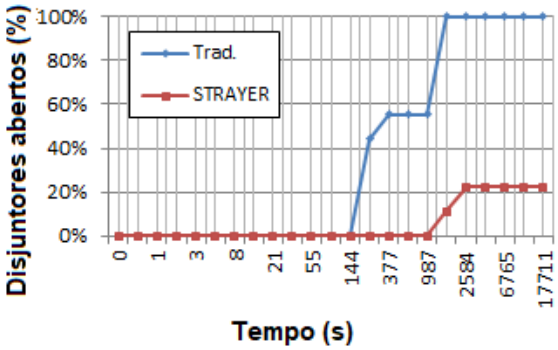
A Figura 5.3(a) apresenta o resultado obtido nos testes relacionados à métrica de Taxa de IED's Afetados através de uma rede direta de TO. É perceptível, nesta etapa, que o número de IED's infectados foi menor no STRAYER do que na arquitetura tradicional. 100 % dos dispositivos de arquitetura tradicional foram afetados em menos de 55 segundos do tempo decorrido. No entanto, apenas 37,5 % dos IED's do STRAYER foram comprometidos. Isso se deve ao gerenciamento de risco realizado contra o acesso promíscuo. O Fluxo Lógico percebeu várias solicitações em pouco tempo e interrompeu a aceitação de comandos. Com este advento automático, foi possível configurar esta função para todos os IED's sem gastar recursos adicionais.

A figura 5.3(b) apresenta uma consequência do sucesso de invasão pela primeira métrica, que é a abertura do disjuntor do IED afetado, acessado pela rede TO. O resultado mostrou que 100 % dos disjuntores na arquitetura tradicional foram operados, justamente porque esses equipamentos estão todos conectados a todos os IED's possíveis. O primeiro disjuntor agiu em menos de 233 segundos. No entanto, como o STRAYER restringe o acesso a todos os disjuntores da *Smart Grid*, apenas 22,2 % deles foram operados. Precisamente, dois disjuntores do mesmo transformador e o disjuntor do barramento interligado foram os equipamentos afetados. Assim, ao perceber o acesso indevido em um dos dois concentradores, o STRAYER bloqueou temporariamente o acesso aos comandos de proteção do disjuntor, retardando o acesso aos mesmos.

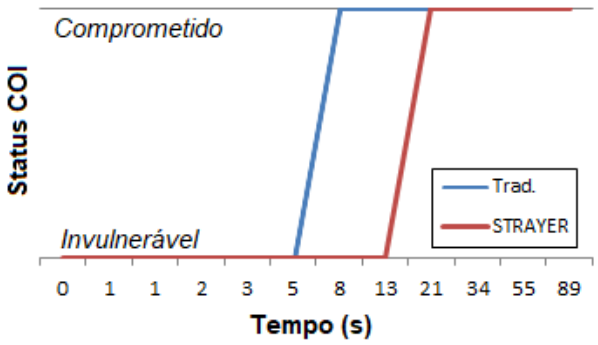
A Figura 5.3(c) apresenta o tempo decorrido para acessar o sistema SCADA da rede TO do COI. Naturalmente, esse sistema geralmente não possui controle de acesso adequado, pois várias pessoas podem fazê-lo (devido aos invasores internos). Como resultado, acessar o COI pela rede TO é praticamente "instantâneo". No entanto, o STRAYER conseguiu atrasar esse acesso em 13 segundos em comparação com a arquitetura tradicional. Portanto, é oportuno pensar que o acesso ao SCADA ainda é um desafio. No entanto, ficou evidente que o STRAYER poderia mitigar o acesso repentino e rápido ao sistema. Isso foi possível porque o STRAYER possui mais dispositivos de rede de diferentes fabricantes e redundâncias



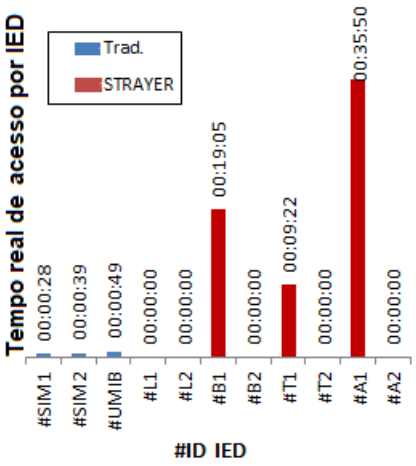
((a)) Taxa de IED's Afetados



((b)) Taxa de disjuntores manobrados



((c)) Permanência de integridade do COI



((d)) Tempo real para acessar um IED

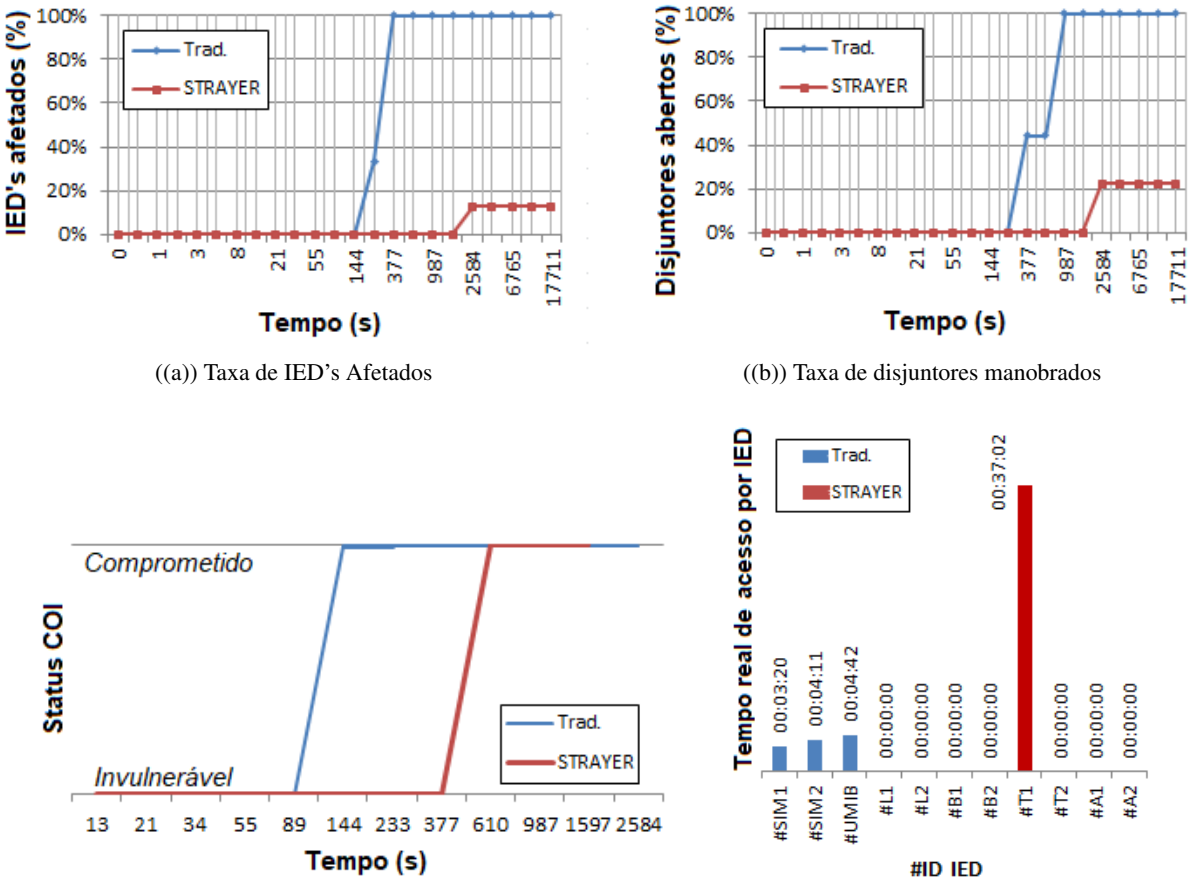
Figura 5.3: Impacto no desempenho do STRAYER quando comparado com a arquitetura tradicional - etapa de acesso da rede TO.

que atrasam o acesso à rede TO.

A Figura 5.3(d) apresenta o tempo gasto para acessar cada IED utilizando o acesso TO. Como esperado, a arquitetura tradicional perdeu seus três IED's em muito pouco tempo, sendo os tempos de *00min28seg* para o primeiro, *00min39seg* para o segundo e *00min49seg* para o último. STRAYER perdeu apenas 3/8 deles em *35min50seg*. Os outros cinco IED's do STRAYER tiveram seus comandos bloqueados pelo fluxo lógico. Não há dúvida de que a quantidade de redundâncias de segurança do STRAYER ajuda no atraso da invasão do IED. Ressalta-se também que os três IED's da arquitetura tradicional causaram um apagão total na *Smart Grid*, enquanto que no STRAYER, apenas um *bay* de transformador e um barramento no lado da tensão abaixada caíram. No entanto, devido à redundância do outro transformador, a *Smart Grid* continuou funcionando. Com o tempo tão alto, seria possível para um administrador de rede bloquear o ataque em tempo hábil.

5.2.2 Etapa de acesso pela rede de Tecnologia da Informação - TI

A Figura 5.4(a) apresenta o resultado referente à Taxa de IED's Afetados, agora utilizando a rede de TI da empresa concessionária de energia. Mesmo assim, a vantagem do STRAYER sobre a arquitetura



((a)) Taxa de IED's Afetados

((b)) Taxa de disjuntores manobrados

((c)) Permanência de integridade do COI

((d)) Tempo real para acessar um IED

Figura 5.4: Impacto no desempenho do STRAYER quando comparado com a arquitetura tradicional - etapa de acesso da rede TI.

tradicional pode ser percebida novamente. Nessa etapa, permaneceu a perda de 100 % dos IED's pela arquitetura tradicional, com a diferença de que houve um pequeno atraso para isso, em comparação com o acesso TO. STRAYER conseguiu minimizar a perda de IED's sobre acesso por TO. Apenas 12,5 % dos IED's foram afetados no tempo decorrido de 2584 segundos. Além das contramedidas adotadas no momento da invasão por TO, no acesso à rede de TI, a lógica de fluxo exigiu a necessidade de autenticação em duas etapas. Isso foi possível com uma autenticação secundária por meio do *firewall* da rede de TI.

A figura 5.4(b) apresenta a abertura dos disjuntores afiliados usando a rede de TI. Nesta etapa, a arquitetura tradicional apenas atrasou, em 610 segundos, o tempo necessário para perder 100 % dos seus disjuntores. Enquanto que STRAYER manteve a integridade de 71,5 % dos disjuntores, perdendo apenas dois deles, simultaneamente. No entanto, houve uma situação especial: o segundo disjuntor só foi aberto pelo sistema de proteção diferencial de um dos transformadores da *Smart Grid*, e não por invasão. Neste caso, quando a proteção percebe que um de seus disjuntores abriu incorretamente (chamado de Falha de Abertura de Disjuntor), ou quando há diferença de corrente entre os dois lados do transformador, os dois disjuntores deste equipamento irão abrir. Então, na verdade, o STRAYER perdeu apenas um disjuntor devido a um ataque cibernético e outro devido à proteção de uma abertura indevida, apenas no tempo decorrido de em 2584 segundos. Assim, o STRAYER provou prevenir um possível ataque em um tempo

maior do que na arquitetura tradicional, mesmo acessando o estágio de rede de TI.

A Figura 5.4(c) apresenta o tempo necessário para invadir o COI em ambos os cenários pela rede de TI. STRAYER conseguiu atrasar o tempo de acesso SCADA em 466 segundos em comparação com a arquitetura tradicional. Os equipamentos de segurança de rede de TI ajudaram em ambos os casos. No entanto, no STRAYER, a autenticação em duas etapas exigida pelo fluxo lógico conseguiu manter o sistema supervisório íntegro por 610 segundos.

A Figura 5.4(d) apresenta o tempo necessário para invadir cada IED através da rede de TI. Ficou bastante evidente que o STRAYER evoluiu seu desempenho nesta fase em relação à arquitetura tradicional. Além de manter uma quantidade menor de IED's invadidos, atrasou significativamente o tempo de invasão em relação ao acesso por TO. A arquitetura tradicional perdeu todos os seus IED's em *03min20seg*, *05min11seg* e *04min42seg*, enquanto o tempo decorrido do único IED perdido pelo STRAYER foi *37min02seg*, e neste caso, é possível eliminar o foco de invasão com a adoção de contramedidas devido ao longo tempo. Através da rede de TI, STRAYER conseguiu atrasar em *32min20seg* o maior tempo de invasão em relação ao cenário de arquitetura tradicional. Mais uma vez, o bloqueio do acesso aos IED's da STRAYER foi parte fundamental deste resultado.

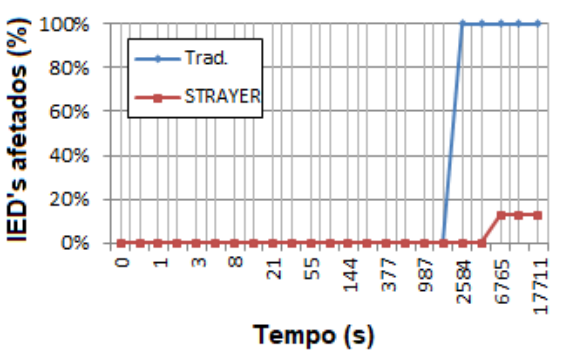
5.2.3 Etapa de acesso remoto

A Figura 5.5(a) apresenta o desempenho dos dois cenários quando analisados de acordo com a métrica Taxa de IED's Afetados, agora por acesso remoto. A arquitetura tradicional manteve sua perda de 100 % de IED's no tempo decorrido de 2584 segundos, enquanto que o STRAYER manteve a integridade de 87,5 % de seus oito IED's. Mais uma vez, STRAYER superou a arquitetura tradicional. A parte de retroalimentação do fluxo lógico STRAYER detectou acesso impróprio ao *switch* principal do SAS, impedindo a tentativa de acesso adicional.

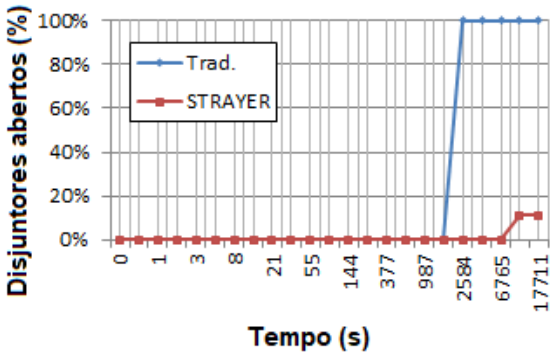
A Figura 5.5(b) apresenta o número de disjuntores afetados via acesso remoto em um determinado tempo. Enquanto 100 % dos disjuntores foram comprometidos na arquitetura tradicional, apenas 11,1 % deles foram abertos no STRAYER. Percebe-se que, mesmo com a invasão de dois IED's, referente à métrica anterior, o STRAYER impediu a abertura de um segundo disjuntor, mantendo a *Smart Grid* em pleno funcionamento. No entanto, houve um apagão total pela arquitetura tradicional.

A Figura 5.5(c) apresenta o tempo de acesso ao Centro de Operações e seu sistema SCADA, remotamente. Pode-se observar que o cenário STRAYER atrasou o tempo de invasão ao COI em 987 segundos em comparação com o cenário tradicional. Também é possível analisar a partir da mesma figura que o tempo de acesso foi maior do que as etapas de acesso às redes de TI e TO.

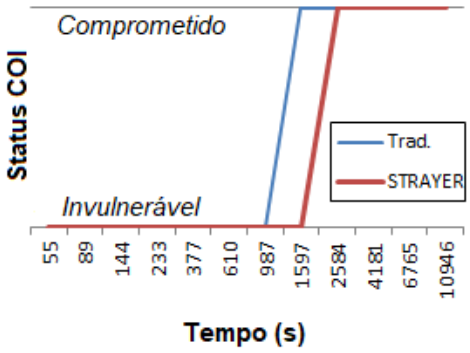
A Figura 5.5(d) apresenta a lista com todos os IED's de cada cenário, com seus respectivos tempos de invasão, por acesso remoto. A arquitetura tradicional não conseguiu mitigar o ataque aos seus IED's e perdeu o acesso a todos os dispositivos em um tempo máximo de *31min52seg* para acesso remoto. A primeira métrica mostrou que STRAYER perdeu apenas um único IED, e mesmo assim, só ocorrendo no tempo transcorrido de *1h43min15seg*, conforme figura 5.5(d) da métrica atual. Com esse tempo, é possível facilmente que um administrador do Centro de Operações de Segurança (SOC) execute o bloqueio do ataque ao COI. A atuação do STRAYER quanto ao atraso de invasão foi evidenciada nesta métrica,



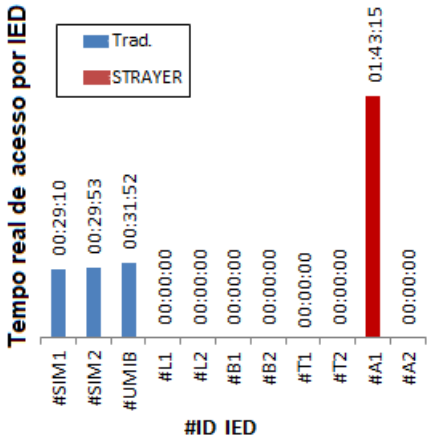
((a)) Taxa de IED's Afetados



((b)) Taxa de disjuntores manobrados



((c)) Permanência de integridade do COI



((d)) Tempo real para acessar um IED

Figura 5.5: Impacto no desempenho do STRAYER quando comparado com a arquitetura tradicional - etapa de acesso remoto.

pois neste caso, atrasou o acesso em mais de uma hora. Esse tempo já é suficiente para a equipe de cibersegurança da empresa já ter tomado medidas preventivas em tempo real para eliminar a invasão.

5.3 DISCUSSÃO

Nesta seção serão discutidos os resultados apresentados anteriormente, fazendo uma comparação geral entre as três etapas de acesso, observando os dados obtidos pelas métricas.

Inicialmente, olhando para os resultados globais, percebe-se que a etapa de Acesso Remoto teve melhor desempenho que as demais. Essa situação é plausível, pois o caminho de acesso remoto é mais longo do que para redes de TO e de TI, que são de acesso mais direto. Isso é muito promissor, pois o histórico de intrusões em *Smart Grids* tende a ser por canais de acesso remoto [13, 14, 15], usando protocolos como o Telnet, FTP e outros serviços TCP. Além disso, notou-se que houve um bloqueio de acesso aos IED's mais rapidamente para a tentativa de acesso à rede TO do que nas demais etapas. Como a invasão é mais rápida nesta rede, consequentemente, o bloqueio também é mais rápido. Por fim, foram apresentadas comparações entre as três etapas de acesso.

6 CONCLUSÃO

Apesar dos recentes avanços das *Smart Grids* e suas recomendações de segurança cibernética, ainda há ataques aos sistemas de automação e proteção nessas estruturas de forma continuada. Como resultado, este trabalho apresentou o problema sistêmico e real das vulnerabilidades de segurança dos padrões tradicionais de arquitetura de automação e propôs a arquitetura STRAYER para reduzir essa ameaça. A arquitetura proposta integra segurança cibernética para monitoramento e blindagem de acesso, interoperabilidade para manter a comunicação entre equipamentos/dispositivos e gerenciamento de risco para manter a confiabilidade e prevenir ataques cibernéticos em tempo real nas *Smart Grids*. Com isso, STRAYER analisou possíveis ataques cibernéticos utilizando lógica de fatores de integração dentro dos dispositivos de rede de uma *Smart Grid*.

Como prova de conceito, um protótipo foi construído para validar o STRAYER, projetado para operar em um SAS. Os resultados mostraram que o STRAYER tem um excelente desempenho no controle de acesso devido à lógica de automação e proteção de um sistema de fornecimento de energia elétrica. Além das reduções na quantidade de IED's afetados por invasões, também foi possível perceber que o STRAYER evitou o colapso de uma *Smart Grid*, tendo apenas perdas mínimas e reversíveis, diferentemente da arquitetura tradicional.

Destacaram-se as seguintes contribuições:

- uma nova arquitetura SAS de *Smart Grid* baseada em adaptações lógicas para tentar evitar ataques cibernéticos.
- a melhoria da eficiência de segurança em relação às arquiteturas de trabalhos relacionados.
- um relato de experiência do emprego da arquitetura em um contexto real.

Recentemente, as contribuições do STRAYER foram validadas e publicadas em veículos acadêmicos de ampla notoriedade. Além do já citado trabalho apresentado em 2020 [3], em 2022, o resultado da pesquisa foi publicação no *Journal of Information Security and Applications*, revista internacionalmente renomada que discursa sobre as atualidades no ramo de segurança da informação.

Como pesquisa futura, pretende-se empregar e avaliar uma arquitetura de aprendizado federado no STRAYER para mitigar problemas de ataques em *Smart Grids*. Adicionalmente, será trabalhada a redução do tempo de invasão ao COI. Com o aprendizado federado, é possível proteger a confidencialidade dos dados, permitindo que os dispositivos construam de forma colaborativa um modelo de defesa eficiente contra ataques, priorizando o monitoramento de dados. Por fim, apoia-se a hipótese de que tal arquitetura pode reduzir o tempo de ataque em uma *Smart Grid*, prolongando sua vida útil.

REFERÊNCIAS BIBLIOGRÁFICAS

1 ABRADEE. *A indústria da eletricidade - VISÃO GERAL DO SETOR*. Associação Brasileira de Distribuidoras de Energia Elétrica, 2022. Disponível em: <https://www.abradee.org.br/setor-eletrico/visao-geral-do-setor/>.

2 GUNDUZ, M.; DAS, R. Cyber-security on smart grid: Threats and potential solutions. *Computer networks*, v. 169, p. 107094, 2020.

3 PAULA, A.; DIAS, R.; SILVA, M.; RIBEIRO, M.; NAKATA, B.; KNORST, N.; SOUZA, J.; MENEGUETTE, R.; GONçALVES, V.; FILHO, G. Integrated automation platform for complete simulation of digital substations with a focus on interoperability and cybersecurity. *In: Annals of the VIII Workshop on Applied Computing in Electronic Government, SBC*, p. 140–147., 2020.

4 IEC. 61850-4 - communication networks and systems for power utility automation - part 4: System and project management. *International Electrotechnical Commission*, v. 61850-4, p. 68, 2013.

5 GOODRICH, M. T.; TAMASSIA, R. *Introdução à Segurança de Computadores*. [S.l.]: Bookman, 2013.

6 ISO. 31000 - risk management – guidelines - second edition. *International Organization for Standardization*, v. 31000, p. 1–23, 2018.

7 NIST. Framework for improving critical infrastructure cybersecurity - version 1.1. *National Institute of Standards and Technology*, v. 1.1, p. 1–55, 2018.

8 IEC. 61850 - communication networks and systems in substations - first edition. *International Electrotechnical Commission*, v. 61850, p. –, 2007.

9 VICENTE, D. Application of iec 61850 standards in electrical power transmission/distribution shared substations. *Thesis from Sao Paulo University*, -, p. 1–117, 2011.

10 GREER, C.; AL et. Nist sp 1108r3 - nist framework and roadmap for smart grid interoperability standards, release 3.0. *National Institute of Standards and Technology*, v. 1108r3, p. 1–246, 2014.

11 CINTUGLU, M.; MOHAMMED, O.; AKKAYA, K.; ULUAGAC, A. A survey on smart grid cyber-physical system testbeds. *IEEE Communications Surveys & Tutorials*, v. 19 n1, p. 446–464, 2016.

12 MUBARAK, S.; HABAEBI, H.; ISLAM, R.; BALLA, A.; TAHIR, M.; ELSHEIKH, A.; SULIMAN, M. Industrial datasets with ics testbed and attack detection using machine learning techniques. *Intelligent Automation & Soft Computing*, -, p. 1–16, 2021.

13 ZHEGULEV, I. *Report: Hackers behind Ukraine power cuts, says US report*. BBC News, 2016. Disponível em: <https://www.bbc.com/news/technology-35667989>.

14 ZHEGULEV, I. *Report: Ukraine asks FBI to help probe suspected Russian hack of Burisma*. Reuters, 2020. Disponível em: <https://www.reuters.com/article/idUSKBN1ZF1KL>.

15 COSTA, L. *Report: Energisa busca restabelecer sistemas após ser alvo de ciberataque*. Reuters Brazil, 2020. Disponível em: <https://br.financas.yahoo.com/noticias>.

16 LÁZARO, J.; ASTARLOA, A.; RODRÍGUEZ, M.; BIDARTE, U.; JIMÉNEZ, J. A survey on vulnerabilities and countermeasures in the communications of the smart grid. *MDPI Electronics*, v. 10, p. 1881, 2021.

17 FAQUIR, D.; CHOULIARAS, N.; SOFIA, V.; OLGA, K.; MAGLARAS, L. Cybersecurity in smart grids, challenges and solutions. *AIMS Electronics and Electrical Engineering*, v. 5, p. 24–37, 2021.

18 YANG, W.; HENG-XUAN, L.; SHI-PING, E.; KAN-JUN, Z. Research on classification of substation background information for monitoring. *In: International Conference on Building Energy Conservation, Thermal Safety and Environmental Pollution Control - ICBTE 2019*, v. 136, p. 01023, 2019.

19 H.VARDHAN; RAMLACHAN, R.; SZELA, W.; GDOWIK, E. Deploying digital substations: Experience with a digital substation pilot in north america. *In: 71st Annual Conference for Protective Relay Engineers (CPRE). IEEE*, -, p. 1–9, 2018.

20 IEC. 61850-1 - communication networks and systems in substations - part 1: Introduction and overview. *International Electrotechnical Commission*, v. 61850-1, p. 44, 2003.

21 FONTES, M. Compliant didactic platform design for commissioning a iec 61850 digital power substation control and protection system. *Dissertação de Mestrado pela Universidade Federal do Rio Grande do Norte*, v. 129f, p. 1–150, 2015.

22 IEC. 61850-7-1 - basic communication structure for substation and feeder equipment – principles and models. *International Electrotechnical Commission*, v. 61850-7-1, p. 284, 2003.

23 IEC. 61850-3 - communication networks and systems for power utility automation - part 3: General requirements. *International Electrotechnical Commission*, v. 61850-3, p. 436, 2013.

24 IEC. 61850-6 - communication networks and systems for power utility automation – part 6: Configuration description language for communication in electrical substations related to ieds. *International Electrotechnical Commission*, v. 61850-6, p. 436, 2009.

25 RAVELLI, C. Análise de interoperabilidade de dados para a impementação de um ambiente de manufatura virtual. *Dissertação de mestrado pela Escola de Engenharia de São Carlos - Universidade de São Paulo (USP)*, p. 65–66, 2003.

26 IEC. 61850-90-1 - communication networks and systems for power utility automation - part 90-1: Use of iec 61850 for the communication between substations. *International Electrotechnical Commission*, v. 61850-90-1, p. 1–79, 2020.

27 TANENBAUM, A. S. *Redes de computadoras*. [S.l.]: Pearson educacition, 2015.

28 KUROSE, J. F.; ROSS, K. W. Redes de computadores e a internet - uma abordagem top-down. *São Paulo: Person*, v. 28, 2014.

29 IEC. 27002 - information technology — security techniques — code of practice for information security controls. *International Electrotechnical Commission*, v. 27002, p. 111, 2013.

30 ONS. Módulo 5 - submódulo 5.13 - controles mínimos de segurança cibernética para o ambiente regulado cibernético. *Manual de Procedimentos da Operação - Operador Nacional do Sistema*, v. 4.1.11, p. 8, 2021.

31 ISA. 95.00.01 - enterprise-control system integration part 1: Models and terminology. *The International Society of Automation*, v. 95.00.01, 2010.

32 IEC. 61850-9-2 - communication networks and systems for power utility automation - part 9-2: Specific communication service mapping (scsm) - sampled values over iso/iec 8802-3. *International Electrotechnical Commission*, v. 61850-9-2, p. 1–65, 2011.

33 HEINISCH, A.; LEITE, L.; SPYER, B.; RABELLO, M. Segurança cibernética para processos operativos em sistemas de energia elétrica. *Published in the Technology and Innovation Management Center - CGTI*, Library of Articles/Reports, p. –, 2012.

34 LELLYS, D.; PAULINO, M.; ALVES d. C.; SCHIMITT, M. Process bus (merging unit): Concept, architecture and impact on substation automation. *Technology and Innovation Management Center - CGTI*, Library of Articles/Reports, p. 1–7, 2016.

35 KIMURA, S.; ROTTA, A.; ABBOUD, R.; MORAES, R.; ZANIRATO, E.; BAHIA, J. Applying iec 61850 to real life: Modernization project for 30 electrical substations. *In: 1st Annual Protection, Automation and Control World Conference*, -, p. 1–18, 2010.

36 LI-QING, G.; JIAN-FENG, W.; JING-YU, T.; MING, Y. Research and application of one-key sequence control technology for substations. *In: International Conference on Building Energy Conservation, Thermal Safety and Environmental Pollution Control - ICBTE 2019*, v. 136, p. 01022, 2019.

37 PANDEY, R.; MISRA, M. Cyber security threats-smart grid infrastructure. *In: 2016 National power systems conference (NPSC)*, -, p. 1–6, 2016.

38 IEC. 61850-8-1 - communication networks and systems in substations - part 8-1: Specific communication service mapping (scsm) - mappings to mms (iso 9506-1 and iso 9506-2) and to iso/iec 8802-3. *International Electrotechnical Commission*, v. 61850-8-1, p. 1–140, 2004.

39 IEC. 61850-90-2 - communication networks and systems for power utility automation - part 90-2: Using iec 61850 for communication between substations and control centres. *International Electrotechnical Commission*, v. 61850-90-2, p. 1–188, 2020.

40 IEC. Iec 62351-6 - power systems management and associated information exchange - data and communications security - part 6: Security for iec 61850. *International Electrotechnical Commission*, v. 62351-6, p. 1–67, 2020.

41 IEC. 9506 - industrial automation systems — manufacturing message specification. *International Electrotechnical Commission*, v. 9506, p. 1–316, 2003.

42 IEC. Iec 62351-4 - power systems management and associated information exchange - data and communications security - part 4: Profiles including mms and derivatives. *International Electrotechnical Commission*, v. 62351-4, p. 1–494, 2018.

43 IEC. 61850-7-410 - basic communication structure - hydroelectric power plants - communication for monitoring and control. *International Electrotechnical Commission*, v. 61850-7-410, p. 1–284, 2015.

44 MITRE. *Network Sniffing*. ATT&CK for ICS, 2022. Disponível em: <ttps://attack.mitre.org/techniques/T1040/>.

45 MITRE. *Brute Force I/O*. ATT&CK for ICS, 2022. Disponível em: <https://attack.mitre.org/techniques/T1110/>.

46 MITRE. *Rootkit*. ATT&CK for ICS, 2022. Disponível em: <https://attack.mitre.org/techniques/T1014/>.

ANEXO I: ESPECIFICAÇÃO TÉCNICA DOS CENÁRIOS

EQUIPAMENTO	FABRICANTE/MODELO	ESPECIFICAÇÃO ORIGINAL
IED'S -Tradiconal: "#SIM1", "#SIM2 e "#UMIB" IED'S - STRAYER: "#A1"	SEL 751 Feeder Protection Relay	Feeder Protection. Sensitive. Neutral Input with 200mA. Arc-Flash Mitigation. Automation and Control. IEEE C37.118. Bay Screen, Authentication Breaker control, phasors andEnergy metering.
IED'S -STRAYER: "#A2"	GE MULTILIN 750 Feeder Protection System	Easy-to-use protection supported by industry-leading software. Accurate and built-in measurement functions. I/O monitoring - improve uptime. IRIG-B time sync, event reporting, waveform capture, data logging.
IED'S -STRAYER: "#T1"	GE MULTILIN 745 Transformer Protection System	Easy-to-use Transformer Protection, supported by the market-leading software toolset. Greater safety for transformer energization. Accurate and built-in measurement functions. Advanced FlexLogic automation features
IED'S -STRAYER: "#T2"	SEL 787 Transformer Protection Relay	Two-Winding Complete Protection. Cost-Saving Transformer Monitoring. Reliable Protection in Harsh Environments. Additional protection and communications options.
IED'S -STRAYER: "#B1" e "#B2"	SIEMENS SIPROTEC 7SJ81	Overcurrent protection with Standardvariant Housing type: Flush mounting; BI: 11; BO: 9 (9ST + 0F + 0HS + 0P). Communications encryption: Normal; Integrated Ethernet port J: for DIGSI 5.
IED'S -STRAYER: "#L1" e "#L2"	SEL 421 Protection, Automation, and Control System	Subcycle Distance Protection. Series-Compensated Transmission Lines. Single- or Three-Pole Operation. Sampled Values (SV) technology using IEC 61850-9-2. Bay Control, Reclosing, and Breaker Failure Protection.
MERGING UNITS (SAMU)	GE REASON MU320E	Process Interface Unit for full bay digitalization. Stand alone Merging Unit for conventional instrument transformers. Remote I/O (RIO) device for interfacing to primary equipment such as circuit breakers and disconnectors. Bay unit for GE B30X distributed bus bar protection system.
GPS	SEL 2488 Satellite-Synchronized Network Clock	Time Distribution. Cable Delay Compensation. Ower utility automation (IEC/IEEE 61850-9-3:2016) profiles. GNSS Vulnerability Mitigation. Authentication/Reliability.
SIMULADOR DE CORRENTE	OMICRON CMC 356 Universal relay test set and commissioning tool	Powerful current sources for testing even high-burden lectromechanical relays. High current amplitudes for 5 A relay testing. High accuracy and versatility for testing static and numerical relays of all types. Integrated network for testing IEC 61850 IEDs. 10-channel analog measurement and transient recording functionality (option).
CONCENTRADORES	SEL 3530 Real-Time Automation Controller (RTAC)	IEC 61131 and IEC 61131 logic engine. Network Security Device. IEC 61850 Integration (GOOSE). IEEE 1613 and protective relay specifications. SCADA Remote Terminal Unit (RTU). Substation Human-Machine Interface (HMI).
SWITCH PRINCIPAL	SEL 2730M Managed 24 Port Ethernet Switch	Ethernet connectivity for SCADA. Maximized Ethernet Network Robustness. IEC 61850-3 standards for communications devices in electric power substations. Secure Network Management (SNMPv3). Network Topology Configuration. Easy Network Commissioning
RELÉS BIESTÁVEIS (SIMULADORES DE DISJUNTOR)	FINDER RB 14.9.125.0000 8A	Command and signaling relay. DC direct current. SET and RESET command priority. Nominal current (In): 8/15A. Motor power (230VAC): 0,37kW
FONTE RECARREGÁVEL PORTÁTIL	TEKSEA Tekpower SWP 3kW	Modes: Source, rechargeable and flotation. 125 Vdc (48 to 155). Comm. protocols: RS485/Modbus/IEC 61850
FIBRA ÓTICA	FURUKAWA COA-MM-P18-COG OPTICAL CORD	Full duplex single-mode. 25 metros

Figura 1: Características dos equipamentos utilizados nos cenários.

ANEXO II: DIAGRAMA UNIFILAR - COM ARQUITETURA TRADICIONAL

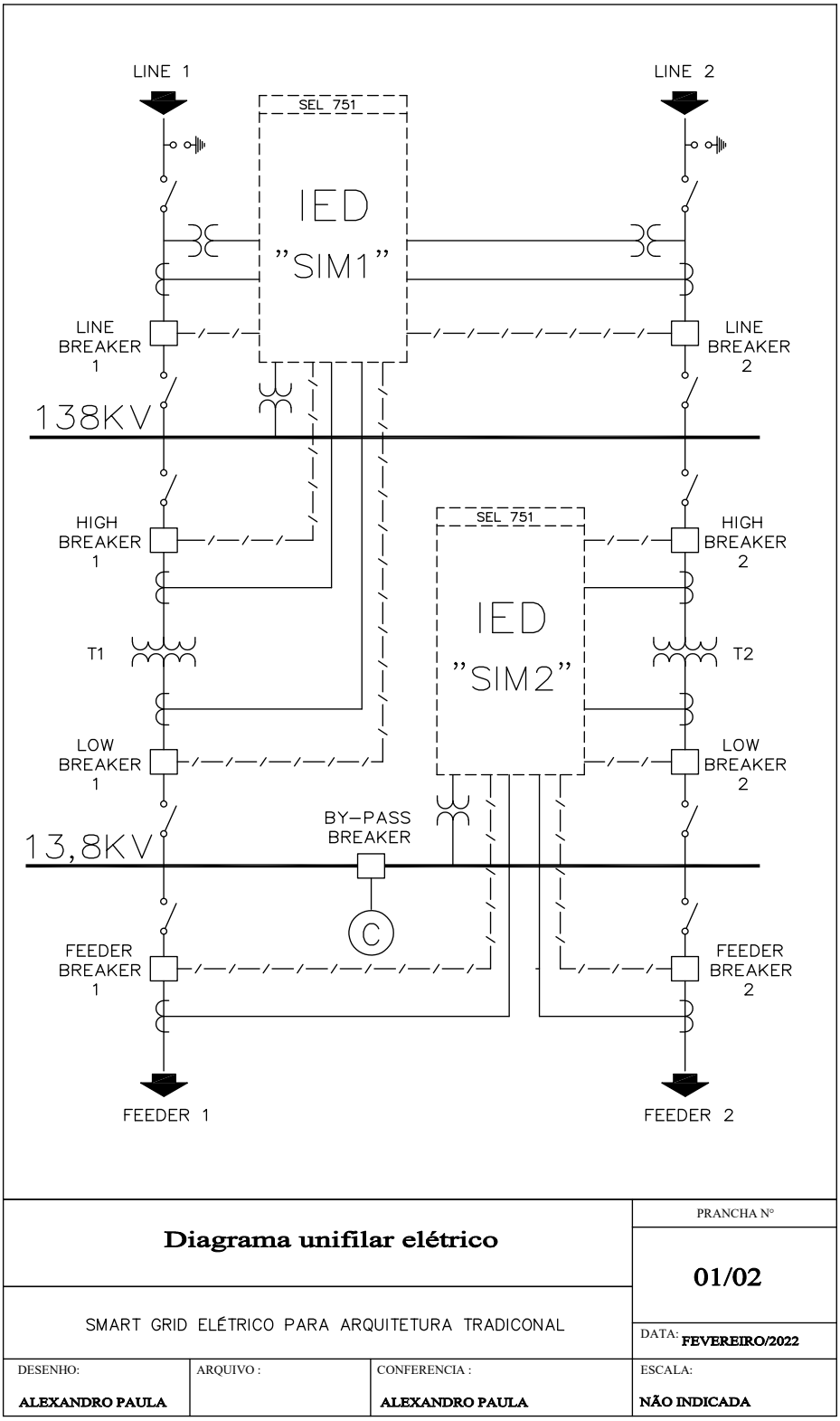


Figura 2: Diagrama unifilar - arquitetura tradicional (início).

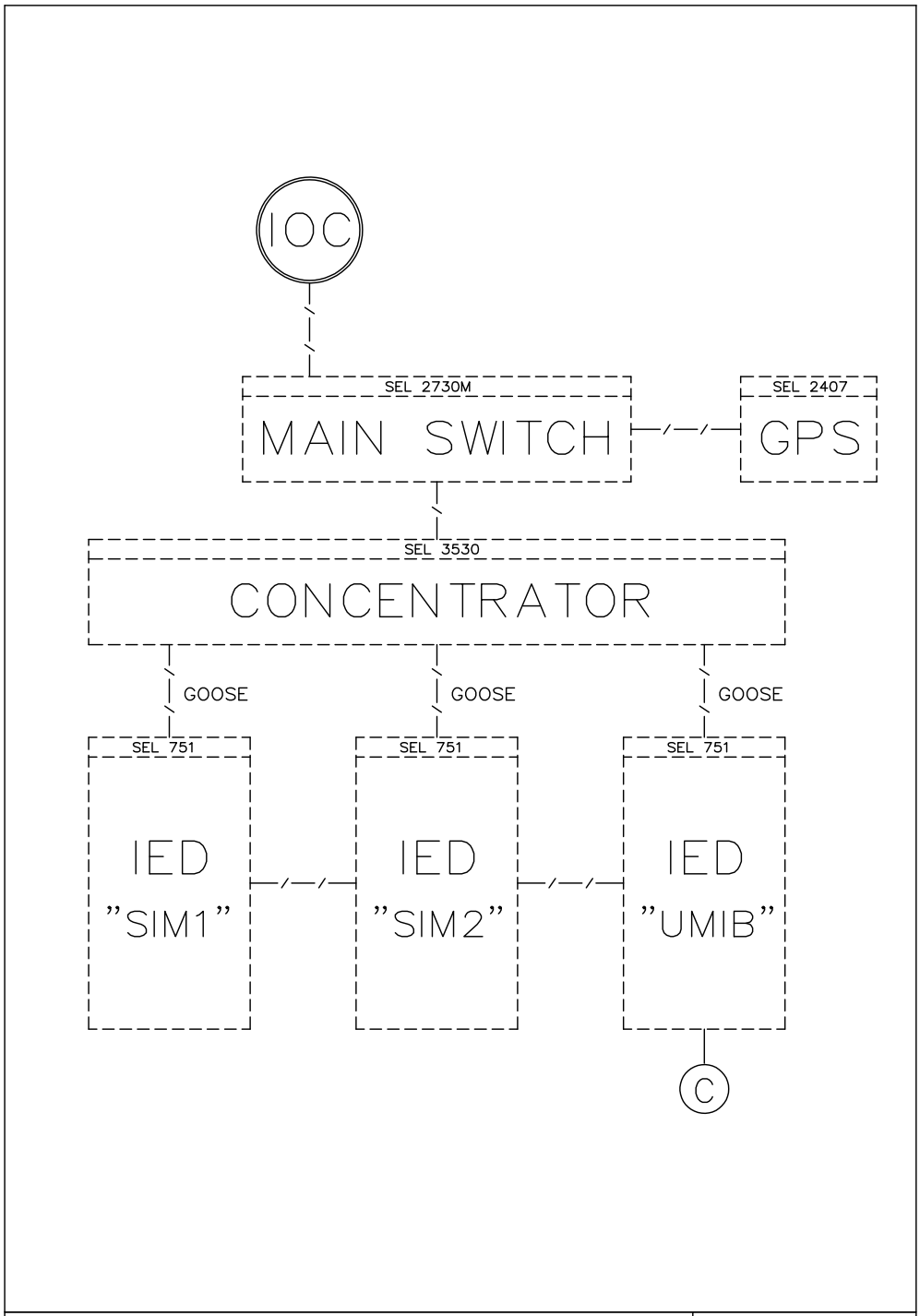


Diagrama unifilar elétrico			PRANCHA N° **02/02**
SMART GRID ELÉTRICO PARA ARQUITETURA TRADICONAL			DATA: **FEVEREIRO/2022**
DESENHO: **ALEXANDRO PAULA**	ARQUIVO :	CONFERENCIA : **ALEXANDRO PAULA**	ESCALA: **NÃO INDICADA**

Figura 3: Diagrama unifilar - arquitetura tradicional (continuação).

ANEXO III: DIAGRAMA UNIFILAR - COM ARQUITETURA ADAPTADA

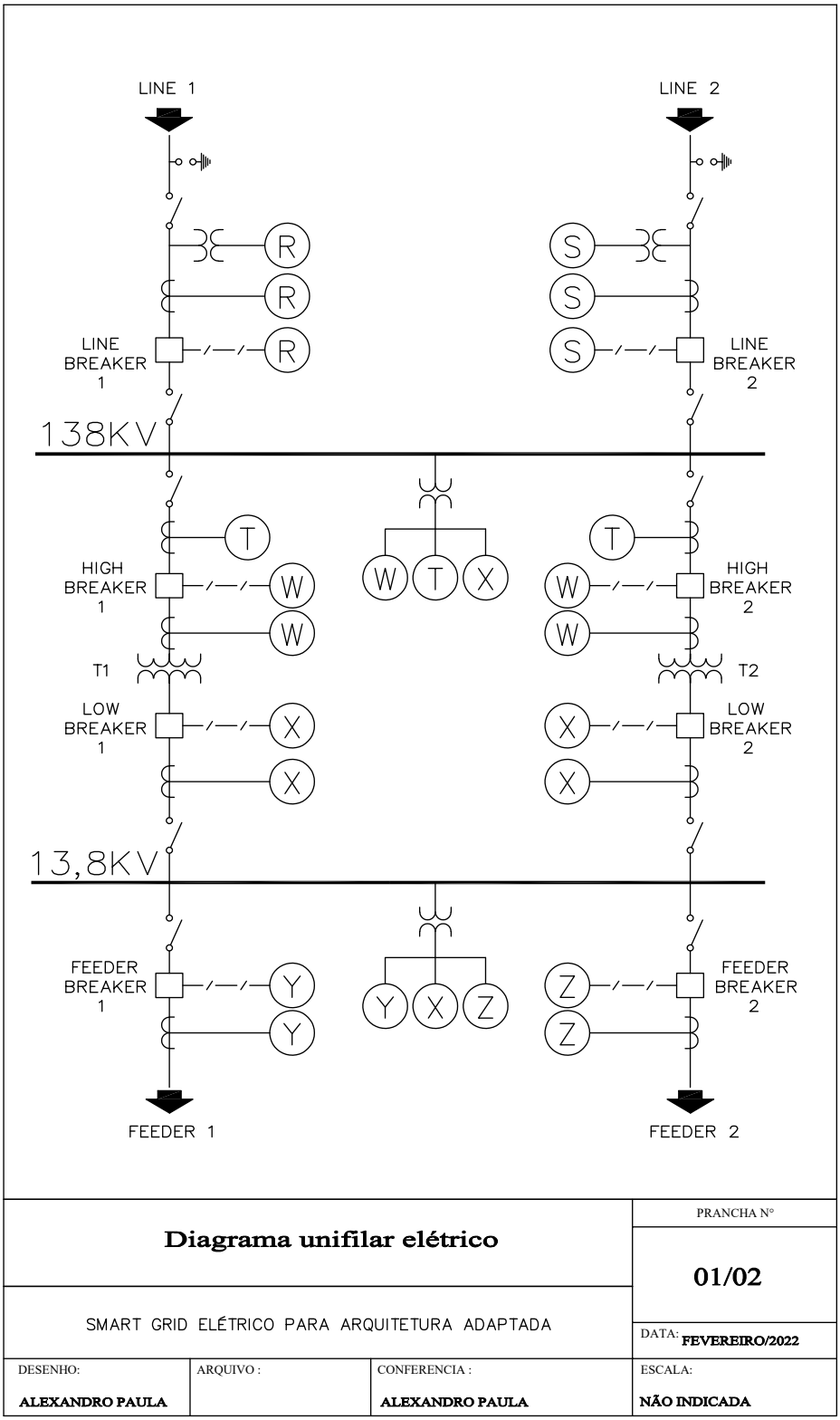


Figura 4: Diagrama unifilar - arquitetura adaptada (início).

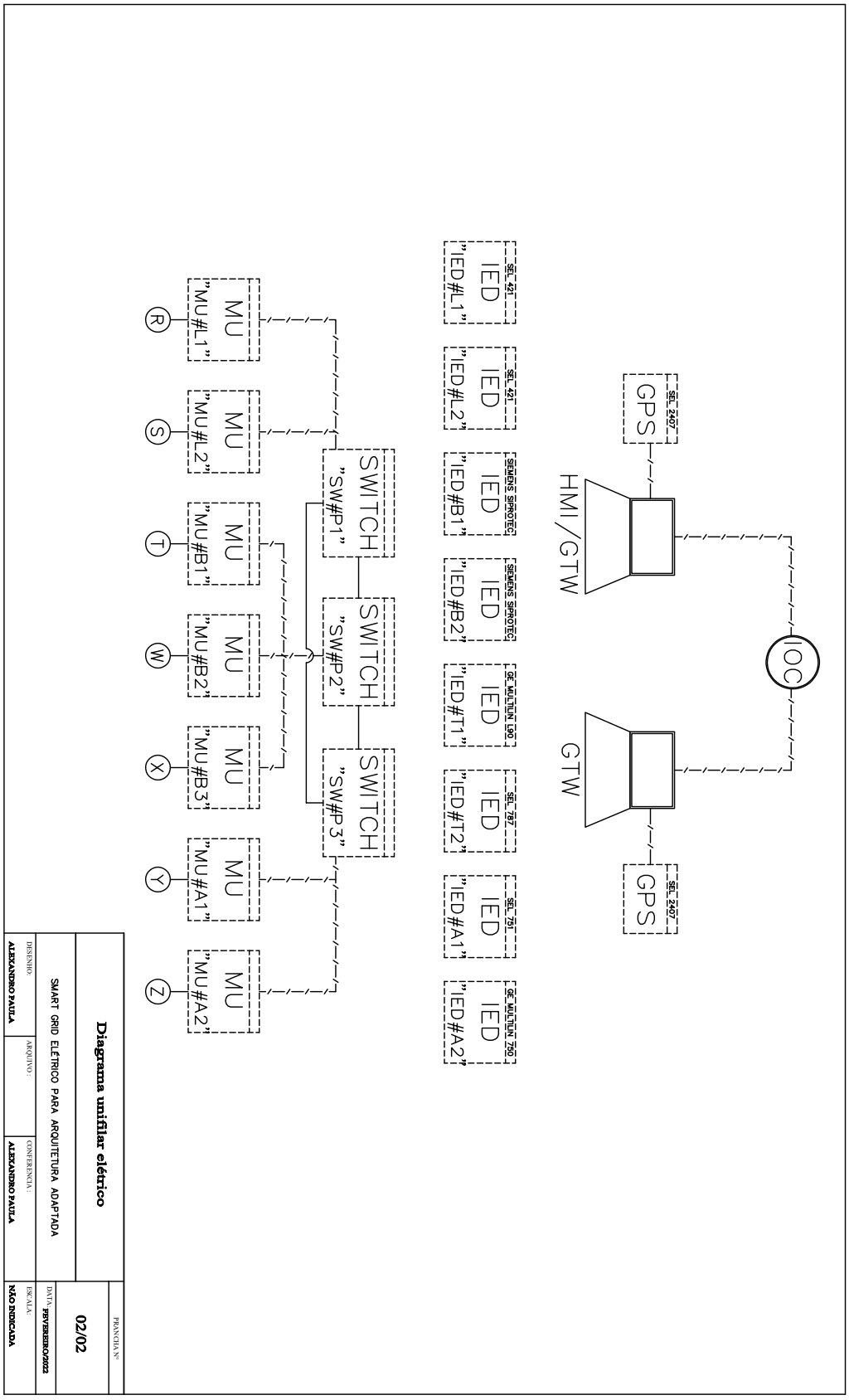


Figura 5: Diagrama unifilar - arquitetura adaptada (continuação).

ANEXO IV: TABELA ANSI DAS FUNÇÕES DE PROTEÇÃO EM IED'S (MAIS UTILIZADOS EM SMART GRIDS)

Cod.	Denominação	Cod.	Denominação
1	Elemento Principal	49	Relé térmico
2	Relé de partida ou fechamento temporizado	50	Relé de sobrecorrente instantâneo
3	Relé de verificação ou interbloqueio	51	Relé de sobrecorrente temporizado
4	Contator principal	52	Disjuntor de corrente alternada
5	Dispositivo de interrupção	53	Relé para excitatriz ou gerador CC
6	Disjuntor de partida	54	Dispositivo de acoplamento
7	Relé de taxa de variação	55	Relé de fator de potência
8	Dispositivo de desligamento da energia de controle	56	Relé de aplicação de campo
9	Dispositivo de reversão	57	Dispositivo de aterramento ou curto-circuito
10	Chave comutadora de sequência das unidades	58	Relé de falha de retificação
11	Dispositivo multifunção	59	Relé de sobretensão
12	Dispositivo de sobrevelocidade	60	Relé de balanço de corrente ou tensão
13	Dispositivo de rotação síncrona	61	Sensor de densidade
14	Dispositivo de subvelocidade	62	Relé temporizador
15	Dispositivo de ajuste ou comparação de velocidade e/ou frequência	63	Relé de pressão de gás (Buchholz)
16	Dispositivo de comunicação de dados	64	Relé detetor de terra
17	Chave de derivação ou descarga	65	Regulador
18	Dispositivo de aceleração ou desaceleração	66	Relé de supervisão do número de partidas
19	Contator de transição partida-marcha	67	Relé direcional de sobrecorrente
20	Válvula operada eletricamente	68	Relé de bloqueio por oscilação de potência
21	Relé de distância	69	Dispositivo de controle permissivo
22	Disjuntor equalizador	70	Reostato
23	Dispositivo de controle de temperatura	71	Dispositivo de detecção de nível
24	Relé de sobreexcitação ou Volts por Hertz	72	Disjuntor de corrente contínua
25	Relé de verificação de Sincronismo ou Sincronização	73	Contator de resistência de carga
26	Dispositivo térmico do equipamento	74	Relé de alarme
27	Relé de subtensão	75	Mecanismo de mudança de posição
28	Detector de chama	76	Relé de sobrecorrente CC
29	Contator de isolamento	77	Dispositivo de telemedição
30	Relé anunciador	78	Relé de medição de ângulo de fase / proteção contra falta de sincronismo
31	Dispositivo de excitação	79	Relé de religamento
32	Relé direcional de potência	80	Chave de fluxo
33	Chave de posicionamento	81	Relé de frequência (sub ou sobre)
34	Dispositivo master de sequência	82	Relé de religamento de carga de CC
35	Dispositivo para operação das escovas ou curto-circuitar anéis coletores	83	Relé de seleção / transferência automática
36	Dispositivo de polaridade ou polarização	84	Mecanismo de operação
37	Relé de subcorrente ou subpotência	85	Relé receptor de sinal de telecomunicação (teleproteção)
38	Dispositivo de proteção de mancal	86	Relé auxiliar de bloqueio
39	Monitor de condições mecânicas	87	Relé de proteção diferencial
40	Relé de perda de excitação ou relé de perda de campo	88	Motor auxiliar ou motor gerador
41	Disjuntor ou chave de campo	89	Chave seccionadora
42	Disjuntor / chave de operação normal	90	Dispositivo de regulação (regulador de tensão)
43	Dispositivo de transferência ou seleção manual	91	Relé direcional de tensão
44	Relé de sequência de partida	92	Relé direcional de tensão e potência
45	Monitor de condições atmosféricas	93	Contator de variação de campo
46	Relé de reversão ou desbalanceamento de corrente	94	Relé de desligamento
47	Relé de reversão ou desbalanceamento de tensão	95	Usado para aplicações específicas
48	Relé de sequência incompleta / partida longa	96	Relé auxiliar de bloqueio de barra

Figura 6: Tabela ANSI (contendo as funções mais utilizadas).

ANEXO V: EXTRATO DE EVENTOS DE MÉTRICAS

Taxa de IED's Afetados			Taxa de Disjuntores abertos			Integridade do COI		
Time (s)	*Trad.*	*STRAYER*	*Time (s)*	*Trad.*	*STRAYER*	*Time (s)*	*Trad.*	*STRAYER*
0	0%	0%	0	0%	0%	0	healthy	healthy
1	0%	0%	1	0%	0%	1	healthy	healthy
1	0%	0%	1	0%	0%	1	healthy	healthy
2	0%	0%	2	0%	0%	2	healthy	healthy
3	0%	0%	3	0%	0%	3	healthy	healthy
5	0%	0%	5	0%	0%	5	healthy	healthy
8	0%	0%	8	0%	0%	8	compromised	healthy
13	0%	0%	13	0%	0%	13	compromised	healthy
21	0%	0%	21	0%	0%	21	compromised	compromised
34	66,6%	0%	34	0%	0%	34	compromised	compromised
55	100%	0%	55	0%	0%	55	compromised	compromised
89	100%	0%	89	0%	0%	89	compromised	compromised
144	100%	0%	144	0%	0%	144	compromised	compromised
233	100%	0%	233	44,4%	0%	233	compromised	compromised
377	100%	0%	377	55,5%	0%	377	compromised	compromised
610	100%	12,5%	610	55,5%	0%	610	compromised	compromised
987	100%	12,5%	987	55,5%	0%	987	compromised	compromised
1597	100%	25,0%	1597	100%	11,1%	1597	compromised	compromised
2584	100%	37,5%	2584	100%	22,2%	2584	compromised	compromised
4181	100%	37,5%	4181	100%	22,2%	4181	compromised	compromised
6765	100%	37,5%	6765	100%	22,2%	6765	compromised	compromised
10946	100%	37,5%	10946	100%	22,2%	10946	compromised	compromised
17711	100%	37,5%	17711	100%	22,2%	17711	compromised	compromised

Figura 7: Eventos detalhados pelo tempo transcorrido do teste de acesso à rede TO, para três métricas.

Taxa de IED's Afetados			Taxa de Disjuntores abertos			Integridade do COI		
Time (s)	*Trad.*	*STRAYER*	*Time (s)*	*Trad.*	*STRAYER*	*Time (s)*	*Trad.*	*STRAYER*
0	0%	0%	0	0%	0%	0	healthy	healthy
1	0%	0%	1	0%	0%	1	healthy	healthy
1	0%	0%	1	0%	0%	1	healthy	healthy
2	0%	0%	2	0%	0%	2	healthy	healthy
3	0%	0%	3	0%	0%	3	healthy	healthy
5	0%	0%	5	0%	0%	5	healthy	healthy
8	0%	0%	8	0%	0%	8	healthy	healthy
13	0%	0%	13	0%	0%	13	healthy	healthy
21	0%	0%	21	0%	0%	21	healthy	healthy
34	0%	0%	34	0%	0%	34	healthy	healthy
55	0%	0%	55	0%	0%	55	healthy	healthy
89	0%	0%	89	0%	0%	89	healthy	healthy
144	0%	0%	144	0%	0%	144	compromised	healthy
233	33,3%	0%	233	0%	0%	233	compromised	healthy
377	100%	0%	377	44,4%	0%	377	compromised	healthy
610	100%	0%	610	44,4%	0%	610	compromised	compromised
987	100%	0%	987	100%	0%	987	compromised	compromised
1597	100%	0%	1597	100%	0%	1597	compromised	compromised
2584	100%	12,5%	2584	100%	22,2%	2584	compromised	compromised
4181	100%	12,5%	4181	100%	22,2%	4181	compromised	compromised
6765	100%	12,5%	6765	100%	22,2%	6765	compromised	compromised
10946	100%	12,5%	10946	100%	22,2%	10946	compromised	compromised
17711	100%	12,5%	17711	100%	22,2%	17711	compromised	compromised

Figura 8: Eventos detalhados pelo tempo transcorrido do teste de acesso à rede TI, para três métricas.

Taxa de IED's Afetados			Taxa de Disjuntores abertos			Integridade do COI		
Time (s)	*Trad.*	*STRAYER*	*Time (s)*	*Trad.*	*STRAYER*	*Time (s)*	*Trad.*	*STRAYER*
0	0%	0%	0	0%	0%	0	healthy	healthy
1	0%	0%	1	0%	0%	1	healthy	healthy
1	0%	0%	1	0%	0%	1	healthy	healthy
2	0%	0%	2	0%	0%	2	healthy	healthy
3	0%	0%	3	0%	0%	3	healthy	healthy
5	0%	0%	5	0%	0%	5	healthy	healthy
8	0%	0%	8	0%	0%	8	healthy	healthy
13	0%	0%	13	0%	0%	13	healthy	healthy
21	0%	0%	21	0%	0%	21	healthy	healthy
34	0%	0%	34	0%	0%	34	healthy	healthy
55	0%	0%	55	0%	0%	55	healthy	healthy
89	0%	0%	89	0%	0%	89	healthy	healthy
144	0%	0%	144	0%	0%	144	healthy	healthy
233	0%	0%	233	0%	0%	233	healthy	healthy
377	0%	0%	377	0%	0%	377	healthy	healthy
610	0%	0%	610	0%	0%	610	healthy	healthy
987	0%	0%	987	0%	0%	987	healthy	healthy
1597	0%	0%	1597	0%	0%	1597	compromised	healthy
2584	100%	0%	2584	100%	0%	2584	compromised	compromised
4181	100%	0%	4181	100%	0%	4181	compromised	compromised
6765	100%	12,5%	6765	100%	0%	6765	compromised	compromised
10946	100%	12,5%	10946	100%	11,1%	10946	compromised	compromised
17711	100%	12,5%	17711	100%	11,1%	17711	compromised	compromised

Figura 9: Eventos detalhados pelo tempo transcorrido do teste de acesso remoto, para três métricas.

ANEXO VI: ESTRUTURA BÁSICA DAS ATIVIDADES DE SEGURANÇA CIBERNÉTICA PARA INFRAESTRUTURAS CRÍTICAS - FRAMEWORK NIST E SUAS REFERÊNCIAS TÉCNICAS

Identificador Exclusivo de Função	Função	Identificador Exclusivo de Categoria	Categoria
ID	Identificar	***ID.AM***	Gerenciamento dos Ativos
		ID.BE	Contexto Empresarial
		ID.GV	Governança
		ID.RA	Avaliação de Risco
		ID.RM	Estratégia de Gerenciamento de Riscos
		ID.SC	Gerenciamento de Riscos da Cadeia de Suprimentos
PR	Proteger	***PR.AC***	Gerenciamento de identidade e controle de acesso
		PR.AT	Conscientização e Treinamento
		PR.DS	Segurança de Dados
		PR.IP	Processos e Procedimentos de Proteção da Informação
		PR.MA	Manutenção
		PR.PT	Tecnologia Protetora
DE	Detectar ou Diagnosticar	***DE.AE***	Anomalias e Incidentes
		DE.CM	Monitoramento Contínuo de Segurança
		DE.DP	Processos de Detecção
RS	Responder	***RS.RP***	Planejamento de Resposta
		RS.CO	Comunicações
		RS.AN	Análise
		RS.MI	Mitigação
		RS.IM	Aperfeiçoamentos
RC	Recuperar	***RC.RP***	Planejamento de Recuperação
		RC.IM	Aperfeiçoamentos
		RC.CO	Comunicações

Figura 10: Identificadores Exclusivos de Função e Categoria. Adaptada de [7].

Função	Categoria	Subcategoria	Referências Informativas
IDENTIFICAR (ID)	Gerenciamento de Ativos (ID.AM): Os dados, pessoal, dispositivos, sistemas e instalações que permitem que a organização atinja objetivos de negócio são identificados e gerenciados de maneira consistente com sua importância relativa para os objetivos organizacionais e a estratégia de risco da organização.	ID.AM-1: Dispositivos físicos e sistemas dentro da organização são inventariados	CIS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR. 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-2: Plataformas de software e aplicações dentro da organização são inventariadas	CIS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR. 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-3: Comunicação organizacional e fluxos de dados são mapeados	CIS CSC 12 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 NIST SP 800-53 Rev. 4 AC-4, 3-CA, CA-9, PL-8
		ID.AM-4: Sistemas de informação externos são catalogados	CIS CSC 12 COBIT 5 APO02.02, APO10.04, DSS01.02 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Recursos (por exemplo, hardware, dispositivos, dados, tempo, pessoal e software) são priorizados com base em suas classificações, criticidade e valor para os negócios	CIS CSC 13, 14 COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 ISA 62443-2-1:2009 4.2.3.6 ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Funções e responsabilidades de segurança cibernética para toda a força laboral e *stakeholders* de terceiros (por exemplo, fornecedores, clientes, parceiros) são estabelecidos	CIS CSC 17, 19 COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11

Figura 11: Estrutura básica com as subcategorias e referências (parte 1) [7].

Função	Categoria	Subcategoria	Referências Informativas
IDENTIFICAR (ID)	Contexto Empresarial (ID.BE): A missão, objetivos, *stakeholders* e atividades da organização são compreendidos e priorizados; essas informações são usadas para informar funções, responsabilidades e decisões de gerenciamento de riscos da segurança cibernética.	ID.BE-1: O papel da organização na cadeia de suprimentos é identificado e comunicado	COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
		ID.BE-2: O lugar da organização na infraestrutura crítica e seu setor industrial é identificado e comunicado	COBIT 5 APO02.06, APO03.01 ISO/IEC 27001:2013 Cláusula 4.1 NIST SP 800-53 Rev. 4 PM-8
		ID.BE-3: Prioridades para missão organizacional, objetivos e atividades são estabelecidas e comunicadas	COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 M-11, SA-14
		ID.BE-4: Dependências e funções críticas para a entrega de serviços críticos são estabelecidas	COBIT 5 APO10.01, BAI04.02, BAI09.02 ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Os requisitos de resiliência para apoiar a prestação de serviços críticos são estabelecidos para todos as condições operacionais (por exemplo, sob coerção/ ataque, durante a recuperação, operações normais)	COBIT 5 BAI03.02, DSS04.02 ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-13, SA- 14
	Governança (ID.GV): As políticas, procedimentos e processos para gerenciar e monitorar os requisitos regulatórios, jurídicos, de risco, ambientais e operacionais da organização são compreendidos e informam gerenciamento do risco de segurança cibernética.	ID. GV-1: A política organizacional de segurança cibernética é estabelecida e comunicada	CIS CSC 19 COBIT 5 APO01.03, APO13.01, EDM01.01, EDM01.02 ISA 62443-2-1:2009 4.3.2.6 ISO/IEC 27001:2013 A.5.1.1 NIST SP 800-53 4 Rev. -1 controles de todas as famílias de controle de segurança

Figura 12: Estrutura básica com as subcategorias e referências (parte 2) [7].

Função	Categoria	Subcategoria	Referências Informativas
IDENTIFICAR (ID)		ID.GV-2: As funções e responsabilidades de segurança cibernética são coordenadas e alinhadas com funções internas e parceiros externos	CIS CSC 19 COBIT 5 APO01.02, APO10.03, APO13.02, DSS05.04 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.15.1.1 NIST SP 800-53 Rev. 4 PS-7, PM-1, PM-2
		ID.GV-3: Os requisitos legais e regulamentares relativos à segurança cibernética, incluindo a privacidade e as obrigações das liberdades civis, são compreendidos e gerenciados	CIS CSC 19 COBIT 5 BAI02.01, MEA03.01, MEA03.04 ISA 62443-2-1:2009 4.4.3.7 ISO/IEC 27001:2013 A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 NIST SP 800-53 4 Rev. -1 controles de todas as famílias de controle de segurança
		ID.GV-4: Processos de governança e gerenciamento de riscos abordam os riscos de segurança cibernética	COBIT 5 EDM03.02, APO12.02, APO12.05, DSS04.02 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 ISO/IEC 27001:2013 Cláusula 6 NIST SP 800-53 Rev. 4 SA-2, PM-3, 7-PM, PM-9, 10 PM, PM-11
	Avaliação de risco (ID.RA): A organização entende o risco de segurança cibernética para operações organizacionais (incluindo missão, funções, imagem ou reputação), ativos organizacionais e indivíduos.	ID.RA-1: As vulnerabilidades dos ativos são identificadas e documentadas	CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Informações sobre ameaças cibernéticas são recebidas de fóruns e fontes de compartilhamento de informações	CIS CSC 4 COBIT 5 BAI08.01 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 4 SI-5, PM-15, PM-16

Figura 13: Estrutura básica com as subcategorias e referências (parte 3) [7].

Função	Categoria	Subcategoria	Referências Informativas
IDENTIFICAR (ID)		**ID.RA-3:** Ameaças internas e externas são identificadas e documentadas	**CIS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** Cláusula 6.1.2 **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM- 16
		ID.RA-4: Potenciais impactos no negócio e probabilidades são identificados na organização	**CIS CSC** 4 **COBIT 5** DSS04.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 6.1.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM- 9, PM-11
		ID.RA-5: Ameaças, vulnerabilidades, probabilidades e impactos são usados para determinar riscos	**CIS CSC** 4 **COBIT 5** APO12.02 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16
		ID.RA-6: As respostas ao risco são identificadas e priorizadas	**CIS CSC** 4 **COBIT 5** APO12.05, APO13.02 **ISO/IEC 27001:2013** Cláusula 6.1.3 **NIST SP 800-53 Rev. 4** PM-4, PM-9
	Estratégia de Gerenciamento de Riscos (ID.RM): As prioridades, restrições, tolerâncias de risco e suposições da organização são estabelecidas e usadas para apoiar as decisões de risco operacional.	**ID.RM-1:** Processos de gerenciamento de risco são estabelecidos, gerenciados e aprovados pelos *stakeholders* organizacionais	**CIS CSC** 4 **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001: 2013** Cláusula 6.1.3, Cláusula 8.3, Cláusula 9.3 **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-2: Tolerância ao risco organizacional é determinada e claramente expressa	**COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.2.6.5 **ISO/IEC 27001:2013** Cláusula 6.1.3, Cláusula 8.3 **NIST SP 800-53 Rev. 4** PM-9

Figura 14: Estrutura básica com as subcategorias e referências (parte 4) [7].

Função	Categoria	Subcategoria	Referências Informativas
IDENTIFICAR (ID)	Gerenciamento de Riscos da Cadeia de Suprimento (ID.SC): As prioridades, restrições, tolerâncias de risco e suposições da organização são definidas e utilizadas para apoiar as decisões de risco associadas ao gerenciamento do risco da cadeia de suprimentos. A organização definiu e implementou os processos para identificar, avaliar e gerenciar os riscos da cadeia de suprimentos.	ID.RM-3: A determinação de tolerância ao risco da organização é permeada pelo seu papel na infraestrutura crítica e na análise de risco específica do setor	COBIT 5 APO12.02 ISO/IEC 27001:2013 Cláusula 6.1.3, Cláusula 8.3 NIST SP 800-53 AP 4 SA-14, PM-8, PM-9 PM-11
		ID.SC-1: Os processos de gerenciamento de riscos da cadeia de suprimentos cibernéticos são identificados, estabelecidos, avaliados, gerenciados e acordados pelos *stakeholders* da organização.	CIS CSC 4 COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 SA-9, SA-12, PM-9
		ID.SC-2: Fornecedores e parceiros terceirizados de sistemas de informação, componentes e serviços são identificados, priorizados e avaliados usando um processo de avaliação de risco da cadeia de suprimentos cibernéticos	COBIT 5 APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-12, SA- 14, SA-15, PM-9
		ID.SC-3: Os contratos com fornecedores e parceiros terceirizados são usados para implementar medidas apropriadas projetadas para atender aos objetivos do programa de segurança cibernética de uma organização e do Plano de Gerenciamento de Riscos da Cadeia de Suprimentos Cibernéticos	COBIT 5 APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 ISA 62443-2-1:2009 4.3.2.6.4, 4.3.2.6.7 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3 NIST SP 800-53 Rev. 4 SA-9, SA-11, SA-12, 9 PM

Figura 15: Estrutura básica com as subcategorias e referências (parte 5) [7].

Função	Categoria	Subcategoria	Referências Informativas
IDENTIFICAR (ID)		**ID.SC-4:** Fornecedores e parceiros terceirizados são avaliados sistematicamente por meio de auditorias, resultados de testes ou outras formas de avaliações para confirmar que estão cumprindo suas obrigações contratuais	**COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 **ISA 62443-2-1:2009** 4.3.2.6.7 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
		ID.SC-5: O planejamento e o teste de resposta e recuperação são realizados com prestadores e fornecedores de serviços terceirizados	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3: 2013** SR 2.8, SR 3.3, SR.6.1, SR-7.3, SR 7.4 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 4** CP-2, CP-4, 3-IR, IR-4, 6-IR, IR-8, IR-9
PROTEGER (PR)	**Gerenciamento de Identidade, Autenticação e Controle de Acesso (PR.AC):** O acesso a ativos físicos e lógicos e recursos associados é limitado a usuários, processos e dispositivos autorizados e é gerenciado de maneira consistente com o risco avaliado de acesso não autorizado a atividades e transações autorizadas.	**PR.AC-1:** Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	**CIS CSC** 1, 5, 15, 16 **COBIT 5** DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.5.1 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR-1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 e3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.AC-2: O acesso físico aos ativos é gerenciado e protegido	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8

Figura 16: Estrutura básica com as subcategorias e referências (parte 6) [7].

Função	Categoria	Subcategoria	Referências Informativas
PROTEGER (PR)		PR.AC-3: O acesso remoto é gerenciado	CIS CSC 12 COBIT 5 APO13.01, DSS01.04, DSS05.03 ISA 62443-2-1:2009 4.3.3.6.6 ISA 62443-3-3:2013 SR 1.13, SR 2.6 ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 NIST SP 800-53 Rev. 4 AC-1, AC-17, 19-AC, AC-20, SC-15
		PR.AC-4: Permissões de acesso e autorizações são gerenciadas, incorporando os princípios de menor privilégio e divisão de tarefas	CIS CSC 3, 5, 12, 14, 15, 16, 18 COBIT 5 DSS05.04 ISA 62443-2-1:2009 4.3.3.7.3 ISA 62443-3-3:2013 SR 2.1 ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, 16-AC, AC-24
		PR.AC-5: A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	CIS CSC 9, 14, 15, 18 COBIT 5 DSS01.05, DSS05.02 ISA 62443-2-1:2009 4.3.3.4 ISA 62443-3-3:2013 SR 3.1, SR 3.8 ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7
		PR.AC-6: As identidades são revisadas, vinculadas a credenciais e confirmadas em interações	CIS CSC ,16 COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03 ISA 62443-2-1:2009 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.4, SR-1.5, SR 1.9, SR 2.1 ISO/IEC 27001:2013, A.7.1.1, A.9.2.1 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, 4-IA, IA-5, IA-8, PE-2, PS-3

Figura 17: Estrutura básica com as subcategorias e referências (parte 7) [7].

Função	Categoria	Subcategoria	Referências Informativas
PROTEGER (PR)		**PR.AC-7:** Usuários, dispositivos e outros recursos são autenticados (por exemplo, fator único, multifator) de acordo com o risco da transação (por exemplo, riscos de segurança e privacidade de indivíduos e outros riscos organizacionais)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
	Conscientização e Treinamento (PR.AT): Os funcionários e parceiros da organização são treinados sobre a conscientização sobre segurança cibernética e são treinados para executar suas obrigações e responsabilidades relacionadas à segurança cibernética, de acordo com os procedimentos e acordos relacionados.	**PR.AT-1:** Todos os utilizadores são informados a respeito e treinados	**CIS CSC** 17, 18 **COBIT 5** APO07.03, BAI05.07 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 **NIST SP 800-53 Rev. 4** AT-2, PM-13
		PR.AT-2: Os usuários privilegiados compreendem suas funções e responsabilidades	**CIS CSC** 5, 17, 18 **COBIT 5** APO07.02, DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-3: *Stakeholders* terceirizados (por exemplo, fornecedores, clientes, parceiros) entendem suas funções e responsabilidades	**CIS CSC** 17 **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2 **NIST SP 800-53 Rev. 4** PS-7, SA-9, SA-16
		PR.AT-4: Executivos seniores compreendem suas funções e responsabilidades	**CIS CSC** 17, 19 **COBIT 5** EDM01.01, APO01.02, APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13

Figura 18: Estrutura básica com as subcategorias e referências (parte 8) [7].

Função	Categoria	Subcategoria	Referências Informativas
PROTEGER (PR)		PR.AT-5: Os funcionários físicos e de segurança cibernética compreendem suas funções e responsabilidades	CIS CSC 17 COBIT 5 APO07.03 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-3, IR-2, PM-13
	Segurança de Dados (PR.DS): As informações e os registros (dados) são gerenciados de maneira consistente com a estratégia de risco da organização para proteger a confidencialidade, a integridade e a disponibilidade de informações.	PR.DS-1: Os dados em repouso são protegidos	CIS CSC 13, 14 COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 ISA 62443-3-3:2013 SR 3.4, SR 4.1 ISO/IEC 27001:2013 A.8.2.3 NIST SP 800-53 Rev. 4 MP-8, 12-SC, SC-28
		PR.DS-2: Os dados em trânsito são protegidos	CIS CSC 13, 14 COBIT 5 APO01.06, DSS05.02, DSS06.06 ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12
		PR.DS-3: Ativos são formalmente gerenciados durante a remoção, transferências e disposição	CIS CSC 1 COBIT 5 BAI09.03 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.4.4.1 ISA 62443-3-3:2013 SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16
		PR.DS-4: A capacidade adequada para garantir a disponibilidade é mantida	CIS CSC 1, 2, 13 COBIT 5 APO13.01, BAI04.04 ISA 62443-3-3:2013 SR 7.1, SR 7.2 ISO/IEC 27001:2013 A.12.1.3, A.17.2.1 NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5
		PR.DS-5: As proteções contra vazamentos de dados são implementadas	CIS CSC 13 COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02 ISA 62443-3-3:2013 SR 5.2 ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2,

Figura 19: Estrutura básica com as subcategorias e referências (parte 9) [7].

Função	Categoria	Subcategoria	Referências Informativas
PROTEGER (PR)			A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3
		PR.DS-6: Os mecanismos de verificação de integridade são usados para verificar o software, o firmware e a integridade das informações	CIS CSC 2, 3 COBIT 5 APO01.06, BAI06.01, DSS06.02 ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 NIST SP 800-53 Rev. 4 SC-16, SI-7
		PR.DS-7: O(s) ambiente(s) de desenvolvimento e teste é separado do ambiente de produção	CIS CSC 18, 20 COBIT 5 BAI03.08, BAI07.04 ISO/IEC 27001:2013 A.12.1.4 NIST SP 800-53 Rev. 4 CM-2
		PR.DS-8: Mecanismos de verificação de integridade são usados para verificar a integridade do hardware	COBIT 5 BAI03.05 ISA 62443-2-1:2009 4.3.2.4.4 ISO/IEC 27001:2013 A.11.2.4 NIST SP 800-53 Rev. 4 SA-10, SI-7
	Processos e Procedimentos de Proteção da Informação (PR.IP): As políticas de segurança (que abordam a finalidade, o escopo, as funções, as responsabilidades, o compromisso de gerenciamento e a coordenação entre as entidades organizacionais), processos e procedimentos são mantidas e usadas para gerenciar a proteção de sistemas e ativos de informações.	PR.IP-1: Uma configuração básica de sistemas de tecnologia de informação/controle industrial é criada e mantida, incorporando princípios de segurança (por exemplo, conceito de menor funcionalidade)	CIS CSC 3, 9, 11 COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR. 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: Um Ciclo de Vida de Desenvolvimento de Sistema para gerenciar sistemas é implementado	CIS CSC 18 COBIT 5 APO13.01, BAI03.01, BAI03.02, BAI03.03 ISA 62443-2-1:2009 4.3.4.3.3 ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1 A.14.2.5 NIST SP 800-53 Rev. 4 PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17

Figura 20: Estrutura básica com as subcategorias e referências (parte 10) [7].

Função	Categoria	Subcategoria	Referências Informativas
PROTEGER (PR)		PR.IP-3: Processos de controle de mudança de configuração estão em funcionamento	CIS CSC 3, 11 COBIT 5 BAI01.06, BAI06.01 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR. 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10
		PR.IP-4: Os Backups de informações são realizados, conservados e testados	CIS CSC 10 COBIT 5 APO13.01, DSS01.01, DSS04.07 ISA 62443-2-1:2009 4.3.4.3.9 ISA 62443-3-3:2013 SR 7.3, SR 7.4 ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9
		PR.IP-5: As políticas e os regulamentos referentes ao ambiente operacional físico dos ativos organizacionais são cumpridos	COBIT 5 DSS01.04, DSS05.05 ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Os dados são destruídos de acordo com a política	COBIT 5 BAI09.03, DSS05.06 ISA 62443-2-1:2009 4.3.4.4 ISA 62443-3-3:2013 SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 NIST SP 800-53 Rev. 4 MP-6
		PR.IP-7: Os processos de proteção são aperfeiçoados	COBIT 5 APO11.06, APO12.06, DSS04.05 ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 ISO / IEC 27001: 2013 A.16.1.6 Cláusula 9, Cláusula 10 NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6

Figura 21: Estrutura básica com as subcategorias e referências (parte 11) [7].

Função	Categoria	Subcategoria	Referências Informativas
PROTEGER (PR)		**PR.IP-8:** A eficácia das tecnologias de proteção é compartilhada	**COBIT 5** BAI08.04, DSS03.04 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
		PR.IP-9: Planos de resposta (Resposta a Incidentes e Continuidade de Negócios) e planos de recuperação (Recuperação de Incidentes e Recuperação de Desastres) estão em vigor e gerenciados	**CIS CSC** 19 **COBIT 5** APO11.06, APO12.06, DSS04.03 **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 **NIST SP 800-53 Rev. 4** CP-2, 7-CP, CP-12, CP-13, IR-7, 8-IR, IR-9, PE-17
		PR.IP-10: Planos de recuperação e resposta são testados	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14
		PR.IP-11: A segurança cibernética está incluída nas práticas de recursos humanos (por exemplo, desaprovisionamento, triagem de pessoal)	**CIS CSC** 5, 16 **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 **ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 **NIST SP 800-53 Rev. 4** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, 7-PS, PS-8, SA-21
		PR.IP-12: Um plano de gerenciamento de vulnerabilidades é desenvolvido e implementado	**CIS CSC** 4, 18, 20 **COBIT 5** BAI03.10, DSS05.01, DSS05.02 **ISO/IEC 27001:2013**A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
	Manutenção (PR.MA): A manutenção e os reparos de componentes de sistemas de controle e informações industriais são executados de acordo com políticas e procedimentos.	**PR. MA-1:** Manutenção e reparo de ativos organizacionais são realizados e registrados, com ferramentas aprovadas e regulamentadas	**COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.7 **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 MA **de Rev. 4-2,** NIST SP 800-53 MA-3, 5-MA, MA-6

Figura 22: Estrutura básica com as subcategorias e referências (parte 12) [7].

Função	Categoria	Subcategoria	Referências Informativas
PROTEGER (PR)		PR.MA-2: A manutenção remota de ativos organizacionais é aprovada, registrada e realizada de maneira a impedir o acesso não autorizado	CIS CSC 3, 5 COBIT 5 DSS05.04 ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 NIST SP 800-53 Rev. 4 MA-4
	Tecnologia Protetora (PR.PT): As soluções de segurança técnica são gerenciadas para garantir a segurança e resiliência de sistemas e ativos, consistentes com políticas, procedimentos e acordos relacionados.	PR.PT-1: Os registros de auditoria/registro são determinados, documentados, implementados e revisados de acordo com a política	CIS CSC 1, 3, 5, 6, 14, 15, 16 COBIT 5 APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR-2.11, SR 2.12 ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 NIST SP 800-53 Rev. 4 AU Família
		PR.PT-2: As mídias removíveis são protegidas e seu uso é restrito de acordo com a política	CIS CSC 8, 13 COBIT 5 APO13.01, DSS05.02, DSS05.06 ISA 62443-3-3:2013 SR 2.3 ISO/IEC 27001:2013 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 NIST SP 800-53 Rev. 4 MP-2 MP-3, MP-4, MP -5, MP-7, MP-8
		PR.PT-3: O princípio de menor funcionalidade é incorporado pela configuração de sistemas para fornecer apenas recursos essenciais	CIS CSC 3, 11, 14 COBIT 5 DSS05.02, DSS05.05, DSS06.06 ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR-1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR-1.10, SR 1.11 SR 1.12, SR. 1.13, SR 2.1, SR 2.2, SR-2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 ISO/IEC 27001:2013 A.9.1.2 NIST SP 800-53 Rev. 4 AC-3, CM-7

Figura 23: Estrutura básica com as subcategorias e referências (parte 13) [7].

Função	Categoria	Subcategoria	Referências Informativas
PROTEGER (PR)		**PR.PT-4:** Redes de comunicação e controle são protegidas	**CIS CSC** 8, 12, 15 **COBIT 5** DSS05.02, APO13.01 **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR-4.1, SR 4.3, SR 5.1, 5.2 de SR, SR 5.3, SR 7.1, SR 7,6 **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, 25-SC, SC-29, SC-32, SC-36, 37-SC, SC-38, SC-39, SC-40, SC-41, SC-43
		PR.PT-5: Alguns mecanismos (por exemplo, *fail-safe, load balancing, hot swap*) são implementados para garantir que requisitos de resiliência funcionem em situações normais e adversas	**COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 **ISA 62443-2-1:2009** 4.3.2.5.2 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6
DETECTAR (DE)	**Anomalias e Incidentes (DE.AE):** Atividade anômala é detectada e o impacto potencial dos eventos é compreendido.	**DE.AE-1:** Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada	**CIS CSC** 1, 4, 6, 12, 13, 15, 16 **COBIT 5** DSS03.01 **ISA 62443-2-1:2009** 4.4.3.3 **ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Os eventos detectados são analisados para compreender os alvos e métodos de ataque	**CIS CSC** 3, 6, 13, 15 **COBIT 5** DSS05.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR-2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4

Figura 24: Estrutura básica com as subcategorias e referências (parte 14) [7].

Função	Categoria	Subcategoria	Referências Informativas
DETECTAR (DE)		DE.AE-1: Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada	CIS CSC 1, 4, 6, 12, 13, 15, 16 COBIT 5 DSS03.01 ISA 62443-2-1:2009 4.4.3.3 ISO/IEC 27001:2013 A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Os eventos detectados são analisados para compreender os alvos e métodos de ataque	CIS CSC 3, 6, 13, 15 COBIT 5 DSS05.07 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 ISO/IEC 27001:2013 A.12.4.1, A.16.1.1, A.16.1.4 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Os dados da ocorrência são coletados e correlacionados a partir de várias fontes e sensores	CIS CSC 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 COBIT 5 BAI08.02 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.12.4.1, A.16.1.7 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: O impacto dos eventos é determinado	CIS CSC 4, 6 COBIT 5 APO12.06, DSS03.01 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4
		DE.AE-5: Os limites de alerta de incidentes são estabelecidos	CIS CSC 6, 19 COBIT 5 APO12.06, DSS03.01 ISA 62443-2-1:2009 4.2.3.10 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8
	Monitoramento Contínuo de Segurança (DE.CM): O sistema de informação e os ativos são monitorados para identificar incidentes de segurança cibernética e verificar a eficácia das medidas de proteção.	DE.CM-1: A rede é monitorada para detectar potenciais incidentes de segurança cibernética	CIS CSC 1, 7, 8, 12, 13, 15, 16 COBIT 5 DSS01.03, DSS03.05, DSS05.07 ISA 62443-3-3:2013 SR 6.2 NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM- 3, SC-5, SC-7, SI-4

Figura 25: Estrutura básica com as subcategorias e referências (parte 15) [7].

Função	Categoria	Subcategoria	Referências Informativas
DETECTAR (DE)		DE.CM-2: O ambiente físico é monitorado para detectar possíveis eventos de segurança cibernética	COBIT 5 DSS01.04, DSS01.05 ISA 62443-2-1:2009 4.3.3.3.8 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2 NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20
		DE.CM-3: A atividade dos colaboradores é monitorada para detectar possíveis eventos de segurança cibernética	CIS CSC 5, 7, 14, 16 COBIT 5 DSS05.07 ISA 62443-3-3:2013 SR 6.2 ISO/IEC 27001:2013 A.12.4.1, A.12.4.3 NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Código malicioso é detectado	CIS CSC 4, 7, 8, 12 COBIT 5 DSS05.01 ISA 62443-2-1:2009 4.3.4.3.8 ISA 62443-3-3:2013 SR 3.2 ISO/IEC 27001:2013 A.12.2.1 NIST SP 800-53 Rev. 4 SI-3, SI-8
		DE.CM-5: Código móvel não autorizado é detectado	CIS CSC 7, 8 COBIT 5 DSS05.01 ISA 62443-3-3:2013 SR 2.4 ISO/IEC 27001:2013 A.12.5.1, A.12.6.2 NIST SP 800-53 Rev. 4 SC-18, SI-4, SC-44
		DE.CM-6: A atividade de provedor de serviços externo é monitorada para detectar possíveis eventos de segurança cibernética	COBIT 5 APO07.06, APO10.05 ISO/IEC 27001:2013 A.15.2.7, A.15.2.1 NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: O monitoramento de colaboradores não autorizados, conexões, dispositivos e software é executado	CIS CSC 1, 2, 3, 5, 9, 12, 13, 15, 16 COBIT 5 DSS05.02, DSS05.05 ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1 NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, 6-PE, PE-20, SI-4
		DE.CM-8: Há realização de varreduras de vulnerabilidade	CIS CSC 4, 20 COBIT 5 BAI03.10, DSS05.01 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-5

Figura 26: Estrutura básica com as subcategorias e referências (parte 16) [7].

Função	Categoria	Subcategoria	Referências Informativas
DETECTAR (DE)	Processos de Detecção (DE.DP): Os processos e procedimentos de detecção são mantidos e testados para garantir a conscientização sobre eventos anômalos	DE.DP-1: Papéis e responsabilidades para a detecção são bem definidos para garantir a prestação de contas	CIS CSC 19 COBIT 5 APO01.02, DSS05.01, DSS06.03 ISA 62443-2-1:2009 4.4.3.1 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14
		DE.DP-2: As atividades de detecção cumprem todos os requisitos aplicáveis	COBIT 5 DSS06.01, MEA03.03, MEA03.04 ISA 62443-2-1:2009 4.4.3.2 ISO/IEC 27001:2013 A.18.1.4, A.18.2.2, A.18.2.3 NIST SP 800-53 Rev. 4 AC-25, CA-2, CA-7, SA- 18, SI-4, PM-14
		DE.DP-3: Os processos de detecção são testados	COBIT 5 APO13.02, DSS05.02 ISA 62443-2-1:2009 4.4.3.2 ISA 62443-3-3:2013 SR 3.3 ISO/IEC 27001:2013 A.14.2.8 NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
		DE.DP-4: Informações de detecção de incidente são comunicadas	CIS CSC 19 COBIT 5 APO08.04, APO12.06, DSS02.05 ISA 62443-2-1:2009 4.3.4.5.9 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.16.1.2, A.16.1.3 NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA- 5, SI-4
		DE.DP-5: Processos de detecção são continuamente aperfeiçoados	COBIT 5 APO11.06, APO12.06, DSS04.05 ISA 62443-2-1:2009 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA- 5, SI-4, PM-14
RESPONDER (RS)	Planejamento de Respostas (RS.RP): Os processos e procedimentos de resposta são executados e mantidos para garantir a resposta a incidentes de segurança cibernética detectados.	RS.RP-1: Plano de resposta é executado durante ou depois de um incidente	CIS CSC 19 COBIT 5 APO12.06, BAI01.10 ISA 62443-2-1:2009 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8

Figura 27: Estrutura básica com as subcategorias e referências (parte 17) [7].

Função	Categoria	Subcategoria	Referências Informativas
RESPONDER (RS)	**Comunicações (RS.CO):** As atividades de resposta são coordenadas com *stakeholders* internos e externos (por exemplo, apoio externo de órgãos fiscalizadores)	**RS.CO-1:** Os colaboradores conhecem seus papéis e a sequência de operações quando uma resposta é necessária	**CIS CSC** 19 **COBIT 5** EDM03.02, APO01.02, APO12.03 **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Os incidentes são informados de acordo com os critérios estabelecidos	**CIS CSC** 19 **COBIT 5** DSS01.03 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3: As informações são compartilhadas de acordo com os planos de resposta	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.2 **ISO/IEC 27001:2013** A.16.1.2, Cláusula 7.4, Cláusula 16.1.2 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: A coordenação com os *stakeholders* ocorre de acordo com os planos de resposta	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** Cláusula 7.4 **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
		RS.CO-5: O compartilhamento voluntário de informações ocorre com os *stakeholders* externos para alcançar uma conscientização situacional mais ampla sobre segurança cibernética	**CIS CSC** 19 **COBIT 5** BAI08.04 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 4** SI-5, PM-15

Figura 28: Estrutura básica com as subcategorias e referências (parte 18) [7].

Função	Categoria	Subcategoria	Referências Informativas
RESPONDER (RS)	**Análise (RS.AN):** A análise é realizada para garantir resposta eficaz e dar apoio às atividades de recuperação.	**RS.AN-1:** As notificações dos sistemas de detecção são analisadas	**CIS CSC** 4, 6, 8, 19 **COBIT 5** DSS02.04, DSS02.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: O impacto do incidente é compreendido	**COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: Há realização de investigações	**COBIT 5** APO12.06, DSS03.02, DSS05.07 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 **ISO/IEC 27001:2013** A.16.1.7 **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: Os incidentes são categorizados de forma consistente com os planos de resposta	**CIS CSC** 19 **COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
		RS.AN-5: Os processos são estabelecidos para receber, analisar e responder às vulnerabilidades divulgadas para a organização a partir de fontes internas e externas (por exemplo, testes internos, boletins de segurança ou pesquisadores de segurança).	**CIS CSC** 4, 19 **COBIT 5** EDM03.02, DSS05.07 **NIST SP 800-53 Rev. 4** SI-5, PM-15

Figura 29: Estrutura básica com as subcategorias e referências (parte 19) [7].

Função	Categoria	Subcategoria	Referências Informativas
RESPONDER (RS)	**Mitigação (RS.MI):** As atividades são realizadas para impedir a expansão de um evento, atenuar seus efeitos e resolver o incidente.	**RS.MI-1:** Os incidentes são contidos	**CIS CSC** 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53 Rev. 4** IR-4
RESPONDER (RS)		**RS.MI-2:** Os incidentes são mitigados	**CIS CSC** 4, 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-3: As vulnerabilidades identificadas recentemente são mitigadas ou documentadas como riscos aceitos	**CIS CSC** 4 **COBIT 5** APO12.06 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
	Aperfeiçoamentos (RS.IM): As atividades de resposta organizacionais são aperfeiçoadas pela incorporação de lições aprendidas de atividades anteriores de detecção/resposta.	**RS.IM-1:** Os planos de resposta incorporam as lições aprendidas	**COBIT 5** BAI01.13 **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 10 **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
		RS.IM-2: As estratégias de resposta são atualizadas	**COBIT 5** BAI01.13, DSS04.08 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 10 **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
RECUPERAR (RC)	**Planejamento de Recuperação (RC.RP):** Os processos e procedimentos de recuperação são executados e mantidos para garantir a restauração de sistemas ou ativos afetados por incidentes de segurança cibernética.	**RC.RP-1:** O Plano de recuperação é executado durante ou após um incidente de segurança cibernética	**CIS CSC** 10 **COBIT 5** APO12.06, DSS02.05, DSS03.04 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8

Figura 30: Estrutura básica com as subcategorias e referências (parte 20) [7].

Função	Categoria	Subcategoria	Referências Informativas
RECUPERAR (RC)	Aperfeiçoamentos (RC.IM): O planejamento e os processos de recuperação são aperfeiçoados pela incorporação de lições aprendidas em atividades futuras	RC. IM-1: Planos de recuperação incorporam as lições aprendidas	COBIT 5 APO12.06, BAI05.07, DSS04.08 ISA 62443-2-1:2009 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6, Cláusula 10 NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
		RC.IM-2: As estratégias de recuperação são atualizadas	COBIT 5 APO12.06, BAI07.08 ISO/IEC 27001:2013 A.16.1.6, Cláusula 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
	Comunicações (RC.CO): As atividades de restauração são coordenadas com partes internas e externas (por exemplo, centros de coordenação, provedores de serviços de Internet, proprietários de sistemas de ataque, vítimas, outras CSIRTs e fornecedores).	RC.CO-1: As relações públicas são gerenciadas	COBIT 5 EDM03.02 ISO/IEC 27001:2013 A.6.1.4, Cláusula 7.4
		RC.CO-2: A reputação é reparada após um incidente	COBIT 5 MEA03.02 ISO/IEC 27001:2013 Cláusula 7.4
		RC.CO-3: As atividades de recuperação são comunicadas aos *stakeholders* internos e externos, bem como às equipes executivas e de gestão.	COBIT 5 APO12.06 ISO/IEC 27001:2013 Cláusula 7.4 NIST SP 800-53 Rev. 4 CP-2, IR-4

Figura 31: Estrutura básica com as subcategorias e referências (parte 21) [7].

ANEXO VII: *PRINT SCREENS* RELEVANTES

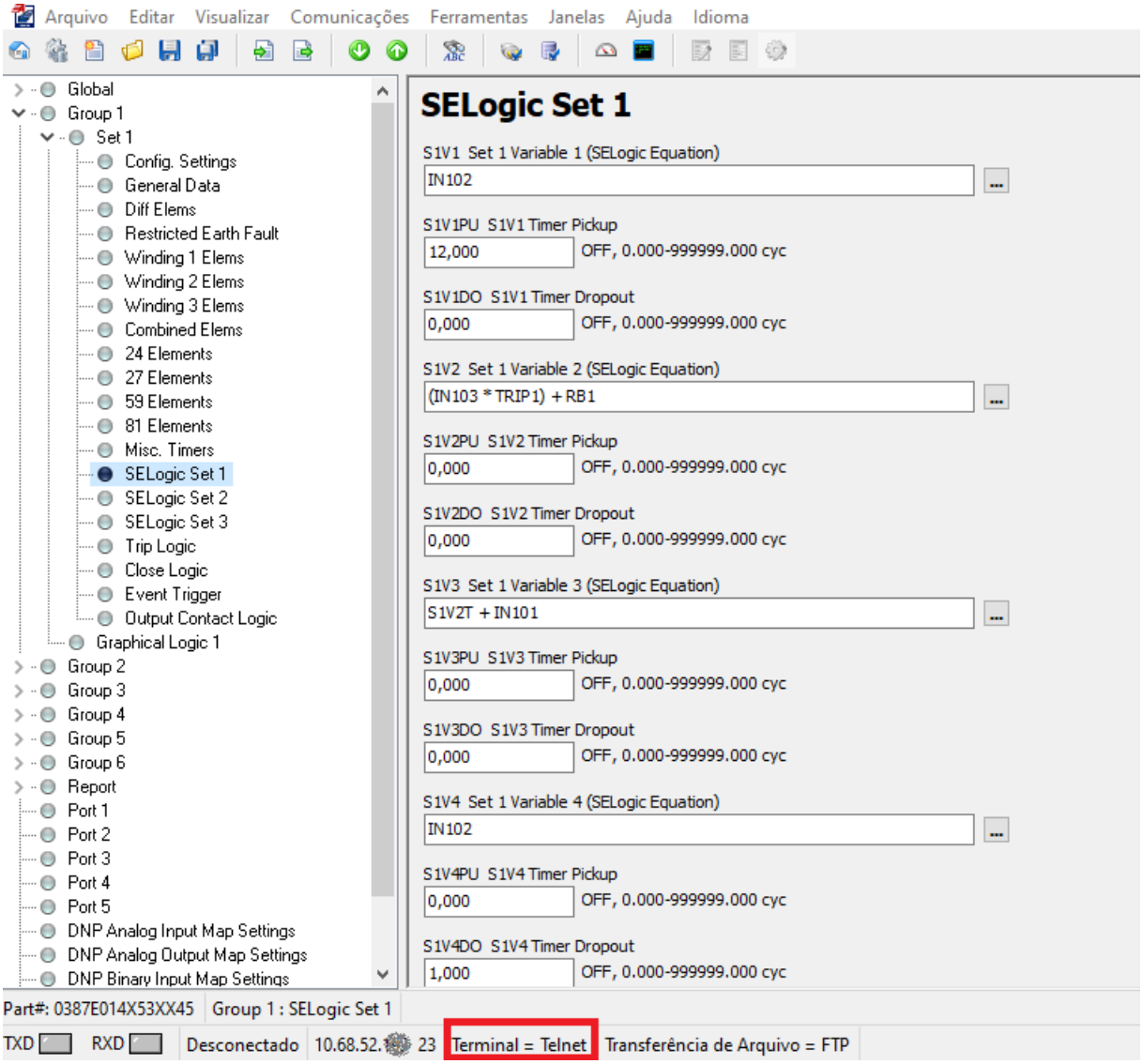


Figura 32: *Print Screen* do momento de êxito no acesso remoto ao IED da SEL na arquitetura tradicional.

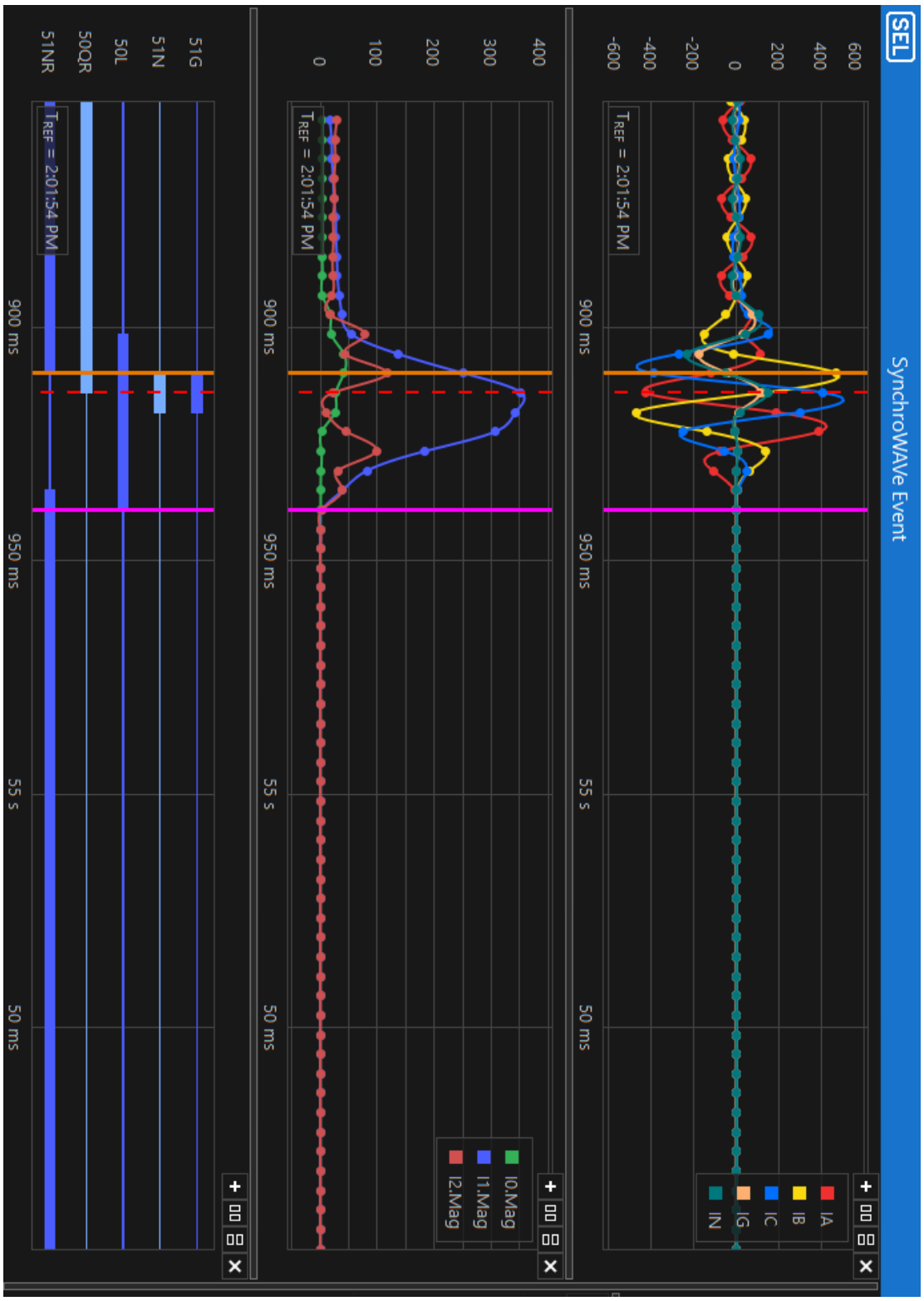


Figura 33: Oscilografia de uma dos transformadores presentes na arquitetura tradicional - momento do acontecimento exato do *blackout*.