UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

EDUARDO ALMEIDA CABRAL

MODELAGEM E AVALIAÇÃO DE SUBESTAÇÃO DIGITAL CONFORME PADRÃO IEC 61850: ABORDAGEM INTEGRADA À SEGURANÇA E RECURSOS DA INDÚSTRIA 4.0 UTILIZANDO MÉTODO STPA

FORTALEZA
2024

EDUARDO ALMEIDA CABRAL

MODELAGEM E AVALIAÇÃO DE SUBESTAÇÃO DIGITAL CONFORME PADRÃO IEC 61850: ABORDAGEM INTEGRADA À SEGURANÇA E RECURSOS DA INDÚSTRIA 4.0 UTILIZANDO MÉTODO STPA

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Engenharia Elétrica. Área de concentração: Sistemas de Energia Elétrica.

Orientador: Profa. Ph.D. Ruth Pastôra Saraiva Leão.

Coorientador: Prof. Dr. Raimundo Furtado Sampaio.

FORTALEZA

2024

EDUARDO ALMEIDA CABRAL

MODELAGEM E AVALIAÇÃO DE SUBESTAÇÃO DIGITAL CONFORME PADRÃO IEC 61850: ABORDAGEM INTEGRADA À SEGURANÇA E RECURSOS DA INDÚSTRIA 4.0 UTILIZANDO MÉTODO STPA

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Engenharia Elétrica. Área de concentração: Sistemas de Energia Elétrica.

Aprovada em: 29/05/2024.

BANCA EXAMINADORA

_____
Profa. Ph.D. Ruth Pastôra Saraiva Leão. (Orientadora)
Universidade Federal do Ceará (UFC)

_____
Prof. Dr. Raimundo Furtado Sampaio (Coorientador)
Universidade Federal do Ceará (UFC)

_____
Prof. Dr. Lucas Silveira Melo
Universidade Federal do Ceará (UFC)

_____
Prof. Dr. Raquel Cristina Filiagi Gregory
Universidade Federal do Ceará (UFC)

A Deus.

Aos meus pais, Alexandre e Eliane.

À minha esposa, Bruna Cabral.

AGRADECIMENTOS

Deixo aqui minha gratidão a Deus, cujo auxílio foi fundamental em minha jornada. Reconheço que sem Ele não teria alcançado este ponto. Agradeço também à Nossa Senhora, a quem recorri em minhas preces e confiei meus passos.

Aos meus pais, Alexandre e Eliane, cujo esforço incansável foi inestimável. Suas noites em claro, sacrifícios e apoio emocional foram essenciais para minha trajetória. Seu apoio e respeito foram a base que me permitiu seguir o caminho que escolhi.

À minha esposa, Bruna Cabral, por todo o apoio e amor. Reconheço que tudo o que construímos é mérito nosso, pois o fizemos juntos.

Aos meus avós, Alvino e Fátima, expresso minha profunda gratidão por acreditarem e investirem em mim. A atenção que dispensaram para garantir minhas condições de estudo não será esquecida.

Aos amigos e profissionais que compartilharam suas experiências e contribuíram para o meu crescimento profissional. Em especial, Bruno Valdivino e Matheus de Souza, com quem compartilhei os desafios do mestrado.

Aos professores do Departamento de Engenharia Elétrica, em especial à Prof. Ph.D. Ruth Pastôra Saraiva Leão e ao Prof. Dr. Raimundo Furtado Sampaio, pela excelente orientação e colaboração para construção deste trabalho. Ao Prof. Dr. Lucas Silveira Melo e à Prof. Dr. Raquel Cristina Filiagi Gregory que contribuíram na otimização deste trabalho.

“Recomenda ao Senhor tuas obras, e teus projetos se realizarão.” (Bíblia Sagrada, Provérbios 16, versículo 3).

RESUMO

A evolução tecnológica e a crescente interação entre humanos e máquinas autônomas têm sido um dos principais motores dos grandes e complexos sistemas. Essa transformação é significativa nas subestações elétricas, impulsionada pela digitalização conforme estabelecido na norma IEC 61850. Subestações são instalações elétricas de alta potência que conectam redes de diferentes níveis de tensão e sua digitalização está no centro da transformação exitosa do sistema elétrico. Nesse contexto, essa Dissertação tem como objetivo apresentar uma metodologia abrangente utilizada na avaliação de segurança de sistemas complexos aplicada para modelagem e avaliação qualitativa de subestação digital padrão IEC 61850. Além disso, o trabalho visa construir uma proposta de subestação digital industrial que incorpora recursos operacionais alinhados com os conceitos da Indústria 4.0, tais como interoperabilidade e modularidade, e uma filosofia de proteção baseada em seletividade lógica padrão IEC 61850. Adicionalmente, é implementado em bancada de teste a filosofia de proteção empregada na subestação industrial, tanto no cenário proposto (digital) quanto no atual (parcialmente digital), comparando o desempenho das filosofias de proteção, e validando em laboratório a interoperabilidade e modularidade no âmbito digital. Para tanto, este trabalho realiza a modelagem de um projeto de subestação digital industrial por meio do método STPA (*System-Theoretic Process Analysis*), a fim de avaliar de forma qualitativa a segurança e confiabilidade das camadas de controle e suas interações. Ações de controle sob responsabilidade do Sistema de Automação da Subestação, com ênfase na conexão de *bay*, são avaliadas com base no método STPA. Testes de bancada são conduzidos para validar os benefícios da filosofia de proteção proposta em comparação com a atual automação da subestação industrial. Os testes são realizados com base nas ações de controle e restrição do sistema obtidas na modelagem STPA. Conclui-se que o STPA é uma importante ferramenta para modelar as interações entre as camadas de controle de subestações digitais, e que a implementação do modelo proposto aumenta a segurança e autonomia para a subestação, em consonância com os pilares da Indústria 4.0.

Palavras-chave: STPA; indústria 4.0; subestação; IEC 61850; sistemas complexos.

ABSTRACT

The technological evolution and the increasing interaction between humans and autonomous machines have been the primary drivers of large and complex systems. This transformation is particularly significant in electrical substations, driven by digitalization as established by the IEC 61850 standard. Within this context, this dissertation aims to present a comprehensive methodology for evaluating the safety of complex systems for modeling and qualitative assessment of IEC 61850 standard digital substations. The work seeks to develop a proposal for an industrial digital substation, embedding operational features aligned with Industry 4.0 concepts, such as interoperability and modularity, into the control structure of the digital substation. Additionally, this research proposes a protection philosophy based on IEC 61850 standard logical selectivity. Furthermore, the protection philosophy employed in the industrial substation is implemented in a test rig, comparing its performance in both digital and partially digital, and validating interoperability and modularity in a digital context in the laboratory. To achieve this goal this work models an industrial digital substation using the System-Theoretic Process Analysis (STPA) method, in order to qualitatively evaluate the safety and reliability of the control layers and their interactions. The digitalization of the substation fosters interoperability among Intelligent Electronic Devices (IEDs) and provides modularity to the electrical system in contingency scenarios. Control actions under the responsibility of the Substation Automation System, with an emphasis on bay connections, are evaluated according to the STPA method. Bench tests are conducted to validate the benefits of the proposed protection philosophy compared to the current automation in the industrial substation. These tests are based on the control actions and system constraints provided by the STPA modeling. The results show that STPA is an important tool for modeling the interactions among the control layers of digital substations and that the implementation of the proposed model enhances the safety and autonomy of the substation, according to Industry 4.0.

Keywords: STPA; industry 4.0; substation; IEC 61850; complex systems.

LISTA DE FIGURAS

Figura 1 – Caminho metodológico dos trabalhos conduzidos nesta Dissertação. 17
Figura 2 – Arquitetura digital da subestação industrial simulada em laboratório. 20
Figura 3 – Taxonomia para níveis de automação em cada revolução industrial. 26
Figura 4 – Níveis hierárquicos baseado no padrão IEC 61850. 32
Figura 5 – Tempo de transmissão da mensagem GOOSE. 33
Figura 6 – Modelo da informação baseado na IEC 61850. 34
Figura 7 – Identificação de dados conforme IEC 61850. 35
Figura 8 – Segurança e confiabilidade: conceitos complementares. 36
Figura 9 – Modelo de sistema ciber-físico. 38
Figura 10 – Métodos para abordagem integrada. 40
Figura 11 – Modos de falha na rede de comunicação. 41
Figura 12 – Mapa conceitual para STPA. 51
Figura 13 – Fase do método STPA. 51
Figura 14 – Relação entre sistema, subsistemas, fronteira e ambiente. 53
Figura 15 – Taxonomia para perigo a nível de sistema. 54
Figura 16 – Taxonomia geral para restrições a nível de sistema. 54
Figura 17 – Alternativa de taxonomia para restrições a nível de sistema que mitigam perdas. 54
Figura 18 – Fluxograma para definição do propósito da análise STPA. 55
Figura 19 – Estrutura hierárquica de controle genérica para STPA. 56
Figura 20 – Fluxograma para construção de uma estrutura de controle STPA. 57
Figura 21 – Taxonomia para ações de controle inseguras no STPA. 58
Figura 22 – Fluxograma para definição de ações de controle inseguras no STPA. 59
Figura 23 – Ambiente de modelagem do software Capella Eclipse. 62
Figura 24 – Tabela de perdas no software Capella. 62
Figura 25 – Inserção de um perigo a nível de sistema no software Capella. 63
Figura 26 – Caminho para gerar um diagrama de controle detalhado no software Capella. 63
Figura 27 – Diagrama de controle detalhado para operadores locais no software Capella. 64
Figura 28 – Diagrama unifilar simplificado da subestação industrial. 65
Figura 29 – Coordenograma dos relés conforme dados da OAP. 67
Figura 30 – Seletividade lógica com comunicação baseada na IEC 61.850. 70
Figura 31 – Lógica do esquema de seletividade com uso de mensagem GOOSE. 71
Figura 32 – Definição das perdas e perigos a nível de sistema. 72

Figura 33 – Definição das restrições a nível de sistema. 72
Figura 34 – Amplitude da aplicação do método STPA adotada no estudo de caso. 73
Figura 35 – Responsabilidades do barramento de bay no software Capella. 74
Figura 36 – Entradas e saídas do barramento de bay no software Capella. 74
Figura 37 – Responsabilidades do IED do transformador no software Capella. 75
Figura 38 – Entradas e saídas do IED do transformador no software Capella. 76
Figura 39 – Responsabilidades do IED do alimentador no software Capella. 76
Figura 40 – Entradas e saídas do IED do alimentador no software Capella. 77
Figura 41 – Investigação das causas dos cenários de perda. 78
Figura 42 – Diagrama geral da estrutura de controle da subestação. 79
Figura 43 – Diagrama detalhado de controle do barramento *interbay*. 81
Figura 44 – Diagrama detalhado de controle do IED do transformador. 82
Figura 45 – Diagrama detalhado de controle do IED do alimentador. 82
Figura 46 – Plataforma para testes em bancada. 84
Figura 47 – Layout das conexões elétricas da plataforma de teste para simulação de sobrecarga e curto-circuito. 87
Figura 48 – Configuração IEC 61850 para RS4. 88
Figura 49 – Configuração IEC 61850 para RS5. 89
Figura 50 – Configuração IEC 61850 para RS2. 89
Figura 51 – Parametrização lógica dos relés. 90
Figura 52 – Layout das conexões elétricas da plataforma de teste para simulação de interoperabilidade e rejeição de cargas. 90
Figura 53 – Comparação de desempenho das filosofias de proteção para sobrecarga no alimentador A-1 de 650A sem falha no disjuntor D-4. 92
Figura 54 – Comparação de desempenho das filosofias de proteção para sobrecarga no alimentador A-1 de 650A com falha no disjuntor D-4. 92
Figura 55 – Comparação de desempenho das filosofias de proteção para curto-circuito no alimentador A-1 sem falha no disjuntor D-4. 93
Figura 56 – Comparação de desempenho das filosofias de proteção para curto-circuito no alimentador A-1 com falha no disjuntor D-4. 94
Figura 57 – Desempenho da filosofia de proteção proposta para curto-circuito no alimentador A-1 e falha na rede de comunicação. 95
Figura 58 – Desempenho da filosofia de proteção proposta para cenário de contingência. 95

LISTA DE QUADROS

Quadro 1 – Classificação de subestações por tecnologias adotadas..... 28

LISTA DE TABELAS

Tabela 1 – OAP para subestação industrial 66
Tabela 2 – Cenários de perda que motivaram testes laboratoriais. 83

LISTA DE ABREVIATURAS E SIGLAS

CAST	*Causal Analysis based on Systems Theory*
CDC	*Common Data Classes*
DA	*Data Atributes*
DO	*Data Objects*
DoS	*Denial of Service*
EPBS	*End-Product Breakdown Structure*
ESG	*Environmental, Social and Governance*
FC	*Functional Constraints*
FDI	*False Data Injection*
FMEA	*Failure Mode and Effect Analysis*
FRAM	*Functional Resonance Analysis Method*
FTA	*Fault Tree Analysis*
GOOSE	*Generic Object-Oriented Substation Event*
HAZOP	*Hazard and Operability Study*
HEART	*Human Error Assessment and Reduction Technique*
HRA	*Human Reliability Analysis*
HSR	*High-Availability Seamless Redundancy*
IDS	*Intruder Detection Systems*
IEC	*International Electrotechnical Commission*
IED	*Intelligent Electronic Device*
IHM	Interfaces Homem-Máquina
IoT	*Internet of Things*
IPS	*Intruder Protection System*
LD	*Logical Devices*
LN	*Logical Nodes*
MAC	*Media Access Control*
MBSE	*Model-Based Systems Engineering*
MITM	*Man-in-the-Middle*
MMS	*Manufacturing Message Specification*
MU	*Merging Unit*
NIC	*Network Interface Card*
OAP	Ordem de Ajuste das Proteções

OPNET	*Optimized Network Engineering Tool*
OSI	*Open System Interconnection*
PAC	Proteção, Automação e Controle
PD	*Physical Devices*
PRP	*Parallel Redundancy Protocol*
PSA	*Probabilistic Safety Assessment*
R-GOOSE	*Routable Generic Object-Oriented Substation Event*
RSA	*Rivest-Shamir-Adleman*
R-SV	*Routable Sampled Values*
RTDS	*Real Time Digital Simulator*
SAS	Sistema de Automação da Subestação
SDN	*Software Defined Networking*
SHA	*Secure Hash Algorithm*
STAMP	*Systems-Theoretic Accident Model and Processes*
STPA	*System-Theoretic Process Analysis*
SV	*Sampled Values*
THERP	*Technique for Human Error Rate Prediction*
TLS	*Transport Layer Security*
UCA	*Unsafety Control Actions*
UCS	Unidade de Controle da Subestação
VPN	*Virtual Private Network*
CAST	*Causal Analysis based on Systems Theory*
CDC	*Common Data Classes*
DA	*Data Atributes*
DO	*Data Objects*

SUMÁRIO

1 INTRODUÇÃO 16
1.1 Motivação 17
1.2 Objetivos 18
1.2.1 Objetivo Geral 18
1.2.2 Objetivos Específicos 18
1.3 Metodologia 18
1.4 Estado da arte na confiabilidade e segurança de subestações 20
1.5 Contribuições 22
1.6 Estrutura do trabalho 23
2 CONFIABILIDADE E SEGURANÇA EM SUBESTAÇÕES NO CONTEXTO DA INDUSTRIA 4.0 24
2.1 Indústria 4.0: uma revisão 24
2.2 Automação de subestações: evolução e desafios futuros 28
2.3 Padrão IEC 61850 para digitalização de subestações 30
2.3.1 Comunicação em níveis hierárquicos 31
2.3.2 Modelo da informação 34
2.4 Confiabilidade e segurança: conceitos não intercambiáveis 35
2.5 Avaliação de segurança em subestações digitais 37
2.5.1 Confiabilidade em sistema ciber-físico de energia 37
2.5.2 Modos de falha em subestações digitais 40
2.5.2.1 Falha na rede de comunicação 41
2.5.2.2 Ataques cibernéticos 44
2.6 Determinação de risco em sistemas complexos 47
2.7 Considerações finais 48
3 FERRAMENTAS DE MODELAGEM 50
3.1 Método *System-Theoretic Process Analysis* (STPA) 50
3.1.1 Definição do propósito da análise 52
3.1.2 Modelagem da estrutura de controle 55
3.1.3 Identificação das ações de controle inseguras 57
3.1.4 Identificação dos cenários de perda 59
3.2 Software Capella para análise STPA 60
3.3 Considerações finais 64
4 PROPOSTA DE AVALIAÇÃO DE SEGURANÇA EM SUBESTAÇÃO DIGITAL UTILIZANDO STPA 65

4.1 Cenário atual da subestação 65
4.2 Proposta de seletividade lógica padrão IEC 61850 69
4.3 Uso de STPA em subestação digital 71
4.4 STPA aplicado à proposta de subestação industrial digital 78
4.5 Considerações finais 83
5 PROPOSTA DE DIGITALIZAÇÃO DE SUBESTAÇÃO INDUSTRIAL 84
5.1 Implementação da plataforma de teste 84
5.2 Configuração da plataforma de Proteção, Automação e Controle (PAC) 86
5.2.1 Cenários de sobrecarga e curto-circuito 86
5.2.2 Falha na rede de comunicação e corte de carga 87
5.3 Validação do modelo proposto na bancada de teste 90
5.4 Considerações finais 96
6 DISCUSSÃO 97
6.1 Aplicação do STPA em subestações digitais 97
6.2 Desempenho das proteções em subestações tradicional e digital 99
6.3 Adoção de recursos operacionais da Indústria 4.0 100
6.4 Considerações finais 101
7 CONCLUSÃO E TRABALHOS FUTUROS 102
7.1 Trabalhos futuros 103
REFERÊNCIAS 104

1 INTRODUÇÃO

A contribuição da indústria para a sociedade não se limita apenas ao valor econômico gerado, mas também abrange aspectos ambientais, sociais e de governança (ESG) (Wan *et al.*, 2023). Uma estratégia eficaz para ampliar a exposição das indústrias a esses critérios ESG envolve a integração de mecanismos da Indústria 4.0 em várias fases do processo produtivo, possibilitando a captura, processamento e gestão de informações em tempo real (Chen; Song; Gao, 2023). Esse cenário caracteriza-se pela combinação de técnicas avançadas de produção e tecnologias digitais, visando proporcionar às empresas dados confiáveis para embasar suas decisões. Ademais, tais soluções tecnológicas podem contribuir para atender de forma eficiente às demandas do ESG e reduzir perdas no âmbito industrial (Alkaraan *et al.*, 2022).

Em Leveson e Thomas (2018), os autores definem perda como um prejuízo a algo significativo para as partes interessadas no sistema. Isso pode abranger desde perda de vidas ou lesões humanas, perdas financeiras, danos materiais, degradação do meio ambiente, ou qualquer outro tipo de dano que seja considerado inaceitável pelas partes interessadas.

A digitalização industrial representa uma ferramenta fundamental para prolongar a vida útil dos ativos, reduzir perdas, aprimorar o atendimento ao cliente, encurtar prazos de entrega, elevar a satisfação dos colaboradores e mitigar os impactos ambientais das operações industriais (Moschko; Blažević, 2023).

Dado o significativo papel da energia elétrica como ativo essencial, a adoção da Indústria 4.0 revela-se crucial na implementação de redes inteligentes, sobretudo em subestações modernas (Lozano *et al.*, 2023). Com o advento das tecnologias de informação e comunicação, a Internet das Coisas (IoT) assume também um papel central na otimização da confiabilidade, disponibilidade e eficiência global dos sistemas de energia modernos (Kapil; Prasad, 2022).

A modernização estruturada das subestações é crucial para garantir o nível de segurança e confiabilidade exigido nas operações industriais. Neste contexto, o investimento na digitalização das subestações, em conformidade com a IEC 61850, tem sido amplamente reconhecido no âmbito industrial, pois esse padrão foi concebido para ser duradouro e compatível com diversos fabricantes, facilitando a integração dos sistemas.

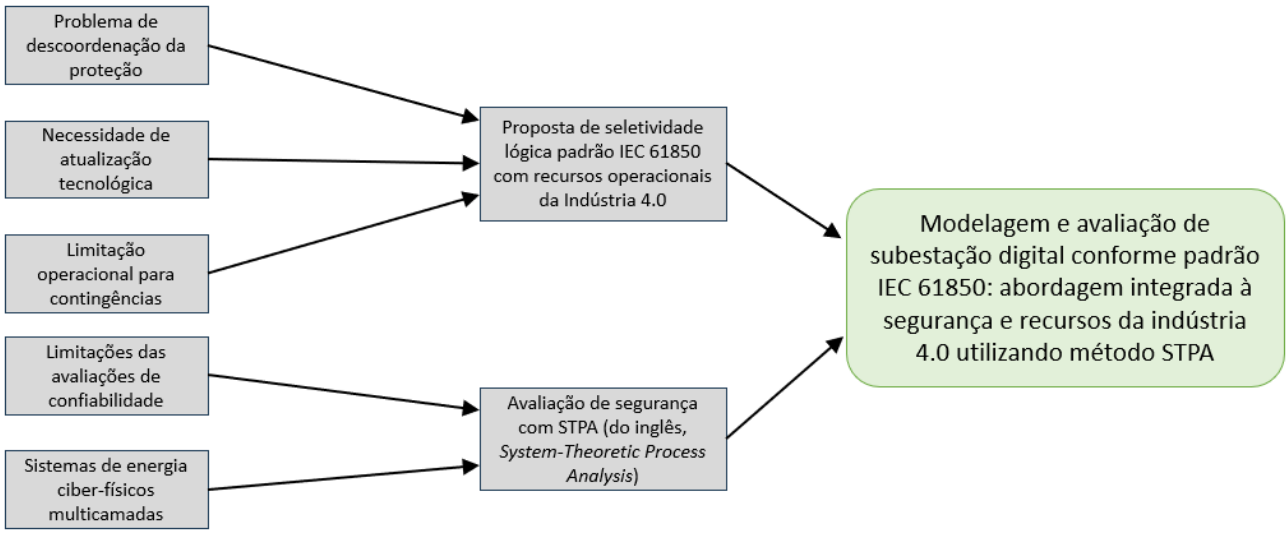
Contudo, a transição para uma configuração digital traz consigo desafios significativos, principalmente devido à complexidade das relações entre os controladores, o que pode comprometer a segurança e o desempenho da subestação.

1.1 Motivação

A subestação industrial avaliada neste estudo tem sido frequentemente afetada por interrupções na produção devido a falhas elétricas e à falta de coordenação dos dispositivos de proteção, ocasionando prejuízos financeiros significativos. Além disso, a falta de recursos operacionais da subestação dificulta o fornecimento parcial de energia à fábrica em cenários de contingência, acarretando parada total de produção. Nesse contexto, surge a demanda por uma atualização tecnológica para a adoção de relés digitais em conformidade com o padrão IEC 61850. Esses relés devem ser capazes de oferecer recursos avançados de seletividade lógica, bem como integrar conceitos da Indústria 4.0 à infraestrutura da subestação, visando mitigar as perdas operacionais.

A literatura reconhece que os conceitos de confiabilidade e segurança são complementares, e que os métodos tradicionais de avaliação de confiabilidade não abordam de forma abrangente os requisitos de segurança para sistemas ciber-físicos complexos. Além disso, observa-se uma lacuna de estudos que utilizam métodos abrangentes para avaliação da segurança em subestações digitais. Portanto, torna-se imperativo avaliar os riscos inerentes ao processo de digitalização da subestação, visando impor restrições funcionais e gerenciar os riscos na operação da subestação industrial. A Figura 1 sintetiza as motivações deste trabalho, destacando os desafios e as propostas de pesquisa que culminaram no título desta Dissertação.

Figura 1 – Caminho metodológico dos trabalhos conduzidos nesta Dissertação.



Fonte: Elaborado pelo autor.

1.2 Objetivos

1.2.1 Objetivo Geral

O objetivo principal é promover a digitalização padrão IEC 61850 de uma subestação industrial, incorporando recursos operacionais alinhados aos princípios da Indústria 4.0, e propor o método SPTA como uma ferramenta para modelagem e avaliação de segurança em subestações digitais.

1.2.2 Objetivos Específicos

- Construir proposta de subestação digital com método de análise de segurança aplicado a sistemas complexos;
- Incorporar interoperabilidade e modularidade, conforme princípios da Indústria 4.0, à estrutura de controle da subestação digital;
- Incorporar seletividade lógica padrão IEC 61850 ao processo de digitalização de uma subestação industrial parcialmente digital;
- Implementar em bancada de teste a filosofia de proteção empregada na subestação industrial tanto no cenário proposto quanto para o atual;
- Comparar desempenho das filosofias de proteção proposta e atualmente implementada;
- Validar em laboratório recursos operacionais da subestação alinhados com os conceitos da Indústria 4.0.

1.3 Metodologia

Com o avanço tecnológico, que possibilita a integração de diversas plataformas para controle de sistemas, a digitalização de informações e a virtualização de processos, aliados às interações entre humanos, máquinas e software, surgem sistemas complexos. As relações entre diferentes componentes e subsistemas aumenta a complexidade geral do sistema. Além disso, à medida que os sistemas se tornam mais automatizados e inteligentes, a colaboração e a coordenação entre humanos e máquinas se tornam essenciais para o funcionamento eficiente e seguro dos sistemas.

Esse processo também é observado nas subestações. Os sistemas elétricos estão

incorporando tecnologias avançadas, como a comunicação em tempo real, a análise de dados em nuvem e o controle remoto, sendo o padrão IEC 61850 crucial nessa evolução. As subestações digitais exigem a integração de uma variedade de dispositivos e sistemas, resultando em uma complexidade significativa em termos de operação, manutenção e segurança.

Portanto, compreender e gerenciar os sistemas é fundamental, tanto para garantir seu desempenho eficaz quanto para mitigar possíveis perdas em contextos adversos. A exploração dos recursos da digitalização dos sistemas, visando obter ganhos em segurança, é crucial nesse contexto. Para isso, é necessário aplicar uma metodologia adequada para avaliar os sistemas complexos, compreender seus recursos funcionais e estabelecer restrições de segurança.

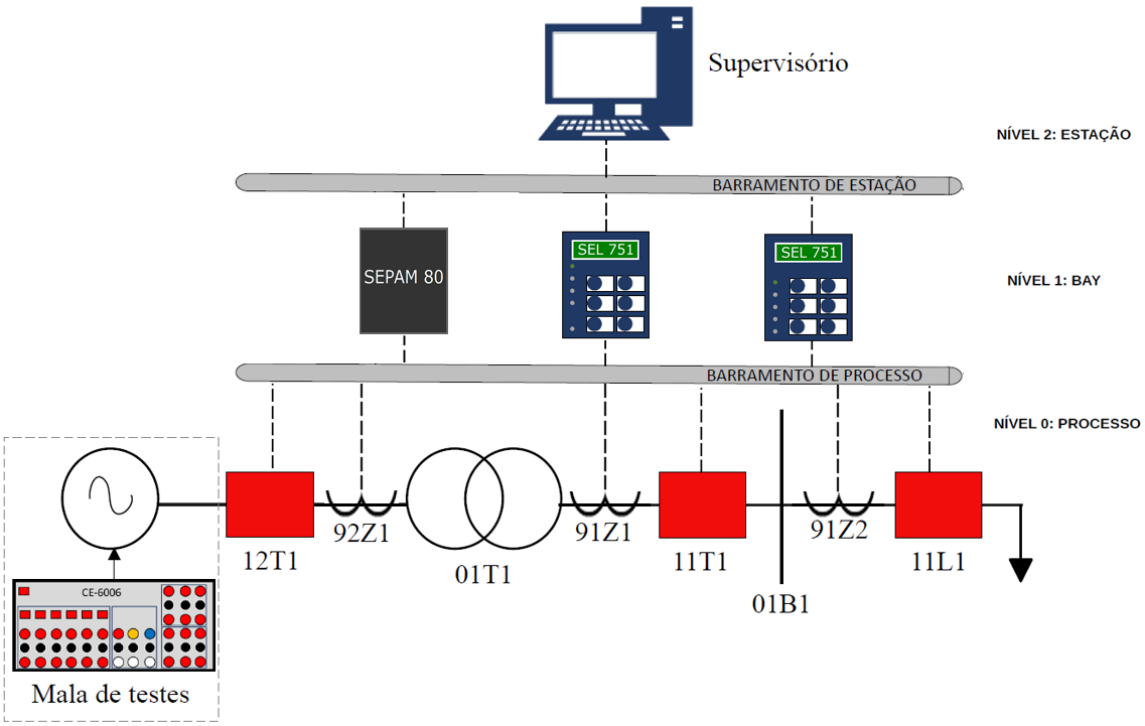
O STPA (do inglês, *System-Theoretic Process Analysis*) é uma técnica de análise de segurança que se fundamenta em um modelo expandido de causalidade de acidentes. Diferentemente das abordagens de confiabilidade tradicionais, o STPA reconhece que os acidentes podem ser originados não apenas por falhas nos componentes do sistema, mas também por interações inseguras entre esses componentes.

Essa técnica é utilizada nesse trabalho para propor a digitalização de uma subestação industrial conforme os padrões da IEC 61850, incorporando à subestação princípios da Indústria 4.0. Além disso, é realizada a avaliação das interações dos subsistemas que compõem a subestação digital, com ênfase no barramento *interbay*, e indicação de restrições de segurança para seus controladores. Nesse processo, recursos digitais para implementação de seletividade lógica são propostos, visando tornar a subestação mais segura, seletiva e coordenada.

Para validar a efetividade da nova filosofia de proteção e implementação de conceitos da Indústria 4.0, são conduzidos testes em laboratório para simular operação da subestação industrial em condições de falta e sobrecarga. A plataforma utilizada é composta por 2 notebooks, dois IEDs, um computador industrial, um *switch* gerenciável e uma mala de testes de relés.

A Figura 2 ilustra a disposição dos equipamentos de comunicação e as conexões simuladas do barramento de processo. A mala de teste é usada para inserir correntes elétricas no sistema para os experimentos e análises pertinentes. Como o objetivo da análise é comparar o desempenho das proteções no cenário digital proposto com o cenário atual de uma subestação em processo de digitalização, os testes foram conduzidos apenas nos níveis de *bay*.

Figura 2 – Arquitetura digital da subestação industrial simulada em laboratório.



Fonte: Adaptado de Freitas (2022).

A análise dos resultados experimentais envolveu a verificação dos tempos de atuação dos IEDs para o cenário atual das proteções e para o cenário digital, conforme fornecido pelo software da mala de testes, em cinco contextos de simulação: sobrecarga com e sem falha de disjuntor, curto-circuito com e sem falha de disjuntor, e curto-circuito com falha na rede de comunicação. O quinto experimento é exclusivo para o cenário de digitalização.

Adicionalmente, os conceitos de interoperabilidade e modularidade, inerentes à Indústria 4.0, foram avaliados por meio de um experimento de corte de carga, usando relés de fabricantes diferentes, por meio de mensagens GOOSE. Os dados temporais obtidos foram cruciais para a comparação tanto do desempenho quanto das capacidades operacionais de cada filosofia de proteção.

1.4 Estado da arte na confiabilidade e segurança de subestações

Em Lazarova-Molnar e Mohamed (2019), os autores enfatizam a importância central da avaliação de confiabilidade e segurança no avanço e aceitação das tecnologias da Indústria 4.0, ao mesmo tempo em que exploram novas direções e possibilidades para análises mais refinadas que essas inovações podem proporcionar. Destaca-se a capacidade que as novas

tecnologias de informação e comunicação possuem de transformar as abordagens tradicionais de confiabilidade e elevar a qualidade das avaliações oferecidas.

O trabalho de Syed e Hoidalen (2023) preenche uma lacuna na literatura ao revisar as abordagens usadas para analisar a confiabilidade de subestações digitais. Esse artigo serve como referência para pesquisadores e profissionais, pois sintetiza métodos e ferramentas de análise de confiabilidade em subestações digitais, oferecendo uma visão abrangente das metodologias e tecnologias aplicadas.

Análise *fuzzy* de árvore de falhas, análise de fatores humanos, estrutura de sistema de classificação e metodologia de decomposição funcional são usadas em Lin e Xu (2023) para derivar uma abordagem quantitativa para avaliar a confiabilidade de um Sistema de Automação de Subestação (SAS). Os autores concluem que variações na probabilidade de erro humano impactam diretamente o nível de confiabilidade do SAS.

Em Zhang et al. (2022), os autores tratam de uma inovação na análise de dados para a gestão do ciclo de vida das subestações, propondo um método composto de avaliação da confiabilidade operacional das subestações. Este método combina a distribuição Weibull de três parâmetros com a estimativa de máxima verossimilhança, capaz de utilizar dados amostrais pequenos e manter alta precisão nos resultados de avaliação.

De acordo com Gholami, Gholami e Mohammadtaheri (2023), os paradigmas atuais de operação e planejamento podem afetar a confiabilidade dos futuros sistemas de energia. Assim, o estudo representa os componentes físicos de um sistema de energia em termos de um modelo multietapa independente. Além disso, propõe um algoritmo para determinar os arranjos possíveis do sistema ciber-físico em vez de usar o método de Monte Carlo. O artigo mostra que as configurações de falha mais prováveis ocorrem quando os sistemas físicos falham, mas os sistemas de proteção operam com sucesso, enquanto as configurações mais severas resultam de falhas no barramento de processos do sistema de proteção.

O trabalho de Zhao (2023) trata da falta de avaliação e controle de riscos em tempo real acerca da integridade dos componentes das subestações. O autor propõe um método de avaliação de riscos em tempo real, utilizando um modelo de importância de equipamento e um modelo de estado operacional, para analisar e calcular a importância dos indicadores de risco das subestações. O método reflete o estado operacional atual, a probabilidade de acidentes e falhas, e suas consequências e impactos.

Por sua vez, Karantaev e Karpenko (2022) propõem o uso de métodos combinados para avaliar a confiabilidade do subsistema de proteção das subestações digitais, considerando a ampla integração das tecnologias da informação e comunicação no setor elétrico. É enfatizado

a importância de desenvolver estratégias robustas para mitigar os riscos representados por ataques cibernéticos em sistemas digitais.

Por sua vez, Smith et al. (2020) destaca a complexidade introduzida pela transição para a rede inteligente nos sistemas elétricos de potência, o que pode resultar em perdas relacionadas à segurança devido a interações imprevistas entre sistemas e ciberataques. Identificar essas perdas e suas causas raiz durante o projeto do sistema é crucial, embora não trivial, exigindo uma abordagem sistemática. O trabalho propõe a integração de duas abordagens para análise sistemática de perigos, STPA e a ERIGrid HTD, e aplica em um estudo de caso para controle de potência reativa para uma rede de distribuição de baixa tensão.

A utilização do STPA para a análise de segurança e confiabilidade em sistemas complexos em detrimento de abordagens tradicionais reflete a necessidade de uma visão mais abrangente e sistêmica dos riscos. Enquanto métodos tradicionais tendem a focar em falhas individuais de componentes, o STPA adota uma abordagem holística, considerando as interações entre os diferentes elementos do sistema e os contextos sociais e organizacionais que influenciam seu funcionamento (Leveson; Thomas, 2018).

1.5 Contribuições

Há disponível na literatura estudos que aplicam o STPA a sistemas complexos, como estruturas de controle de aeronaves e segurança da informação em redes de computadores. Da mesma forma, há trabalhos que discutem as evoluções tecnológicas ocorridas durante as revoluções industriais ou que abordam os desafios associados à digitalização das subestações elétricas conforme o padrão IEC 61850, os quais estão prontamente disponíveis na esfera acadêmica. Contudo, até o momento, não foi identificada na literatura aplicação do método STPA para a modelagem de subestações digitais em conformidade com o padrão IEC 61850, considerando a adoção de conceitos tecnológicos da Indústria 4.0.

A literatura reconhece as subestações digitais como sistemas complexos e propõe a avaliação da segurança desses sistemas por meio da subdivisão em camadas de controle utilizando diversas ferramentas e métodos tradicionais. Este estudo apresenta uma nova ferramenta que facilita a aplicação do STPA às subestações digitais, permitindo a posterior avaliação da segurança do sistema e das interações entre os seus componentes.

A principal contribuição deste trabalho é a realização de uma avaliação abrangente da segurança de uma subestação industrial digitalizada, utilizando uma ferramenta unificada.

Esta avaliação considera a transição do sistema de proteção convencional para um quadro digital conforme o padrão IEC 61850, com a capacidade de incorporar ao Sistema de Automação e Supervisão (SAS) os princípios da Indústria 4.0. Além disso, é demonstrado como a IEC 61850 pode contribuir para o ganho de segurança em subestações digitais.

1.6 Estrutura do trabalho

Esta dissertação está dividida em sete capítulos. No Capítulo 1, o trabalho é contextualizado com a apresentação de objetivos, metodologia, revisão bibliográfica e contribuição.

O Capítulo 2 apresenta a evolução tecnológica promovida pelas revoluções industriais e o processo de digitalização das subestações com base no padrão IEC 61850, bem como os desafios para determinar risco em sistemas complexos, tais como subestações digitais.

O Capítulo 3 descreve as ferramentas usadas avaliação de segurança da proposta de digitalização de uma subestação industrial do ramo têxtil.

O Capítulo 4 apresenta a construção e aplicação de um modelo STPA para avaliação de segurança de uma subestação digital, evidenciando os requisitos para segurança operacional.

O Capítulo 5 mostra os equipamentos, softwares e o processos de configuração necessários para simular e validar o modelo proposto na bancada de testes. Além disso, são apresentados os resultados obtidos nos experimentos laboratoriais que avaliam o desempenho das proteções da subestação nos contextos convencional e digital.

O Capítulo 6 discute o desempenho operacional do cenário atual das proteções da subestação e do cenário digital proposto, objetivando comprovar tanto a redução do tempo para eliminação de falhas no sistema elétrico quanto a eficácia do método STPA para modelar subestações digitais. Além disso, são avaliados os ganhos operacionais resultantes da adoção dos princípios da Indústria 4.0 em uma subestação industrial.

Ademais, o Capítulo 7 finaliza o trabalho com as conclusões obtidas e os trabalhos futuros.

2 CONFIABILIDADE E SEGURANÇA EM SUBESTAÇÕES NO CONTEXTO DA INDUSTRIA 4.0

A evolução da Indústria 4.0 desempenha um papel crucial na transformação das subestações elétricas, impulsionando a automação e digitalização desses sistemas por meio do padrão IEC 61850. Este padrão estabelece diretrizes para a digitalização das subestações, permitindo a integração de equipamentos de diferentes fabricantes e facilitando a supervisão, controle e automação dos processos elétricos. Por outro lado, a digitalização da subestação traz desafios significativos em termos de segurança cibernética e avaliação de riscos operacionais, uma vez que transforma a subestação em um sistema ciber-físico complexo.

Nesse contexto, as três primeiras seções desse capítulo suportam a proposta de seletividade lógica padrão IEC 61850, com adesão recursos da Indústria 4.0, como alternativa às problemáticas apresentadas na Figura 1. Inicialmente, são apresentados os avanços tecnológicos tanto na indústria, por meio das quatro revoluções industriais, quanto nas subestações. Na sequência, destaca-se a importância da IEC 61850 no processo de digitalização das subestações e seus principais requisitos técnicos utilizados na proposta de digitalização da subestação industrial.

Na sequência, é feito uma discussão sobre os desafios da avaliação de segurança em sistemas complexos, a fim de subsidiar a escolha do método para avaliação de segurança da subestação industrial no arcabouço digital.

2.1 Indústria 4.0: uma revisão

A história das revoluções industriais é marcada por transformações profundas na maneira de produzir bens e serviços, moldando a sociedade, a economia e a tecnologia ao longo dos séculos. A primeira revolução industrial, que teve início no final do século XVIII, foi caracterizada pela mecanização dos processos produtivos, impulsionada pelo surgimento de máquinas a vapor e a invenção do tear mecânico. Esse período viu o surgimento das fábricas e o deslocamento massivo da população rural para as cidades em busca de trabalho, criando desafios como condições precárias de trabalho e desigualdades sociais (Groumpos, 2021).

A segunda revolução industrial ficou marcada como revolução tecnológica. Ela ocorreu no final do século XIX, trouxe avanços tecnológicos significativos, incluindo a produção em linhas de montagem, motores à gasolina e telefones. A eletrificação impulsionou a industrialização e urbanização. A utilização de linhas de montagem permitiu uma produção

mais eficiente e com menor custo. A urbanização acelerada e a produção em massa geraram desafios ambientais complexos (Groumpos, 2021).

A terceira revolução industrial, ocorrida no século XX, é reconhecida como revolução da automação. Dentre as tecnologias introduzidas nesse período, destacam-se a utilização de computadores e da internet no processo fabril. Tais tecnologias viabilizaram a globalização da produção. Por outro lado, a mão de obra humana foi substituída em massa por máquinas autônomas durante esse período (Groumpos, 2021).

Finalmente, a quarta revolução industrial começou no início do século XXI e é identificada como revolução digital. Esse período é caracterizado pela integração de tecnologias digitais como a Internet das Coisas, inteligência artificial e big data. São estabelecidos sistemas de produção ciber-físicos por meio da interconexão de sistemas virtuais, máquinas produtivas e pessoas. No entanto, essa revolução apresenta desafios significativos, incluindo a rápida mudança tecnológica e a necessidade de requalificação profissional para acompanhar as demandas do mercado de trabalho em constante evolução (Groumpos, 2021).

Para Kopeinig, Woschank e Olipp, (2024), tecnologias da Indústria 4.0, como Análise de Big Data, Internet das Coisas e Inteligência Artificial, podem apoiar a transição geral para um ambiente mais sustentável e ajudar a reduzir o uso de matérias-primas, produção de resíduos e consumo de combustível. No entanto, a literatura indica a necessidade de mais pesquisas para uma compreensão completa do impacto da Indústria 4.0 na sustentabilidade.

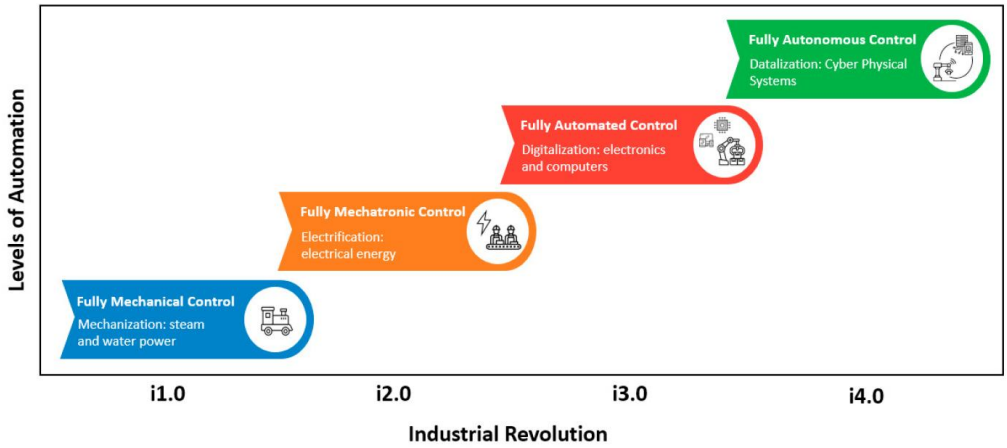
A Indústria 5.0 baseia-se nos avanços tecnológicos da Indústria 4.0, tais como Internet das Coisas (IoT), Inteligência Artificial (IA), Big Data, computação em nuvem, robótica avançada e sistemas ciberfísicos. A Indústria 5.0 expande essas inovações com uma abordagem voltada para a interação humano-máquina, visando a personalização dos processos produtivos e atender às necessidades sociais e ambientais (Bosovska *et al.*, 2022).Cada revolução industrial trouxe consigo avanços tecnológicos significativos, mas também desafios sociais, econômicos e ambientais que exigiram respostas políticas, regulamentações e adaptações por parte da sociedade. O progresso tecnológico é inevitável, mas é essencial garantir que seja acompanhado por políticas e práticas que promovam a inclusão, a equidade e a sustentabilidade.

O nível de automação qualifica a interação entre operadores humanos e computadores no controle de um sistema complexo (Barbieri; España; Sanchez-Londoño, 2022). A Figura 3 apresenta uma taxonomia capaz de ilustrar os diferentes níveis de controle introduzidos nas quatro primeiras revoluções industriais.

A Indústria 4.0 é caracterizada pela ampla adoção de tecnologias digitais,

expandindo a eletrônica própria da Indústria 3.0 para coletas de dados em tempo real, processamento em nuvem e *big data*, especialmente para sistemas elétricos e de energia. A digitalização emerge como um elemento intrínseco e catalisador do desenvolvimento do sistema produtivo global, incluindo a indústria de energia elétrica (Bosovska *et al.*, 2022).

Figura 3 – Taxonomia para níveis de automação em cada revolução industrial.



Fonte: Barbieri; España; Sanchez-Londoño (2022).

Há seis princípios que redefinem a operação dos sistemas industriais e fundamentam a Indústria 4.0, a saber: interoperabilidade, Internet das Coisas (IoT), virtualização, coleta de dados em tempo real, descentralização e modularização (Hall; Schumacher; Bildstein, 2022).

A interoperabilidade estabelece a capacidade de diferentes dispositivos e sistemas se comunicarem de forma eficiente, promovendo uma integração harmoniosa. A ascensão IoT traz consigo a conectividade entre objetos físicos e virtuais, permitindo a acessibilidade remota e a adaptação universal por meio do protocolo IP. A virtualização de processos físicos possibilita o monitoramento em tempo real de sistemas complexos, viabilizando uma compreensão aprofundada do ambiente produtivo (Hall; Schumacher; Bildstein, 2022).

A coleta de dados em tempo real e o processamento instantâneo dessas informações reduzem o tempo necessário para a tomada de decisão e fortalecem a agilidade operacional. A descentralização e a tomada de decisão autônoma conferem maior flexibilidade e independência aos sistemas, enquanto a modularização e flexibilização na produção redefinem as estruturas industriais, promovendo eficiência e adaptabilidade. Em conjunto, esses princípios delineiam uma era industrial impulsionada pela convergência entre o mundo físico e digital (Hall; Schumacher; Bildstein, 2022).

A digitalização industrial é uma ferramenta crucial para estender a durabilidade dos ativos, diminuir perdas financeiras, aprimorar o atendimento ao cliente, reduzir os prazos de entrega, elevar a satisfação dos colaboradores e reduzir os impactos ambientais das indústrias (Moschko; Blažević, 2023).

Por outro lado, os desafios associados à implementação da Indústria 4.0 são abrangentes e incluem fatores como: segurança cibernética, padronização dos protocolos de comunicação entre diferentes fabricantes, resistência à mudança de cultura organizacional, manutenção da qualidade de um volume excessivo de dados, desenvolvimento sustentável e falta de habilidades dos funcionários (Hagström; Bergsjö; Wahrén, 2023).

O trabalho de Alsaadi (2022) examina os desafios para a adoção de tecnologias da Indústria 4.0 no setor manufatureiro e apresenta um modelo estrutural para esses obstáculos. A falta de capacitação dos trabalhadores e infraestrutura tecnológica em fase inicial de aceitação e implementação são os principais desafios. O estudo oferece um modelo que permite a tomadores de decisão e profissionais abordar esses obstáculos de forma eficaz, facilitando a adoção dos princípios da Indústria 4.0 no setor manufatureiro.

Esses fatores destacam a complexidade para a ampla adoção dos princípios da Indústria 4.0, enfatizando a necessidade de abordar elementos técnicos, organizacionais e humanos para garantir uma digitalização bem-sucedida nos processos industriais.

A indústria 4.0 permeia toda a cadeia de valor da corporação (Nagy *et al.*, 2018). Considerando que a energia elétrica é um ativo importante, a Indústria 4.0 é crucial na implementação de redes inteligentes, especialmente quando se consideram subestações modernas (Lozano *et al.*, 2023). Nesse contexto, é oportuno estender o advento das tecnologias digitais e dos sistemas ciber-físicos às subestações a fim de aumentar a confiabilidade, segurança e eficiência geral dos sistemas de energia sem perder de vista os desafios associados a adoção dos princípios da Indústria 4.0 (Kapil; Prasad, 2022).

Em Kapil e Prasad (2022), os autores revisam a disponibilidade da IoT em uma subestação do sistema de transmissão de energia, a fim de encontrar lacunas que precisam ser preenchidas durante a digitalização da subestação. São listados os principais componentes e sensores inteligentes necessários para proteger e monitorar os equipamentos da subestação em relação aos seus parâmetros e saúde operacional. É destacado a importância de software analítico que integre os dados e subsidie estratégias de gestão de ativos.

2.2 Automação de subestações: evolução e desafios futuros

A automação de subestações tem evoluído significativamente ao longo do tempo, passando de operações manuais para sistemas digitais avançados. Inicialmente, utilizavam-se relés eletromecânicos, que foram gradualmente substituídos por relés estáticos, sistemas baseados em RTU (do inglês, *Remote Terminal Units*) e, mais recentemente, por IEDs com capacidades avançadas de processamento (Sen; Bakka, 2021).

Em Santos et al. (2024), destaca-se que a transformação digital na indústria elétrica está impulsionando a pesquisa em subestações inteligentes. O autor demonstra o aumento das publicações sobre subestações digitais no período de 2005 a 2022 por meio de uma análise bibliométrica. Embora o autor tenha reunido trabalhos de 2023, estes foram excluídos pois o ano ainda não havia sido concluído na época do estudo. Além da análise bibliométrica, o autor propõe um modelo de quatro estágios para o nível de automação das subestações, indo de convencionais a inteligentes, com base nos trabalhos reunidos.

O modelo considera oito requisitos para classificar a subestação: protocolo de comunicação, hardware para dados, dispositivos para proteção, controle e automação, transformadores de instrumento, método de aquisição de dados, método de análise de dados, política de manutenção e competências técnicas da equipe operacional. O Quadro 1 sintetiza as tecnologias de cada requisito utilizadas em cada nível de automação da subestação de acordo com Santos et al. (2024).

Quadro 1 – Classificação de subestações por tecnologias adotadas.

REQUISITOS	CLASSIFICAÇÃO DE SUBESTAÇÃO POR TECNOLOGIAS ADOTADAS			
	Convencional	Estágio inicial de digitalização	Digital (Estado da arte)	Inteligente (Perspectiva futura)
Protocolo de comunicação	Não possui. Apenas sinais analógicos	Proprietário e/ou padrões antigos (DNP3.0, IEC 60870 e ModBus)	IEC 61850	IEC 61850
Hardware para dados de processo	Cabos de cobre	Cabos de cobre	Cabos de cobre e fibra óptica	Fibra óptica e tecnologias wireless
Dispositivos de proteção, controle e automação	Relés eletromecânicos e de estado sólido	Relés numéricos e IEDs de 1ª geração	Dispositivos eletrônicos inteligentes	Proteção centralizada e controle
Transformadores de instrumentos	Convencional	Convencional	Convencional, ocasionalmente com Mergit Unit	Totalmente digital (eletrônico)
Métodos de aquisição de dados	Manual. Assistido por dispositivos não integrados	Manual e digital. Uso de SCADA	Digital com alguma integração	Totalmente integrado, digital e autônomos
Análise de dados	Apenas em caso de falha	Não funciona em tempo real. Sistema SCADA integrado	Software em tempo real	Análise de Big Data e algorítimos de inteligência artificial
Política de manutenção	Preventiva e corretiva	Preventiva e corretiva	Preventiva, corretiva e preditiva (baseada em condições)	Preventiva, corretiva e preditiva (baseada em condições)
Competências técnicas da equipe operacional	Eletromecânica	Eletromecânica + Eletrônica	Eletrônica + Redes + Elétrica	Redes + Dados + Eletrônica + Elétrica

Fonte: Adaptado de Santos et al. (2024).

Uma subestação convencional opera com dados analógicos e representa o paradigma arquitetônico anterior aos anos 1970. Já as subestações digitais em estágio inicial apresentam dados analógicos de nível de processo, com protocolos proprietários, sendo comuns nas décadas de 1980 e 1990. As subestações digitais atuais incorporam um barramento de processo digital, comunicações baseadas em IEC 61850 e transformadores de instrumentos convencionais. Ocasionalmente, essa classe de subestação possui seus sinais analógicos digitalizados usando *Merging Unit*, que então se conectam ao barramento de processo da subestação. As subestações inteligentes representam o futuro, com transformadores de instrumentos de baixa potência e funções avançadas, ainda em fase de desenvolvimento tecnológico (Santos *et al.*, 2024).

A evolução dos dispositivos de proteção, controle e automação é crucial para o ganho de recursos operacionais e de segurança da subestação. Enquanto subestações convencionais utilizam relés eletromecânicos independentes para proteção, subestações digitais empregam IEDs, que integram várias funções de automação e supervisão. Já em subestações inteligentes, há uma tendência de centralizar funções de automação em um sistema de proteção e controle. Além disso, a virtualização e as tecnologias em nuvem estão sendo amplamente adotadas para melhorar os sistemas de proteção, permitindo uma maior flexibilidade e integração entre os dispositivos (Santos *et al.*, 2024).

Os protocolos de comunicação em sistemas de automação de subestações também passaram por evoluções significativas ao longo do tempo. Inicialmente, as subestações convencionais operavam com sinais analógicos, sem troca de dados digitalizados. Com o avanço da automação, as primeiras subestações digitais adotaram protocolos específicos do fornecedor e proprietários. Posteriormente, surgiram protocolos padronizados, como DNP3.0, IEC 60870 e ModBus, visando melhorar a troca de dados e o desempenho. Contudo, esses protocolos apresentam problemas, tais como: incompatibilidade com outros dispositivos, restrição do número de dispositivos conectados em um link de dados, falta de padrão para definir estrutura de dados, baixa taxa de transmissão de dados, falta de recursos de criptografia e segurança. O IEC 61850 é capaz de substituir os padrões legados e solucionar esses problemas para aplicações atuais e futuras em subestações (Kumar *et al.*, 2023).

O meio físico para o fluxo de dados conforme protocolos supracitados evoluiu de fios de cobre para conexões de fibra óptica, formando o barramento de processo. Embora a fibra óptica tenha sido relatada desde os anos 1980, sua adoção ampla ocorreu nos anos 2000. Subestações atuais combinam fios de cobre e fibra óptica para digitalizar sinais analógicos. A transmissão sem fio, como o 5G, está em pesquisa, mas sua adoção em dados críticos de

processo ainda é limitada (Santos *et al.*, 2024; Sen; Bakka, 2021).

A aquisição de dados em subestações convencionais é predominantemente manual, envolvendo anotações e preenchimento de formulários, enquanto dispositivos digitais permitem a aquisição contínua de dados. A análise tradicionalmente era realizada apenas em caso de falhas, exigindo esforço significativo. As subestações digitais apresentam sistemas SCADA para adquirir e exibir dados. Embora o monitoramento contínuo de condições em tempo real seja implementado, há espaço para melhorias na integração de dados e processamento em tempo real em subestações inteligentes. A análise de *big data* e aplicativos de inteligência artificial estão em destaque para análise de dados em subestações (Santos *et al.*, 2024).

As subestações convencionais e digitais em estágio inicial empregam manutenção preventiva e corretiva. No entanto, a manutenção baseada em condições, que prevê falhas por meio de dados auxiliares, é uma área de pesquisa desde os anos 1990, oferecendo potenciais benefícios de redução de custos e aumento da vida útil dos equipamentos. Nas subestações inteligentes, a disponibilidade avançada de dados permite uma integração mais eficaz da manutenção preditiva ou baseada em condições. As mudanças nas competências necessárias para operar e manter as subestações de energia também são destacadas, com a necessidade crescente de habilidades relacionadas a redes de computadores e análise de dados, além das habilidades tradicionais (Santos *et al.*, 2024).

A proposta de Santos et al. (2024) pode aprimorar o planejamento de investimentos e avaliação de projetos de subestações, tanto atuais quanto futuros, além de contribuir para a padronização das terminologias e definições utilizadas no campo. No entanto, é importante observar que as subestações raramente se encaixam perfeitamente em uma única categoria, pois frequentemente apresentam uma variedade de equipamentos de diferentes épocas e atualizações ao longo do tempo.

Os desafios em subestações cada vez mais virtualizadas incluem preocupações com segurança cibernética, desenvolvimento de transformadores de instrumentos de baixa potência, sincronização de tempo, *design* de redes digitais, análise de custo/benefício, análise de *big data* e políticas de manutenção preditiva. Além disso, os aspectos organizacionais, como competências necessárias e impactos regulatórios, são temas importantes a serem explorados.

2.3 Padrão IEC 61850 para digitalização de subestações

Em uma subestação clássica, os sinais elétricos são transmitidos por meio de fios de cobre do dispositivo de campo até a sala de controle, resultando em falhas constantes,

manutenção elevada e custos operacionais (Lozano *et al.*, 2023).

A revolução digital tem influenciado a operação das subestações de energia. O padrão IEC 61850 possibilita a substituição das conexões de cobre entre as salas de controle das subestações e o equipamento do pátio por redes digitais Ethernet (Kaur *et al.*, 2022).

A IEC 61850 fornece um padrão global para comunicação entre dispositivos do sistema de energia por meio de um conjunto de protocolos com *links* de comunicação personalizados, utilizados para automação, proteção e controle de subestações (Kaur *et al.*, 2022).

As subestações desempenham papéis críticos dentro do sistema de energia, portanto, devem ser configuradas em redes confiáveis e de baixa latência a fim de garantir segurança operacional e proteções assertivas. Tais exigências não são atendidas por padrões de comunicação anteriores, a exemplo de ModBus, DNP3 e IEC 60870. A IEC 61850 oferece protocolos e modelo para resolver esse desafio, além de proporcionar a interoperabilidade de dispositivos de diferentes fabricantes (Lozano *et al.*, 2023).

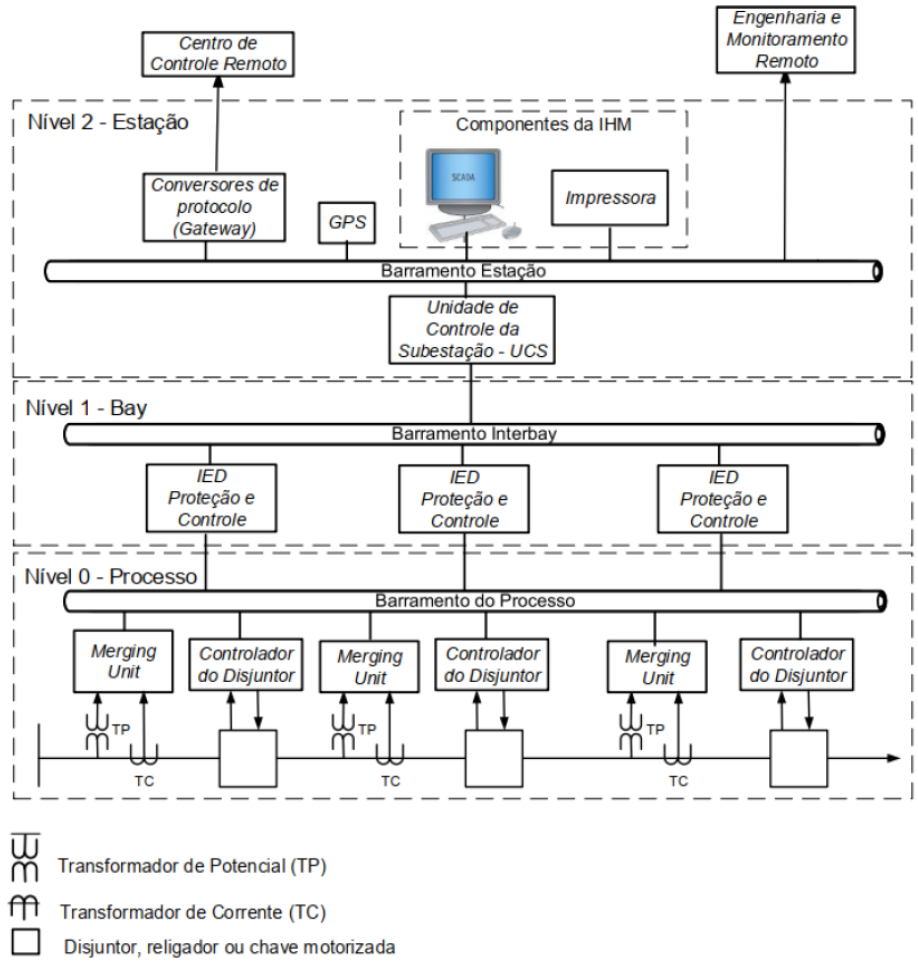
2.3.1 Comunicação em níveis hierárquicos

A IEC 61850 aloca as funcionalidades do sistema de automação da subestação em três níveis hierárquicos, a saber: Processo, Vão (*Bay*) e Estação, conforme ilustrado na Figura 4. Há comunicação entre os dispositivos do mesmo nível funcional e entre diferentes níveis hierárquicos, conforme protocolos específicos (Lozano *et al.*, 2023).

O nível de processo interage diretamente com os equipamentos que compõem o sistema elétrico, como sensores de corrente e de tensão, disjuntores e *merging unit* (MU). No nível *bay*, estão os Dispositivos Eletrônicos Inteligentes (IEDs), responsáveis pela tomada de decisão de controle e proteção de cada *bay* da subestação, de acordo com os dados recebidos do nível de processo. Já no nível estação, está a Unidade de Controle da Subestação (UCS) responsável pela supervisão e operação do sistema. Ela permite a operação remota, configuração do SCADA e Interfaces Homem-Máquina (IHMs) (Lozano *et al.*, 2023).

A comunicação entre os equipamentos da subestação ocorre por meio de três protocolos de rede distintos, que atendem a diferentes requisitos. Do nível de processo para o nível de *bay*, utiliza-se o protocolo *Sampled Values* (SV). Dentro do nível *bay*, a comunicação é estabelecida por meio do protocolo *Generic Object Oriented Substation Event* (GOOSE). Já as mensagens do nível *bay* para o nível de estação seguem o protocolo *Manufacturing Message Specification* (MMS) (Lozano *et al.*, 2023).

Figura 4 – Níveis hierárquicos baseado no padrão IEC 61850.



Fonte: Sampaio (2017).

A IEC 61850 subdivide o padrão da pilha *Open System Interconnection* (OSI) em dois grupos: Perfil-A e Perfil-T. O Perfil-A inclui os protocolos que podem operar nas três camadas superiores do modelo OSI: Aplicação, Apresentação e Sessão. Já o Perfil-T está restrito às quatro camadas inferiores: Transporte, Rede, Enlace e Física (IEC 61850-8-1, 2004).

O protocolo SV é utilizado na digitalização de sinais analógicos por meio de amostragens em taxas predefinidas. Tais sinais são reconstruídos pelos equipamentos do nível de *bay*. O SV é baseado no modelo de comunicação editor-assinante e usa *multicast* para a transmissão de dados conforme Perfil-T. A IEC 61850 9-2 em sua edição *Ligth Edition* traz requisitos específicos de sincronização de tempo, taxa de amostragem e de *datasets* para um sistema com frequência de 60 Hz. É proposto uma taxa de 80 e 256 amostras por ciclo em sistemas de proteção e medição, respectivamente (Aftab *et al.*, 2020; Lozano *et al.*, 2023).

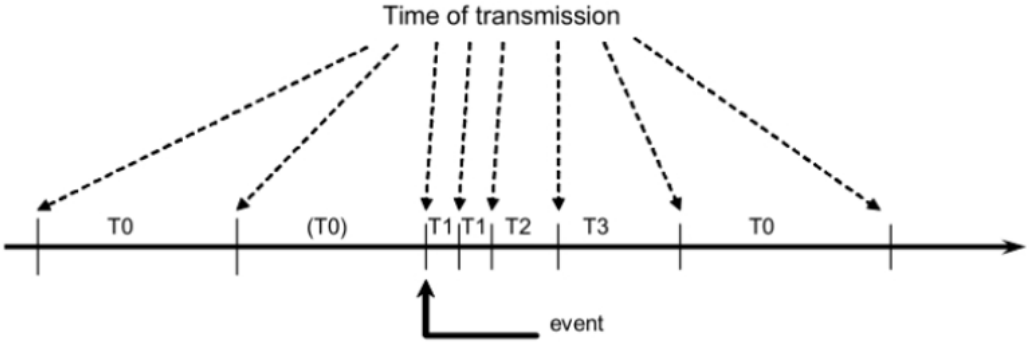
O GOOSE utiliza modelo editor-assinante na comunicação entre IEDs. Sua transmissão de dados é periódica e via pacotes de *multicast* enviados conforme Perfil-T de comunicação (Lozano *et al.*, 2023).

O tempo de envio da GOOSE é um parâmetro crucial, pois essa mensagem leva dados necessários à atuação das proteções da subestação. Nesse contexto, há dois parâmetros essenciais para esse protocolo: tempo máximo e tempo mínimo. O primeiro é o tempo para enviar mensagens quando não há eventos no sistema, enquanto o segundo define o tempo de transmissão quando um evento ocorre. Tipicamente, o tempo máximo é na ordem de um segundo e o tempo mínimo um ou cinco milissegundos. Caso algum assinante não receba uma mensagem no tempo máximo, ele deve indicar falha de comunicação (Lozano *et al.*, 2023).

Quando eventos que afetam os dados associados à mensagem GOOSE ocorrem, o intervalo entre duas mensagens sucessivas diminui e depois aumenta gradualmente até atingir o tempo máximo novamente (Lozano *et al.*, 2023).

A Figura 5 mostra o envio das mensagens GOOSE durante a operação normal e em resposta a eventos.

Figura 5 – Tempo de transmissão da mensagem GOOSE.



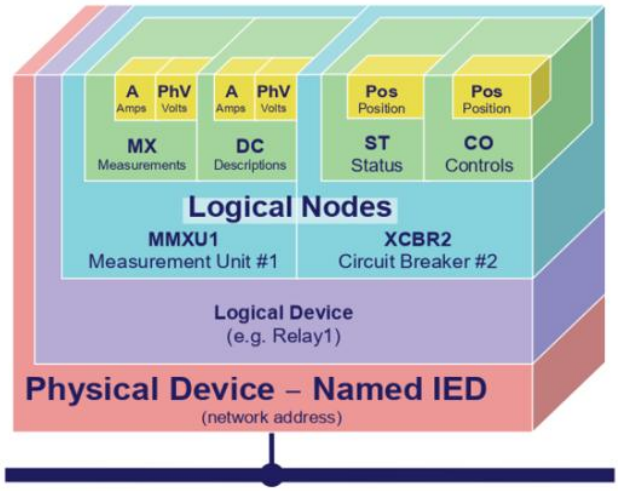
T0: tempo de retransmissão em condições estáveis.
T(0): tempo de retransmissão antes da ocorrência de um evento e que pode ser encurtado.
T1: menor tempo de retransmissão.
T2,T3: tempos de retransmissão que retornam gradualmente até o tempo máximo.
Fonte: Freitas (2022).

O MMS é um padrão internacional para troca de mensagens em que o tempo de transmissão não é crítico. Esse protocolo é usado para aquisição de dados e envio de comandos por meio da arquitetura cliente-servidor, seguindo Perfil-A ou Perfil-T de comunicação. A supervisão das grandezas elétricas é feita por meio de relatório, ou *reports*. Os *reports* enviam as informações relacionadas a um determinado *dataset*. O MMS prioriza estabelecer conexões e diminuir a possibilidade de erros no envio da informação, em detrimento da velocidade de comunicação (Aftab *et al.*, 2020).

2.3.2 Modelo da informação

A IEC 61850 define uma estrutura hierárquica de elementos concatenados, onde o elemento mais externo encapsula elementos com características mais básicas. A Figura 6 ilustra essa modelagem.

Figura 6 – Modelo da informação baseado na IEC 61850.



Fonte: Lozano et al., (2023).

Os *Physical Devices* (PD) são IEDs, fisicamente ligado a um barramento,que desempenham funções de proteção, supervisão ou controle de uma subestação.

Os *Logical Devices* (LD) compõem a estrutura interna do PD. Os LDspodem estar vinculados a várias funções do IED, incluindo proteção, lógica de operação, dentre outras. O padrão determina que deve haver pelo menos um LD em cada PD, entretanto, os fabricantes de IEDs optam por criar vários LDs com base em funções similares. Por exemplo, os componentes de medição são agrupados como um LD, enquanto os elementos de proteção são associados a outro LD. Não há um critério imperativo para essa organização (Lozano *et al.*, 2023).

A IEC 61850 fragmenta todas as funções conhecidas em uma subestação em *Logical Nodes* (LN). Os LN são agrupados para formar um LD. Os LN devem seguir uma sintaxe de nomenclatura obrigatória de quatro letras cujo primeiro caractere indica a funcionalidade conforme definido pela IEC 61850-7-4 (Lozano *et al.*, 2023).

Cada LD deve conter, pelo menos, três LN: o nó LLN0, crucial para registrar mensagens GOOSE, *DataSets* e relatórios; o nó LPHD, que registra as características físicas do dispositivo; e um terceiro nó qualquer. Os LN são subfunções do dispositivo que podem representar medições de grandezas elétricas, funções de proteção, equipamentos físicos, dentre

outros (International Electrotechnical Commission, 2003).

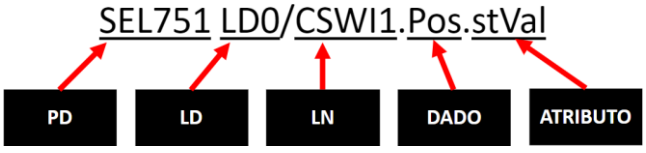
Um LN é composto por *Data Objects* (DO) que representam instâncias de informação com atributos. Cada DO pertence a uma determinada *Common Data Classes* (CDC). Os CDC são conjuntos de dados que descrevem informações comuns e frequentemente usadas por diferentes dispositivos. Essas classes de dados são categorizadas de acordo com sua funcionalidade e são utilizadas para padronizar a representação e a troca de informações entre os dispositivos em uma subestação. O uso de CDC ajuda a garantir a consistência e a interoperabilidade entre os dispositivos de diferentes fabricantes dentro de uma subestação.

Os *Data Atributes* (DA) são o núcleo do modelo e representam a informação. Para o LN de uma seccionadora, um dos seus DA é o *Status Value* (stVal). Esse atributo indica a condição atual da seccionadora, a saber: aberto, fechado, estado intermediário ou defeituoso (International Electrotechnical Commission, 2003).

Os DA podem ser agrupados em *datasets* e utilizados para diversas funcionalidades, como a criação de registros de operação. O nível de acesso aos DA por parte dos serviços de comunicação depende das *Functional Constraints* (FC). As FCscategorizam o acesso como informação de *status* (ST), medidas (MX), controle (CO), configuração (CF), descrição (DC) e definição estendida (EX) (International Electrotechnical Commission, 2003).

Vale ressaltar que a identificação de um dado é única, conforme estabelecido pelo padrão IEC 61850. A Figura 7 ilustra como um dado é identificado. Nesse modelo, o PD é identificado como SEL751. Na sequência, o LD é especificado como LD0. O fabricante *Schweitzer Engineering Laboratories* (SEL) opta por alocar todos os LN do seu relé em LD único. O LN CSWI1 se refere ao *status* da seccionadora. O dado transmitido pela informação é a posição da seccionadora (Pos), e seu atributo, stVal, pode variar em diferentes estados, como mencionado anteriormente.

Figura 7 – Identificação de dados conforme IEC 61850.



Fonte: Elaborado pelo autor.

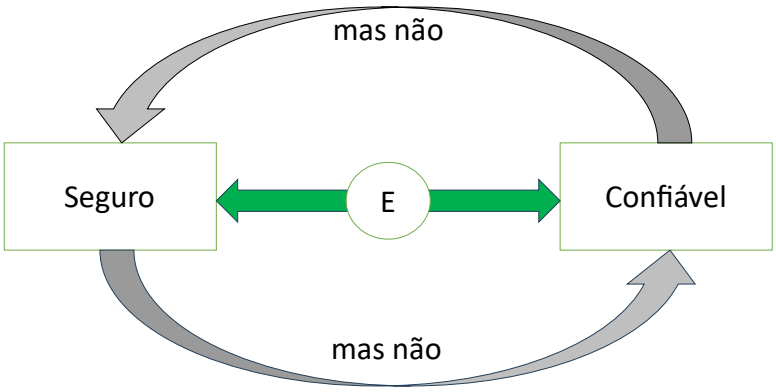
2.4 Confiabilidade e segurança: conceitos não intercambiáveis

Confiabilidade e segurança são conceitos distintos, frequentemente mal interpretados como intercambiáveis. Enquanto a confiabilidade é centrada na operação de um

sistema ou dispositivo sem falhas nas funções predeterminadas, a segurança refere-se à prevenção de perdas. A engenharia de confiabilidade foca em garantir o desempenho dos sistemas, enquanto a engenharia de segurança se dedica à mitigação de perigos e riscos para alcançar um nível aceitável de proteção (Mulazzani, 1985; Ross, 2021).

Embora a alta confiabilidade seja crucial para a segurança do sistema, ela não é uma garantia de segurança (Mulazzani, 1985). O trabalho de Ross (2021) exemplifica a relação de segurança e confiabilidade citando o desastre na *Deepwater Horizon Oil Rig* e a explosão da refinaria *Texas City*, resultado de uma série de falhas técnicas e operacionais, demonstrando que falhas de segurança podem ocorrer mesmo em sistemas confiáveis (Ross, 2021). A Figura 8 ilustra a relação entre os conceitos de confiabilidade e segurança.

Figura 8 – Segurança e confiabilidade: conceitos complementares.



Fonte: Elaborado pelo autor.

Embora confiabilidade e segurança sejam conceitos distintos, é possível encontrar um equilíbrio entre esses dois aspectos, especialmente em situações críticas (Singh; Singh, 2021).

Em Cabral et al. (2024), os autores mostram que ao substituir seccionadoras por disjuntores à montante de transformadores de potência no âmbito de subestação industrial, há uma redução do índice de disponibilidade do sistema, uma vez que a taxa de falha do disjuntor é superior à chave seccionadora. Entretanto, tal alteração torna o sistema mais seguro, uma vez que os operadores podem seccionar o sistema de forma remota, minimizando perda de vida humana, além de agregar recursos operacionais para cenários de contingência.

Portanto, um sistema pode ser projetado para ser confiável, mas ainda inseguro, se aspectos críticos de segurança forem negligenciados (Tamascelli *et al.*, 2024).

Por outro lado, Leveson (2011) enriquece o debate ao evidenciar que o contexto em

que o sistema está inserido impacta diretamente nas relações de segurança e confiabilidade. O autor mostra que ações não confiáveis em contexto específico podem contribuir com a segurança, exemplificando o pouso de emergência realizado no rio Hudson em junho de 1972, executado pelo piloto Bryce McCormick, quando uma porta de carga abriu em voo. O piloto agiu de forma contrária aos procedimentos de voo, portanto de forma não confiável. Porém, suas ações garantiram a segurança dos passageiros e um pouso de sucesso sob condições adversas.

O trabalho de Leveson (2011) enfatiza que para alcançar uma segurança abrangente do sistema, é essencial abordar os aspectos de confiabilidade e segurança de forma independente e em conjunto, reconhecendo suas contribuições distintas e possíveis conflitos. Logo, revisar a literatura para compreender as abordagens de confiabilidade para subestações digitais, bem como os modos de falha desse sistema, contribui para avaliação abrangente de segurança.

2.5 Avaliação de segurança em subestações digitais

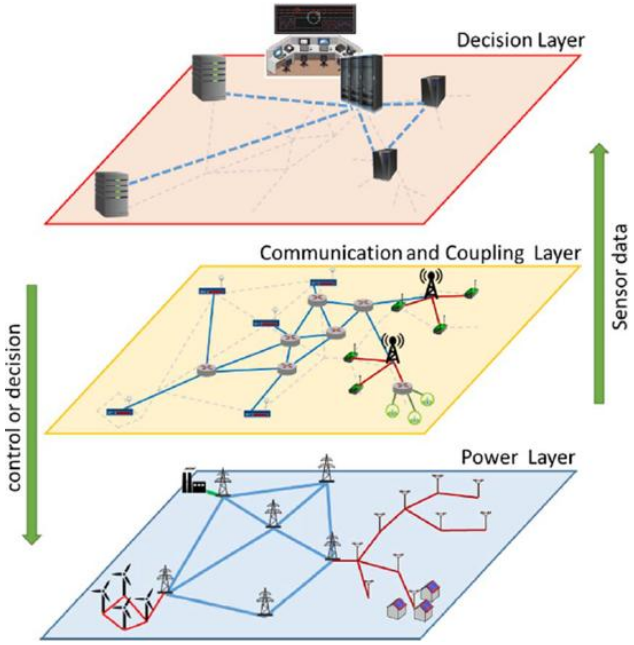
As subestações digitais são cruciais para redes elétricas inteligentes e estão intrinsecamente ligadas às tecnologias de informação e comunicação. A análise de confiabilidade em subestações convencionais possui métodos e abordagens bem estabelecidos na literatura. Entretanto, tais abordagens não atendem de forma abrangente às subestações digitais. Dessa forma, avaliar a confiabilidade e segurança em subestações digitais ainda é um desafio (Syed; Hoidalen, 2023).

2.5.1 Confiabilidade em sistema ciber-físico de energia

A confiabilidade da medição de sinais elétricos, envio de *trip* e intertravamento entre IED, usando conexão com fio entre sensores e IED, era em grande parte determinística em subestações convencionais. No entanto, a confiabilidade em subestações digitais depende da rede de comunicação, principalmente usando a tecnologia Ethernet. A interação e dependência entre dispositivos de energia e tecnologias da informação, ou dispositivos cibernéticos, constituem o sistema de energia ciber-físico (Syed; Hoidalen, 2023).

A Figura 9 apresenta uma modelagem para sistema de energia ciber-físico por meio da subdivisão do sistema em camadas.

Figura 9 – Modelo de sistema ciber-físico.



Fonte: Syed e Hoidalen (2023).

A camada de energia, composta por dispositivos físicos como transformadores, disjuntores, seccionadoras, entre outros, está interligada à camada de comunicação e acoplamento por meio de sensores e dispositivos de execução de comando. A confiabilidade dessa camada pode ser modelada utilizando técnicas tradicionais de análise de confiabilidade, a exemplo do modelo de Markov (Aravinthan *et al.*, 2018).

A camada de comunicação e acoplamento é constituída por dispositivos de interface e pela rede de comunicação. Essa camada viabiliza a medição e o controle da camada de energia, além das funções de tomada de decisão na camada superior. Para garantir a confiabilidade do sistema de energia, é essencial manter redundância na rede de comunicação. O atraso e a perda de dados devem ser considerados ao modelar a confiabilidade dessa camada (Aravinthan *et al.*, 2018).

A camada de decisão em um sistema de energia utiliza condições estimadas dos estados operacionais, obtidas a partir de medições em tempo real, para tomar decisões. Ataques cibernéticos devem ser considerados na avaliação de confiabilidade desta camada, pois podem distorcer medições ao invadir (*hacker*) sensores ou injetar dados falsos nos *links* de comunicação. Tais ações podem resultar em decisões incorretas, mau funcionamento e blecautes.

A modelagem de confiabilidade para sistema de energia ciber-físico pode ser realizada considerando os possíveis estados de cada camada, tanto no nível dos seus componentes quanto no nível do sistema (Aravinthan *et al.*, 2018).

Nesse contexto, há dois principais desafios para avaliar a confiabilidade de um sistema de energia ciber-físico: diferentes modos de falha por camada e falta de dados históricos. A funcionalidade dos equipamentos de energia está associada à rede de comunicação e à camada de decisão, onde cada camada tem seus próprios modos de falha, incluindo software. Além disso, a obtenção de parâmetros como taxas de falha e taxas de reparo é comprometida pela falta de dados históricos (Syed; Hoidalen, 2023).

Em Syed e Hoidalen (2023), é realizado uma revisão da literatura sobre métodos usados para avaliar a confiabilidade de subestações digitais. O autor categoriza as estratégias encontradas na literatura em abordagens isoladas ou integradas, dependendo de como os equipamentos primários e secundários são avaliados.

Os equipamentos primários se referem aos dispositivos físicos localizados na camada de potência da subestação, como transformadores, disjuntores, chaves seccionadoras, entre outros. Por outro lado, os equipamentos secundários são aqueles que compõem a camada de comunicação e decisão, como sistema de automação, controle, supervisão e proteção (Santos *et al.*, 2024).

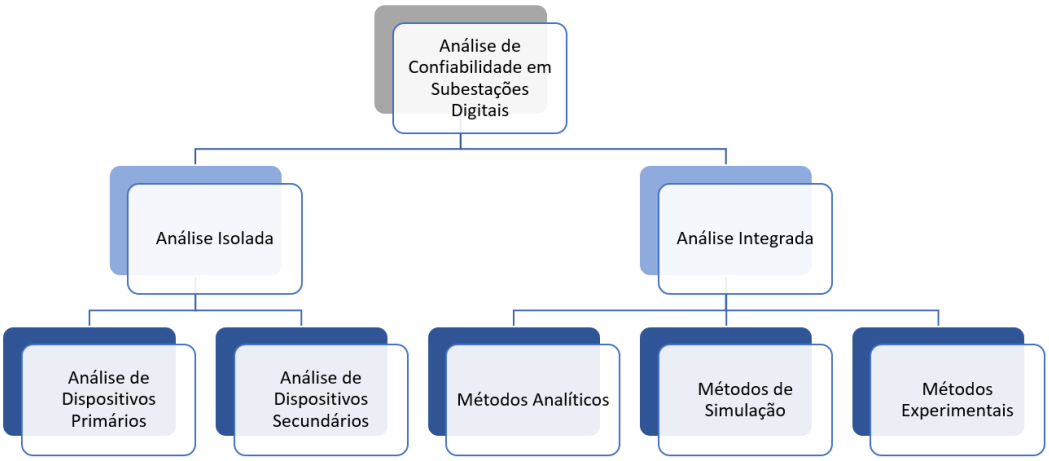
Na abordagem isolada, a digitalização é limitada ao barramento de estação da subestação e não é objeto de preocupação significativa para a proteção do sistema. Portanto, os estudos que seguem essa abordagem aplicam métodos semelhantes aos das subestações convencionais, avaliando os equipamentos primários sem considerar as influências dos equipamentos secundários. Técnicas como Análise de Árvore de Falhas, Diagrama de Blocos de Confiabilidade, Medida de Importância de Confiabilidade de Birnbaum e Valor de Realização de Risco são aplicadas de forma isolada aos equipamentos primários e secundários (Syed; Hoidalen, 2023).

A digitalização completa da subestação e a dependência do funcionamento dos equipamentos primários no sistema secundário direcionou os esforços recentes de pesquisa para compreensão dos modos de falha associados ao sistema secundário e estabelecer uma conexão com os dispositivos primários (Syed; Hoidalen, 2023).

O trabalho de Syed e Hoidalen (2023) divide a abordagem integrada em métodos analíticos, de simulação e experimentais, conforme ilustrado na Figura 10. Os métodos analíticos envolvem o uso de técnicas teóricas e modelos matemáticos para avaliar a confiabilidade do sistema, segmentando o processo em etapas definidas. Esses métodos têm como base análises quantitativas e qualitativas dos componentes e suas interações. O autor destaca as técnicas de Diagramas de Blocos, Espaço de Estados de Markov e Simulação de Monte Carlo, que podem ser empregados em conjunto ou como suporte para novas

metodologias.

Figura 10 – Métodos para abordagem integrada.



Fonte: Elaborado pelo autor.

Por outro lado, os métodos de simulação usam software ou ferramentas de simulação, como o *Optimized Network Engineering Tool* (OPNET), para modelar o comportamento do sistema em um ambiente virtual. Eles permitem a análise do desempenho do sistema em diferentes condições e cenários, fornecendo resultados mais próximos da realidade.

Já os métodos experimentais envolvem a implementação de testes práticos em ambiente real ou laboratorial com *Real Time Digital Simulator* (RTDS). Eles permitem avaliar o desempenho do sistema em condições controladas e observar diretamente o comportamento dos componentes e da rede em situações específicas.

É essencial integrar as camadas física e lógica para obter resultados assertivos nas avaliações de confiabilidade. No entanto, devido à complexidade do sistema, várias metodologias foram desenvolvidas, e ainda não há uma abordagem única e abrangente. A padronização e a definição de índices e modos de falha são fundamentais para uma avaliação abrangente da confiabilidade dos sistemas digitais de energia.

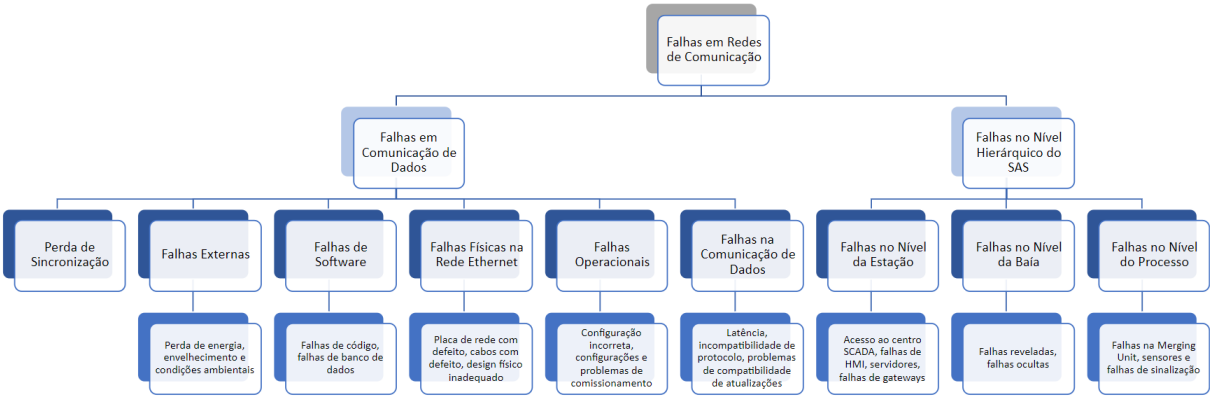
2.5.2 Modos de falha em subestações digitais

A rede de comunicação é crucial para as subestações digitais, porém, sua introdução também trouxe consigo um conjunto distinto de vulnerabilidades em comparação com os sistemas convencionais de controle e proteção. Essas vulnerabilidades podem ser categorizadas como falhas na própria rede de comunicação e como alvos potenciais de ciberataques.

2.5.2.1 Falha na rede de comunicação

Um diagrama de árvore dos modos de falha na rede de comunicação é apresentado na Figura 11. Os modos de falha são mitigados por meio de um projeto de rede adequado, engenharia de tráfego e componentes redundantes (Syed; Hoidalen, 2023).

Figura 11 – Modos de falha na rede de comunicação.



Fonte: Adaptado de Syed; Hoidalen (2023).

A sincronização precisa entre dispositivos é uma prioridade, especialmente com a crescente adoção do padrão IEC 61850, que especifica a necessidade de sincronização dos dados coletados no nível de processo. A perda ou falha na fonte de sincronização pode afetar a utilidade dos dados e levar a condições inseguras de operação (Syed; Hoidalen, 2023).

Além disso, falhas externas, como perda de energia e condições ambientais adversas, podem comprometer o funcionamento do sistema. A perda de energia, decorrente de falhas no sistema de distribuição ou surtos na fonte de alimentação, pode reiniciar dispositivos e causar falhas no sistema. Para mitigar esses problemas, é possível fornecer redundância de energia para dispositivos-chave, como servidores e *switches*. As condições ambientais, como temperatura, também representam uma preocupação, pois podem causar falhas nos equipamentos de comunicação e no cabeamento associado. O acúmulo de sujeira em componentes eletrônicos também é uma ameaça, pois pode reduzir a eficácia do sistema de resfriamento e até causar incêndios em condições extremas (Syed; Hoidalen, 2023).

As falhas de software, como defeitos de código e falhas de banco de dados, representam riscos significativos para a operação eficaz dos sistemas de automação de subestações. As ferramentas de programação disponíveis para os IED oferecem uma variedade de recursos, como operadores booleanos, elementos de equação de controle, elementos binários, quantidades analógicas e operadores matemáticos. A complexidade dos projetos de software

influencia diretamente a frequência de falhas esperadas. Especialmente, a incorporação de *latches* e unidades de atraso de tempo para desenvolver lógicas de proteção e controle aumenta a sofisticação da lógica e, consequentemente, a probabilidade de ocorrência de falhas (Syed; Hoidalen, 2023).

À medida que novos conjuntos de dados são coletados do sistema de energia, o tamanho do banco de dados gradualmente aumenta. É fundamental armazenar esses conjuntos de dados em unidades protegidas a fim de evitar acesso não autorizado, seja para leitura ou escrita, garantindo assim a integridade e segurança dos dados. Qualquer interrupção ou descompasso inesperado nos dados armazenados no banco de dados pode afetar negativamente o funcionamento do software (Syed; Hoidalen, 2023).

Os problemas de conectividade de rede em SAS surgem devido a diversas razões, como defeitos em *Network Interface Card* (NIC), cabos danificados, terminações inadequadas ou comprimento excessivo dos cabos. Essas questões frequentemente afetam a camada física do modelo OSI, que inclui NICs, roteadores e *switches*, podendo resultar na desconexão de segmentos da rede quando os cabos entre os nós são desconectados. Para mitigar esses riscos, caminhos totalmente redundantes, encontrados em topologias como *High-Availability Seamless Redundancy* (HSR) e *Parallel Redundancy Protocol* (PRP), têm se mostrado soluções eficazes (Syed; Hoidalen, 2023).

Colisões na rede Ethernet resultam na geração de *runts* e *giants*, que são pacotes inválidos de tamanho pequeno e grande, respectivamente, destacando a importância da escolha de comprimentos adequados de cabo para evitar tais problemas. Além disso, falhas operacionais, decorrentes de deficiências no projeto e na engenharia, podem ocasionar operações incorretas no sistema de energia. Durante o comissionamento de IED, é crucial testar intertravamentos, controles e lógica de proteção para assegurar o funcionamento adequado (Syed; Hoidalen, 2023).

Falhas de comunicação de dados, que se distinguem das falhas na estrutura da rede, apresentam desafios adicionais devido à ausência de ferramentas específicas para sua identificação, o que torna sua resolução mais complexa. A interoperabilidade entre dispositivos é constantemente testada pela diversidade de protocolos, apesar dos esforços do IEC 61850 para padronização. A implantação de *switches* multiprotocolo para garantir a integridade e interoperabilidade do sistema é a solução mais viável (Syed; Hoidalen, 2023).

Problemas de compatibilidade provenientes de atualizações de hardware, software ou firmware também podem impactar significativamente a operação da rede. Além disso, há dois tipos inevitáveis de latência na rede: a constante e a variável. A latência constante está

diretamente ligada aos atrasos naturais em nós e conexões e é determinada pela estrutura física da rede e pela largura de banda disponível, sendo calculável e previsível. Por outro lado, a latência variável é influenciada pelo tráfego e pela carga na rede. A ocorrência de comunicações simultâneas entre dispositivos em uma largura de banda compartilhada ou falhas na rede tendem a aumentar a latência variável (Syed; Hoidalen, 2023).

As falhas no nível da estação representam um desafio significativo devido à dificuldade em identificar sua origem. Para mitigar esse risco, a adoção de fontes de conteúdo redundantes, incluindo Interfaces Homem-Máquina (IHM), servidores e *gateways* redundantes, é uma prática recomendada no SAS. O servidor é o principal componente do nível da estação, uma vez que sua falha pode resultar em perda permanente de dados no SAS. O espelhamento emerge como um método eficaz para fornecer redundância de espera à quente entre servidores, garantindo a continuidade das operações em caso de falha, com a transferência de carga ocorrendo de forma rápida e eficiente (Syed; Hoidalen, 2023).

O nível de *bay* é essencial para a integridade do SAS, sendo responsável pela coleta de dados, execução de comandos e proteção e controle da rede de energia. Comparativamente aos demais níveis, as falhas neste nível têm um impacto mais severo na operação da rede. Tais falhas podem ser reveladas, quando os IEDs detectam e respondem, ou ocultas, permanecendo invisíveis até que uma falha ocorra. Para evitar falhas ocultas, os IED são equipados com mecanismos de autoteste e diagnóstico (Syed; Hoidalen, 2023).

Falhas ocultas podem levar o sistema a operar inadequadamente, causando interrupções indesejadas ou falhando em responder quando necessário. Isso é especialmente preocupante em relação aos IED multifuncionais, onde uma única falha pode desativar todas as funções críticas do sistema (Syed; Hoidalen, 2023).

As falhas no nível de processo ocorrem nos equipamentos responsáveis pela coleta de dados, tais como TCs, TPs, MUs e sensores. O controle, proteção e monitoramento do sistema de energia dependem dos dados coletados por esses equipamentos. Portanto, quaisquer falhas nesse nível podem comprometer a interação adequada entre as redes de energia e o SAS (Syed; Hoidalen, 2023).

A compreensão dos diferentes modos de falha é fundamental para o desenvolvimento de modelos abrangentes de avaliação de confiabilidade de SASs e redes de energia. Tal compreensão contribui para a identificação de áreas críticas e a implementação de medidas preventivas para garantir a operação eficiente e segura desses sistemas em um *framework* único de avaliação (Syed; Hoidalen, 2023).

2.5.2.2 Ataques cibernéticos

A arquitetura das subestações digitais proporciona interoperabilidade e acesso remoto para monitoramento e controle, mas também apresenta riscos de segurança, pois os protocolos de comunicação podem ser explorados por intrusos. Ataques coordenados podem modificar pacotes de comunicação para perturbar funções de proteção e medição, desencadeando operações defeituosas, que podem prejudicar gravemente o sistema elétrico e seus usuários (Shikhin; Trutneva, 2023).

Os ciberataques em subestações seguem quatro estágios principais: reconhecimento, varredura, exploração e manutenção de acesso. A fase de reconhecimento consiste em observar e analisar a rede para reunir informações sobre o alvo. Em seguida, vem a varredura de endereços IP, portas e serviços da rede, durante a qual o *hacker* procura vulnerabilidades a serem exploradas para o ciberataque. A exploração é o cerne do ataque, pois é o momento em que o *hacker* atua ativamente no sistema. Por fim, as ações do intruso são direcionadas a manutenção do acesso ao alvo, resgatando *backdoors* e programas de malware investidos anteriormente (Hussain *et al.*, 2021).

As quatro fases supracitadas do ciberataque em subestações em duas etapas: acesso à rede da subestação e exploração do acesso. O desempenho do sistema não pode ser afetado ao empregar soluções de monitoramento e análise em tempo real, como *Intruder Detection Systems* (IDS). Portanto, um *hacker* pode acessar a rede de uma subestação explorando *firewalls*, usando redes públicas e acesso à internet, encontrando senhas fracas, principalmente senhas padrão durante a fase de comissionamento, explorando vulnerabilidades em sistemas operacionais obsoletos e enviando unidades flash USB infectadas por software malicioso (Hussain *et al.*, 2021).

Cada tipo de ataque cibernético apresenta características distintas que os diferenciam em métodos de execução, objetivos e impactos. O ataque por meio de malware abrange uma variedade de software malicioso, como vírus, *worms* e *ransomware*, desenvolvidos para infiltrar-se em sistemas e causar danos ou roubar informações. Os ataques de *Denial of Service* (DoS) sobrecarregam sistemas ou redes com tráfego excessivo, impedindo o acesso legítimo aos serviços. O *Man-in-the-Middle* (MITM) intercepta e monitora comunicações entre duas partes, permitindo ao invasor capturar informações confidenciais. O *Popping the HMI* visa comprometer o sistema de controle industrial, explorando vulnerabilidades na interface Homem-Máquina. O *False Data Injection* (FDI) envolve a injeção de dados falsos em sistemas de controle, potencialmente resultando em decisões errôneas. O

Replaying intercepta e reproduz comunicações legítimas para enganar sistemas. O *Channel Jamming* sobrecarrega canais de comunicação com ruído, tornando a comunicação inutilizável. Finalmente, o *Spoofing* envolve a falsificação de identificadores de dispositivos para obter acesso não autorizado (Hussain *et al.*, 2021).

Em Shikhin e Trutneva (2023), os autores avaliam os níveis de risco de ataques cibernéticos a diferentes recursos de informação dentro do sistema de controle da subestação digital, considerando fatores como a criticidade dos recursos, a probabilidade de um ataque e as possíveis consequências de uma intrusão cibernética bem-sucedida. O trabalho contribui para uma abordagem direcionada a mitigar riscos e aprimorar as ações de segurança cibernética.

Uma forma de atacar a subestação é violar os requisitos de atraso das mensagens. Em Hussain et al. (2021), o autor divide os dados trafegados na rede da subestação em mensagens críticas e não críticas em relação ao tempo. Para mensagens não críticas em relação ao tempo, o *Transport Layer Security* (TLS) é baseado em TCP/IP e *Media Access Control* (MAC) para garantir confidencialidade e integridade dos dados. Já para mensagens críticas em relação ao tempo, a camada de *link* de dados é conectada diretamente à camada de aplicação e o TCP/IP é evitado, assim como qualquer mecanismo de criptografia. A autenticação é obtida com MAC usando *Secure Hash Algorithm* (SHA), assinada digitalmente com um sistema de chave pública *Rivest-Shamir-Adleman* (RSA).

Por sua vez, Akbarzadeh et al. (2023) se concentram em ataques cibernéticos direcionados ao Protocolo de Tempo de Precisão (PTP) utilizado para sincronização das mensagens em subestações digitais padrão IEC 61850. As principais contribuições do trabalho é o estudo das possíveis consequências dos ataques cibernéticos ao PTP e o desenvolvimento de estratégias de mitigação para proteção contra esses ataques.

Diferente da mensagem MMS, as mensagens GOOSE e SV são críticas em relação ao tempo. As mensagens GOOSE devem possuir atraso inferior a 3 milissegundos e comprimento de 160 a 310. Um *hacker* pode usar um ataque MITM para impedir um comando de abertura do disjuntor ou pode realizar desarmes falsos dos disjuntores. Já as mensagens SV permitem atrasos inferiores a 3 milissegundos e comprimentos de 190 a 340 bytes. Essas mensagens são propensas a ataques lógicos FDI que mantêm o controlador inconsciente do desempenho real dos dispositivos de campo até que o dano seja concretizado. Outra forma de ataque é forçar o controlador a iniciar medidas de proteção inoportunas por meio da inserção de dados falsos dos dispositivos de campo (Hussain *et al.*, 2021).

A mensagem MMS também pode ser alvo de ataques. Essa mensagem deve conter atraso de tempo inferior a 100 milissegundos e comprimento de 1480 bytes. Inicialmente, o

invasor obtém acesso ao IED por meio de diversos ataques, como MITM, FDI e *Replaying*. Em seguida, lançam um ataque de DoS a partir dos IED comprometidos em direção à IHM, tornando-o irresponsivo a solicitações e/ou comandos legítimos. Quando a IHM é controlada pelo invasor, a magnitude potencial do dano é superior à exploração de mensagens GOOSE e SV (Hussain *et al.*, 2021).

O trabalho de Abraham et al. (2023) investiga a detecção de ataques cibernéticos em subestações digitais por meio de simulações, destacando a importância da detecção precoce para mitigar os impactos nas operações da rede elétrica. O autor compara algoritmos de aprendizado de máquina na detecção de ataques de *Replaying* e FDI, identificando o modelo estatístico de regressão logística como alternativa eficaz para detecção de ataques de *Replaying*, enquanto a Máquina de Vetores de Suporte (MVS), algoritmo de aprendizado de máquina, se sobressai na detecção de injeções de dados falsos, especialmente em termos de tempo de computação.

Em Hussain et al. (2021), contramedidas são discutidas em três níveis de proteção para evitar ataques. Primeiro, proteger a rede de comunicação, depois os dados, e, por fim, os dispositivos da subestação.

A *Software Defined Networking* (SDN) é proposta para garantir integridade da rede de comunicação da subestação. O objetivo desta rede é isolar o tráfego, detectar anomalias e colocar *firewalls* e controles de *spoofing*. As contramedidas nesta etapa podem ser empregar IDS e *Intruder Protection System* (IPS) para monitorar tentativas de intrusão que podem ser evitadas usando *Virtual Private Network* (VPN), *honeypots* e outras soluções feitas sob medida para ataques previamente conhecidos (Hussain *et al.*, 2021).

Quando a proteção de acesso à rede é superada, os dados da subestação devem ser protegidos por novas contramedidas. Para proteger a comunicação de dados entre os dispositivos da subestação, métodos como criptografia e gerenciamento de chaves podem ser implantados. Os próprios protocolos de comunicação GOOSE e SV podem ser utilizados em suas versões roteáveis, *Routable Generic Object-Oriented Substation Event* (R-GOOSE) e *Routable Sampled Values* (R-SV), respectivamente, projetadas para permitir o roteamento dessas mensagens em redes IP (Hussain *et al.*, 2021).

O dispositivo mais cobiçado no ciberataque a uma subestação é o IED, pois ele é capaz executar comandos críticos, tais como desenergização de alimentadores e bloqueio de energização do sistema elétrico. Sua segurança é proposta na literatura recente usando diferentes algoritmos e IDS incorporados nos IED para detectar os comportamentos anormais nas mensagens recebidas sem impactar nas funções de proteção do dispositivo. Essa solução

está em fase de desenvolvimento na comunidade acadêmica (Hussain *et al.*, 2021).

2.6 Determinação de risco em sistemas complexos

Um sistema é um conjunto de elementos interconectados que trabalham juntos para alcançar um objetivo comum ou realizar uma função específica. A complexidade dos sistemas pode variar, sendo definida pelos relacionamentos e interações entre seus componentes (Leveson; Thomas, 2018).

A evolução das técnicas de determinação de risco em sistemas é dividida ao longo do tempo em cinco etapas distintas, cada uma caracterizada por abordagens e preocupações específicas relacionadas à segurança e gestão de riscos (Waterson *et al.*, 2015).

A primeira fase é denominada de Período Tecnológico, que se estende desde a Segunda Revolução Industrial até o pós-Segunda Guerra Mundial. O foco principal dessa fase é a prevenção de acidentes por meio de medidas para evitar falhas em equipamentos e estruturas. Neste período, surgiram métodos como a *Failure Mode and Effect Analysis* (FMEA), a *Fault Tree Analysis* (FTA) e o *Hazard and Operability Study* (HAZOP), que visavam identificar e mitigar possíveis falhas em sistemas complexos (Roque, 2022; Waterson *et al.*, 2015) .

Em seguida, o Período dos Fatores Humanos emergiu após o acidente da planta nuclear de *Three Mile Island* em 1979, reconhecendo a importância de considerar os aspectos humanos nas análises de segurança. Durante esta fase, foram desenvolvidos métodos como a *Human Reliability Analysis* (HRA), incluindo técnicas específicas como a *Technique for Human Error Rate Prediction* (THERP) e o método *Human Error Assessment and Reduction Technique* (HEART) (Roque, 2022; Waterson *et al.*, 2015).

A terceiro fase, denominada Período do Gerenciamento Organizacional, surgiu devido à percepção das limitações das abordagens anteriores e à necessidade de incluir aspectos organizacionais na gestão de riscos. Neste contexto, métodos como o *Accident Mapping* (AcciMap) e o *Swiss Cheese Model* foram introduzidos para avaliar acidentes e incidentes de causas complexas interdependentes (Roque, 2022; Waterson *et al.*, 2015).

Posteriormente, o Período de Integração propôs a combinação e sinergia dos três primeiros períodos, visando uma abordagem mais abrangente e holística para o gerenciamento de riscos. Esta fase incluiu a aplicação de métodos como a *Probabilistic Safety Assessment* (PSA) em conjunto com análises de fatores humanos e organizacionais (Roque, 2022; Waterson *et al.*, 2015).

Por fim, a Era Adaptativa surge como uma resposta à complexidade crescente dos

sistemas organizacionais, destacando a necessidade de adaptação contínua e consideração de riscos inesperados. Métodos como o *Functional Resonance Analysis Method* (FRAM) e o *Systems-Theoretic Accident Model and Processes* (STAMP) foram desenvolvidos para abordar questões de resiliência e adaptabilidade em ambientes organizacionais complexos (Roque, 2022; Waterson *et al.*, 2015; MIT, [202-?]).

Sistemas complexos são compostos por subsistemas interligados e possuem propriedades que resultam das interações entre seus componentes. A modelagem e análise desses sistemas ajudam a compreender como mudanças locais podem influenciar comportamentos globais. No entanto, técnicas tradicionais de otimização podem não ser adequadas para lidar com a complexidade desses sistemas (Jiang *et al.*, 2016).

A teoria dos sistemas é um conjunto de princípios que podem ser usados para compreender o comportamento de sistemas complexos (Leveson, 2004).

Em Bertalanffy (1968), o autor apresenta conceitos fundamentais para a compreensão da dinâmica e funcionamento dos sistemas complexos. A retroalimentação é o mecanismo pelo qual as informações sobre o estado atual do sistema são utilizadas para ajustar seu comportamento. Já o princípio da equifinalidade ressalta a capacidade dos sistemas de alcançar um mesmo resultado por diferentes caminhos ou processos. Além disso, a hierarquia de sistemas reconhece a organização em diferentes níveis de complexidade, enquanto a homeostase descreve a tendência dos sistemas em manter um estado de equilíbrio interno diante de mudanças ambientais.

Nesse contexto, Leveson (2004) desenvolve um novo modelo de causalidade de acidentes baseado na teoria dos sistemas chamado de STAMP. Esse modelo expande o conceito tradicional de causalidade, tratando a segurança como um problema dinâmico de controle.

Diferente dos métodos tradicionais, o STAMP inclui fatores como software, ações humanas, procedimentos operacionais e cultura de segurança na modelagem e avaliação de sistemas complexos. Esse modelo não é um método de análise em si, mas é a base para ferramentas como *System-Theoretic Process Analysis* (STPA) e *Causal Analysis based on Systems Theory* (CAST). STPA é uma análise proativa, enquanto CAST é retroativa. Ambas as ferramentas são usadas para identificar causas potenciais de acidentes e gerenciar riscos (Leveson; Thomas, 2018).

2.7 Considerações finais

A Indústria 4.0 está impulsionando a automação e digitalização das subestações

elétricas, com o padrão IEC 61850 desempenhando um papel central nesse processo. No entanto, a segurança cibernética e a avaliação de riscos operacionais são áreas críticas que precisam ser abordadas para garantir a confiabilidade e integridade dos sistemas de energia elétrica em um ambiente digitalizado. Nesse sentido, o método *System-Theoretic Process Analysis* (STPA) surge como alternativa para avaliação de segurança em sistemas complexos conforme é explorado no Capítulo 3.

3 FERRAMENTAS DE MODELAGEM

Neste Capítulo são abordados os conceitos do método STPA, destacando seu propósito, a modelagem da estrutura de controle, a identificação de ações de controle inseguras e cenários de perda. Além disso, é apresentado a ferramenta utilizada para aplicação do STPA a uma subestação industrial.

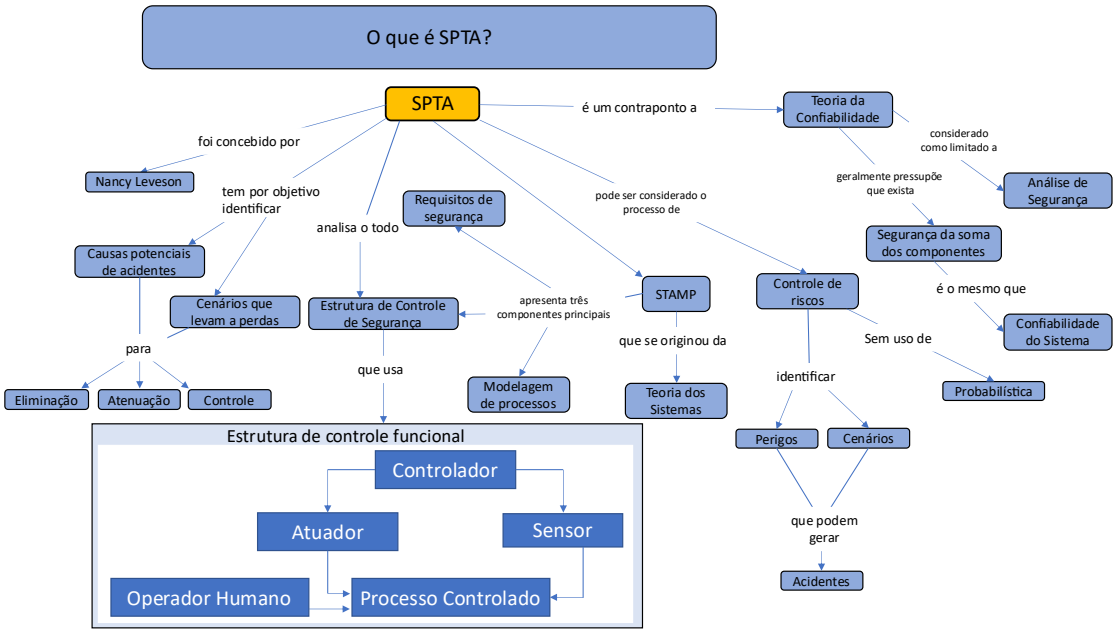
3.1 Método *System-Theoretic Process Analysis* (STPA)

Os sistemas complexos modernos demandam uma compreensão profunda das interações entre os aspectos técnicos, humanos, sociais e organizacionais que os compõem. Na tentativa de modelar a dinâmica desses sistemas, Leveson (2004) propõe o modelo causal STAMP, no qual falhas residem em todo o sistema, e que cada elemento desempenha um papel essencial, dando assim suporte a uma análise multicausal. O STAMP não se caracteriza como um método de análise, mas sim como um modelo ou conjunto de pressupostos que delineiam a forma como os acidentes ocorrem.

O STPA é uma técnica de análise de riscos e cenários indesejados advinda do modelo STAMP. Ela emprega uma coleção de loops de controle interativos para examinar o sistema, identificando cenários de risco e potenciais perdas. Ao contrário de métodos tradicionais, o STPA busca identificar mais fatores causais e cenários perigosos sem avaliar ou produzir probabilidades de perigo, visto que em sistemas complexos, as probabilidades disponíveis podem omitir importantes fatores causais. A confiança em análises probabilísticas imprecisas pode gerar falsa segurança e potencialmente levar a acidentes devido à falta de correção de falhas no projeto (Leveson, 2004).

A Figura 12 apresenta um mapa conceitual acerca do método STPA, destacando o autor e origem do método, bem como seus objetivos. Vale destacar que o STPA surge como uma alternativa às abordagens de confiabilidade, centrado na identificação e controle dos cenários de risco sem utilizar análises estatísticas ou avaliações de probabilidade para os contextos de perda. Além disso, o método modela a estrutura de controle do sistema definindo controladores, processos controlados, sensores e *feedbacks*, sem descartar a ação de operadores humanos.

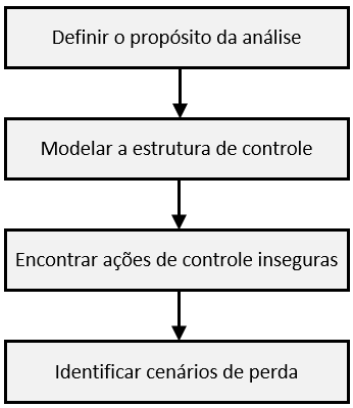
Figura 12 – Mapa conceitual para STPA.



Fonte: Adaptado de Borges et al. (2021)

O método STPA é composto por quatro fases, conforme ilustrado Figura 13. O primeiro passo é a definição do propósito da análise, que inclui identificar os tipos de perdas a serem prevenidas e delinear a extensão de aplicação do STPA. Essa amplitude pode variar desde objetivos tradicionais de segurança até questões mais amplas, como privacidade e desempenho do sistema (Leveson; Thomas, 2018).

Figura 13 – Fase do método STPA.



Fonte: Elaborado pelo autor.

Em seguida, é elaborado o modelo da estrutura de controle do sistema com relacionamentos funcionais e as interações do sistema por meio de *loops* de controle de *feedback*. Esse modelo passa por refinamentos iterativos para incorporar mais detalhes sobre o sistema (Leveson; Thomas, 2018).

Posteriormente, as ações de controle na estrutura de controle são analisadas para examinar como elas podem resultar nas perdas identificadas anteriormente, gerando requisitos funcionais e restrições para o sistema. Além disso, são identificados os motivos pelos quais o controle inseguro pode ocorrer, por meio da criação de cenários que explicam como *feedback* incorreto, requisitos inadequados, erros de projeto e falhas de componentes podem levar a perdas, bem como ações de controle seguras podem não ser adequadamente seguidas ou executadas, resultando em perdas (Leveson; Thomas, 2018).

Uma característica marcante do STPA é a rastreabilidade completa dos eventos, desde os primeiros requisitos, como perdas, até as últimas ações de controle e seus responsáveis. Isso aumenta a manutenibilidade e a evolução da modelagem e análise do sistema (Leveson; Thomas, 2018).

3.1.1 Definição do propósito da análise

O processo inicial na implementação do STPA é estabelecer o propósito da análise por meio de quatro etapas, a saber: determinar perdas, identificar perigos em nível de sistema, estabelecer restrições em nível de sistema e refinar perigos em nível de sistema (Leveson; Thomas, 2018).

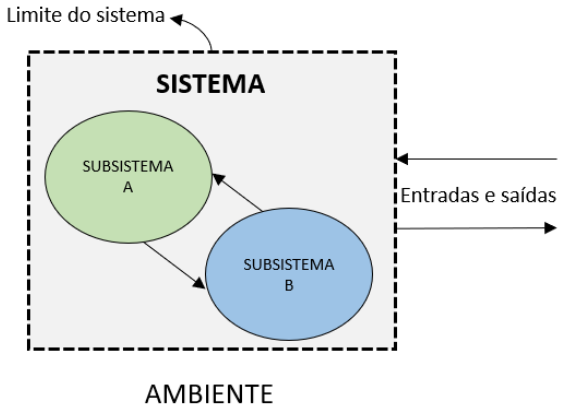
Uma abordagem geral para identificar perdas é composta por quatro etapas: identificar partes interessadas, reconhecer o que as partes interessadas valorizam, definir as perdas e detectar perigos em nível de sistema. As perdas não devem fazer referência a componentes individuais ou causas específicas e podem envolver aspectos do ambiente externo que não são diretamente controlados pelo projetista do sistema (Leveson; Thomas, 2018).

A segunda etapa na definição do propósito da análise é a identificação dos perigos em nível de sistema. Esses perigos são estados ou condições no sistema que, quando ocorrem simultaneamente com condições ambientais adversas, resultam em uma perda (Leveson; Thomas, 2018).

Para identificar os perigos em nível de sistema, é fundamental primeiro definir o que será incluído no sistema e onde será estabelecido seu limite. O sistema deve ser delineado de modo que o projetista tenha controle de todas as suas partes. Perigos e perdas são conceitos diferentes, pois a perda é o evento adverso real, como dano, lesão, ou morte, que ocorre como resultado de um ou mais perigos que não foram adequadamente controlados. Além disso, as perdas podem abranger aspectos ambientais sobre os quais os projetistas têm controle parcial ou nenhum controle (Leveson; Thomas, 2018).

A Figura 14 ilustra o limite do sistema como uma abstração que separa o sistema de seu ambiente.

Figura 14 – Relação entre sistema, subsistemas, fronteira e ambiente.



Fonte: Adaptado de Leveson e Thomas (2018).

Em Leveson e Thomas (2018), o autor determina três critérios fundamentais para definir perigos em nível de sistema, a saber: perigos são estados ou condições do sistema e não causas em nível de componente ou estados ambientais, que levarão a uma perda em algum ambiente de pior caso e descrevem estados ou condições a serem evitadas.

É importante salientar que o STPA é um método iterativo e os perigos não precisam ser definitivos. Etapas posteriores do método podem revelar novos perigos. A lista de perigos em nível de sistema pode ser revisada conforme necessário (Leveson; Thomas, 2018).

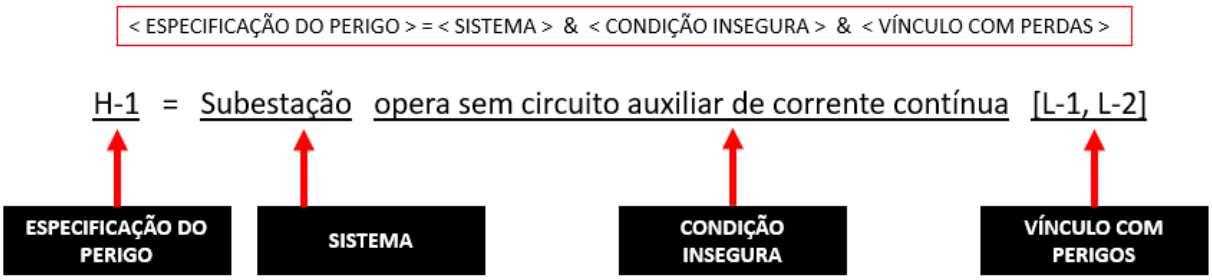
Uma vez que os perigos estejam mapeados, o método segue para a determinação das restrições em nível de sistema, impondo limitações ou condições que devem ser mantidas para evitar os perigos e, consequentemente, perdas. As restrições também podem definir como o sistema deve se comportar para minimizar as perdas caso os perigos ocorram. Elas não devem especificar uma solução para condições de perigo, e sim ações que o sistema deve ser capaz de executar (Leveson; Thomas, 2018).

Após identificar e revisar os perigos em nível de sistema, é importante refiná-los em subperigos. Embora não sejam essenciais para todas as aplicações do STPA, os subperigos podem ser úteis em análises extensas e contextos complexos, orientando etapas posteriores, como a modelagem da estrutura de controle. O refinamento começa pela identificação dos processos ou atividades básicas do sistema que devem ser controlados para evitar esses perigos. Isso pode ser feito questionando o que precisa ser controlado para prevenir cada perigo. A partir das respostas, é possível definir os subperigos (Leveson; Thomas, 2018).

Em Leveson e Thomas (2018), os autores sugerem uma taxonomia para registro dos

perigos e restrições a nível de sistema a fim de manter a rastreabilidade dos eventos dentro do STPA. Na Figura 15 é apresenta a taxonomia para os perigos a nível de sistema.

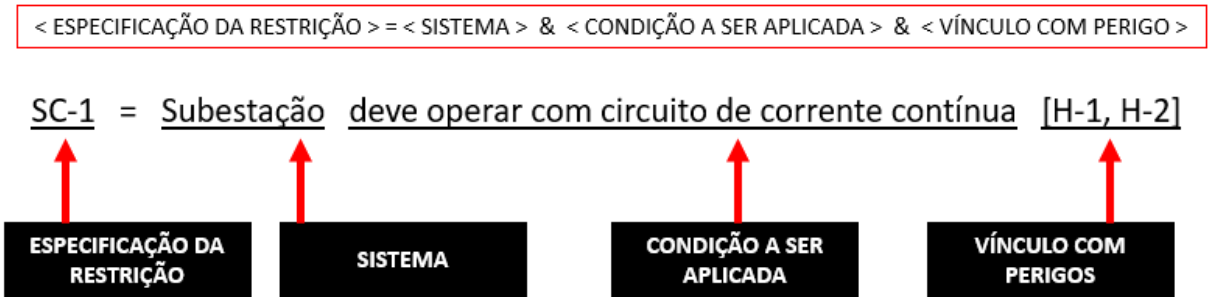
Figura 15 – Taxonomia para perigo a nível de sistema.



Fonte: Elaborado pelo autor.

Na Figura 16 é apresentada a estrutura para cadastro das restrições a nível de sistema.

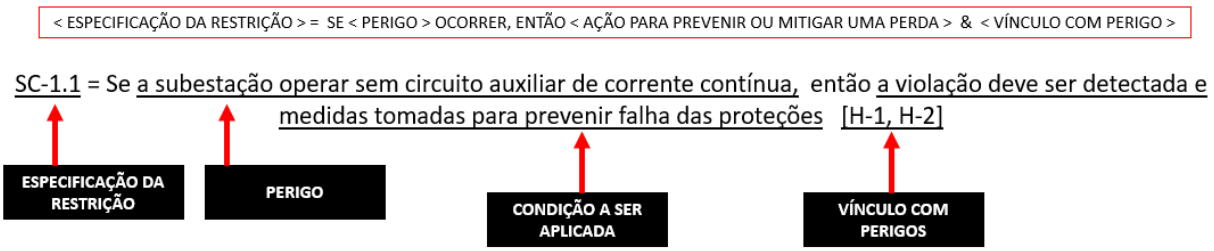
Figura 16 – Taxonomia geral para restrições a nível de sistema.



Fonte: Elaborado pelo autor.

Além das taxonomias supracitadas, a Figura 17 ilustra uma opção de modelo para restrições a nível de sistema que visem mitigar perdas.

Figura 17 – Alternativa de taxonomia para restrições a nível de sistema que mitigam perdas.

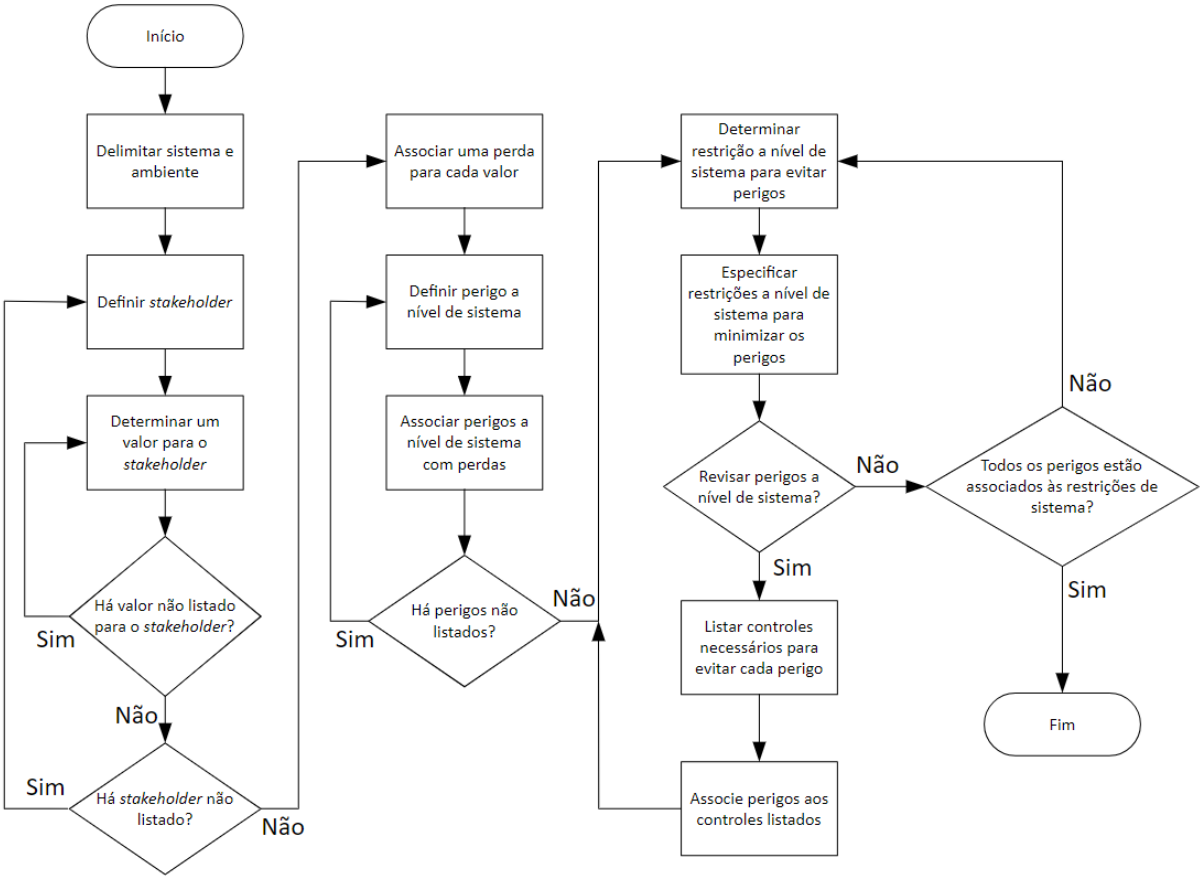


Fonte: Elaborado pelo autor.

A rastreabilidade não segue, necessariamente, uma correspondência de um para um. Tanto uma restrição pode ser aplicada para prevenir múltiplos perigos, quanto vários perigos

podem estar associados a uma única restrição. Além disso, cada perigo pode resultar em uma ou mais perdas (Leveson; Thomas, 2018). A Figura 18 sintetiza as ações necessárias para definição do propósito da análise.

Figura 18 – Fluxograma para definição do propósito da análise STPA.



Fonte: Elaborado pelo autor.

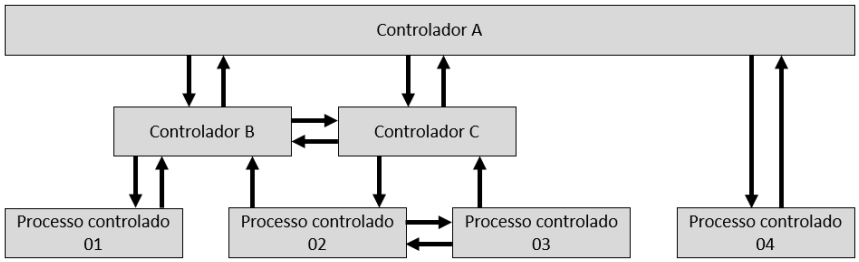
3.1.2 Modelagem da estrutura de controle

O próximo passo no STPA é modelar a estrutura de controle hierárquica, composta por *loops* de controle de retroalimentação, que impõem restrições ao comportamento do sistema. Os controladores possuem modelos de processo para tomar decisões, atualizados por meio de *feedback*. Múltiplos *loops* de controle interagindo podem ser modelados por meio de uma estrutura de controle hierárquica que contenha pelo menos cinco tipos de elementos, a saber: controladores, ações de controle, *feedback*, outras entradas/saídas e processos controlados (Leveson; Thomas, 2018).

A interação entre o controlador e o processo controlado fornece uma base para entender as interações complexas que podem levar a perdas. O eixo vertical em uma estrutura

de controle hierárquica indica a autoridade de controle dentro do sistema, onde cada entidade tem controle sobre as entidades abaixo dela e está sujeita à autoridade das entidades acima. As setas descendentes representam ações de controle, enquanto as setas ascendentes representam feedback. As setas horizontais representam outras informações que não expressam autoridade de controle entre emitente e receptor. Todas as conexões da estrutura de controle representam informações que podem ser transmitidas, sem necessariamente corresponderem a conexões físicas (Leveson; Thomas, 2018). Um loop de controle genérico é ilustrado na Figura 19.

Figura 19 – Estrutura hierárquica de controle genérica para STPA.



Fonte: Adaptado de Leveson e Thomas (2018).

O eixo vertical em uma estrutura de controle hierárquica indica a autoridade de controle dentro do sistema, onde cada entidade tem controle sobre as entidades abaixo dela e está sujeita à autoridade das entidades acima. As setas descendentes representam ações de controle, enquanto as setas ascendentes representam *feedback*. As setas horizontais representam outras informações que não expressam autoridade de controle entre emitente e receptor. Todas as conexões da estrutura de controle representam informações que podem ser transmitidas, sem necessariamente corresponderem a conexões físicas (Leveson; Thomas, 2018).

É importante notar que o STPA não presume obediência, pois o envio de uma ação de controle pelo controlador não garante que ela será seguida. Nesse sentido, um dos principais objetivos do STPA é analisar a estrutura de controle e antecipar comportamentos inseguros causados pelas ações de controle ou falta delas (Leveson; Thomas, 2018).

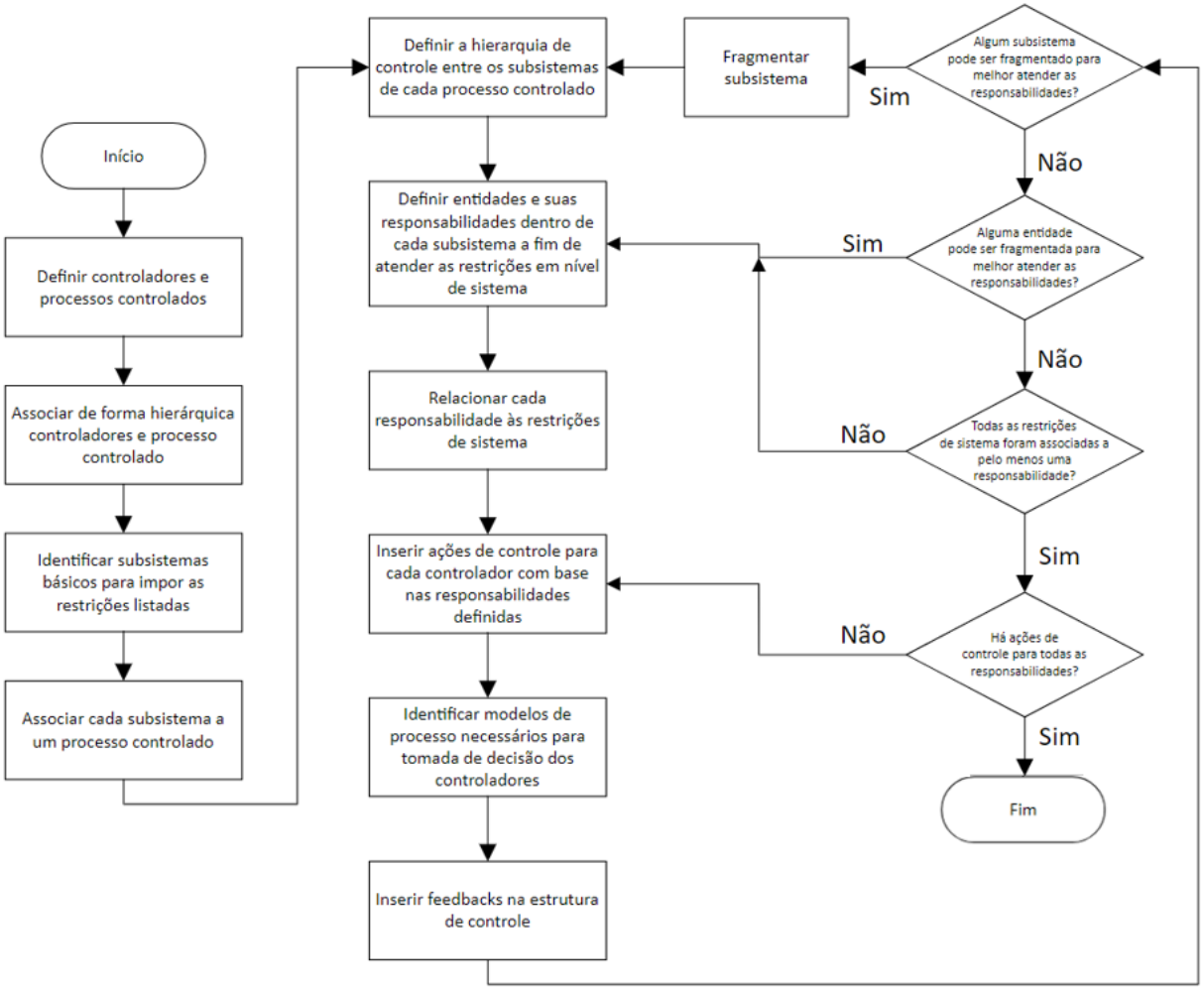
A modelagem começa abstrata e é detalhada gradualmente. Durante a modelagem da estrutura de controle, as responsabilidades são atribuídas a cada entidade para garantir o cumprimento das restrições a nível de sistema identificadas na primeira etapa do método (Leveson; Thomas, 2018).

As ações de controle são definidas com base nas responsabilidades. Já o *feedback* deriva das ações de controle e das responsabilidades, com base nos modelos de processo que os controladores precisam para tomar decisões. A estrutura de controle enfatiza relacionamentos e interações funcionais, úteis para identificar falhas de design, inconsistência de requisitos,

erros humanos e de software. Erros na hierarquia de controle não impactam significativamente a análise do STPA, uma vez que os próximos passos do método revelam as interações inseguras entre as entidades de controle (Leveson; Thomas, 2018).

A Figura 20 apresenta por meio de um fluxograma a sequência de ações realizadas para construção da estrutura de controle do sistema de proteção e controle de uma subestação industrial.

Figura 20 – Fluxograma para construção de uma estrutura de controle STPA.



Fonte: Elaborado pelo autor.

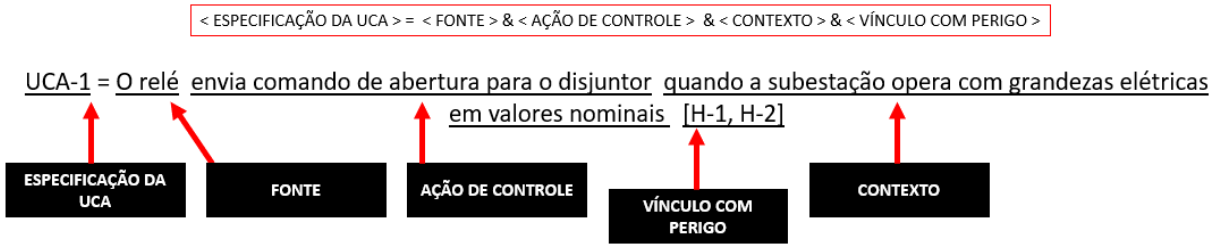
3.1.3 Identificação das ações de controle inseguras

Uma vez modelada a estrutura de controle, o próximo passo é identificar as *Unsafety Control Actions* (UCAs). Uma UCA é uma ação de controle que, em um contexto específico e em um cenário de pior caso, resultará em perigo. Qualquer contexto relevante pode

ser referenciado em uma UCA, incluindo condições ambientais (Leveson; Thomas, 2018).

Em Leveson e Thomas (2018), os autores recomendam usar expressões como "quando", "enquanto" ou "durante" ao formular uma UCA para desenvolver o contexto. Uma taxonomia para registrar UCAs é apresentada na Figura 21, sendo a ordem das partes do texto não crítica, desde que todas as cinco partes sejam incluídas no registro da UCA.

Figura 21 – Taxonomia para ações de controle inseguras no STPA.



Fonte: Elaborado pelo autor.

Existem quatro maneiras pelas quais uma ação de controle pode ser insegura dado um contexto específico: quando sua ausência leva a um perigo; quando sua realização leva a um perigo; quando é realizada de forma inadequada, como muito cedo, muito tarde ou fora de ordem; e quando é mantida por muito tempo ou interrompida precocemente. Cada UCA deve ser associada a um ou mais perigos (Leveson; Thomas, 2018).

O objetivo do STPA não é avaliar a probabilidade de cenários de melhor ou pior caso ou presumir as capacidades e respostas dos operadores, mas sim identificar os comportamentos a serem evitados (Leveson; Thomas, 2018).

Em um cenário de melhor caso, as proteções de retaguarda funcionam conforme esperado e o perigo é evitado. Por outro lado, em um cenário de pior caso, as proteções de retaguarda podem falhar, ser insuficientes ou ineficazes para a situação (Leveson; Thomas, 2018).

O STPA identifica as UCAs a serem evitadas, e elas são usadas para derivar requisitos funcionais e decisões de design para prevenir ou mitigar essas UCAs. Uma vez identificado o comportamento potencialmente inseguro, características de *design* específicas podem ser desenvolvidas e retaguardas adicionadas se a proteção ainda não existir, ou a adequação das decisões de design existentes e das retaguardas podem ser avaliadas se a filosofia de controle já estiver em vigor (Leveson; Thomas, 2018).

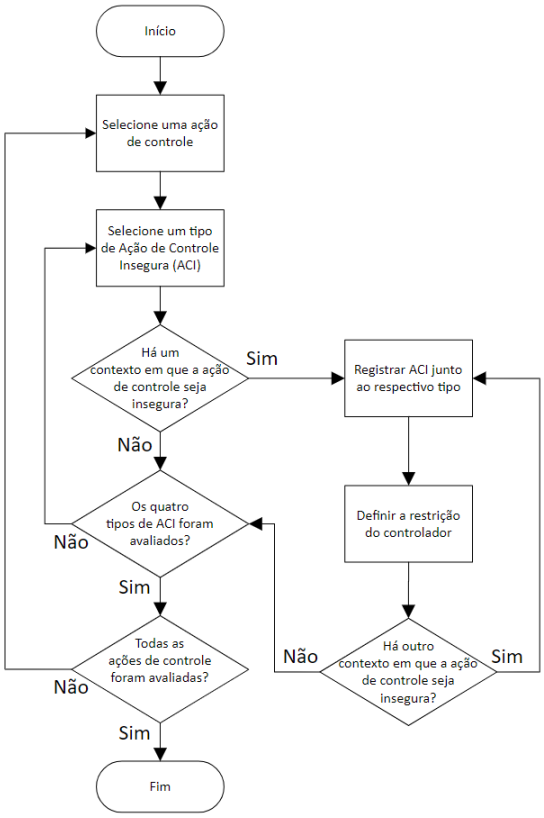
É importante destacar que o STPA é um processo iterativo e não precisa ser seguido de maneira linear. Resultados anteriores podem ser atualizados conforme a análise avança e mais informações se tornam disponíveis. Dentro desse método, seres humanos são tratados da

mesma forma que outros componentes do sistema e podem ser facilmente integrados à análise geral (Leveson; Thomas, 2018).

Após a identificação das UCAs, elas podem ser traduzidas em restrições sobre o comportamento de cada controlador. Uma restrição do controlador determina os comportamentos que o controlador deve seguir para prevenir UCAs (Leveson; Thomas, 2018).

A Figura 22 sintetiza as etapas necessárias para definição as ações de controle inseguras.

Figura 22 – Fluxograma para definição de ações de controle inseguras no STPA.



Fonte: Elaborado pelo autor.

3.1.4 Identificação dos cenários de perda

O cenário de perda descreve os fatores causais que podem resultar em ações de controle inseguras e perigos. Existem dois tipos de cenários de perda: aqueles que explicam por que ocorrem as Ações de Controle Inseguras, destacando sensores e controladores, e aqueles que abordam por que as ações de controle são executadas incorretamente ou não são executadas, considerando atuadores e o processo controlado (Leveson; Thomas, 2018).

Identificar contextos que levam às ações de controle inseguras requer foco no

comportamento inseguro do controlador e em *feedbacks* e informações inadequadas. Avaliando o comportamento inseguro do controlador, há quatro tipos de falha: falha física no controlador, algoritmo de controle inadequado, entrada de controle insegura e modelo de processo inadequado. Para controladores humanos, o algoritmo de controle representa a tomada de decisão, moldada por fatores como treinamento e experiência (Leveson; Thomas, 2018).

Na avaliação de *feedbacks* e informações inadequadas, é essencial identificar sua origem para explicar possíveis problemas. As principais causas incluem mensagens incorretas ou a falta delas nos controladores, falhas no meio de comunicação e ataques cibernéticos (Leveson; Thomas, 2018).

No segundo cenário, cada ação de controle é examinada quanto a falhas nos atuadores e no processo controlado. Falhas nos atuadores podem ocorrer devido a não execução ou execução incorreta das ações de controle. Além disso, ações de controle podem ser executadas erroneamente devido a informações incorretas ou ausentes, respostas inadequadas do controlador ou atuações independentes dos atuadores (Leveson; Thomas, 2018).

3.2 Software Capella para análise STPA

Existem diversas ferramentas para a aplicação do método STPA, tanto em versões comerciais quanto gratuitas. O Instituto de Tecnologia de Massachusetts (MIT) lista as ferramentas conhecidas para a implementação deste método em MIT ([s. d.]). Entre as opções gratuitas, o software Capella foi escolhido para este trabalho devido à disponibilidade de manuais e à execução do software no ambiente de desenvolvimento Eclipse.

O Capella versão 6.1 implementa o método Arcadia (do inglês, *Architecture Analysis and Design Integrated Approach*) por meio de uma metodologia consolidada para aplicações industriais, sendo capaz de utilizar modelos gráficos para definir, analisar, projetar e validar arquiteturas de sistemas (Roques, 2016).

Arcadia é um método de engenharia baseado em modelo para o projeto arquitetônico de sistemas, hardware e software, desenvolvido pela Thales Group entre 2005 e 2010 através de um processo iterativo envolvendo arquitetos operacionais de todos os domínios de negócios da empresa (Roques, 2016).

O método Arcadia segue cinco etapas. A primeira fase é concentrada na análise das necessidades e objetivos do cliente, indo além dos requisitos do sistema. A segunda etapa foca no próprio sistema, definindo como é possível satisfazer as necessidades operacionais, comportamento e qualidades esperadas. Já a terceira fase detalha os componentes do sistema

com base nas decisões de engenharia. A quarta etapa visa construir a arquitetura lógica final do projeto, enquanto a quinta etapa contribui para uma estrutura analítica do produto final e modelos que descrevem a especificação de cada subsistema, componente de hardware ou software, formalizando a definição dos requisitos dos componentes do sistema (Roques, 2016).

O método Arcadia, executado através da ferramenta Capella, aproveita a abordagem de cima para baixo, começando pela necessidade operacional do sistema para definir e validar requisitos, construindo uma arquitetura lógica neutra em tecnologia para, em seguida, especificar funções e serviços técnicos de uma arquitetura física para sua implementação (Roques, 2016).

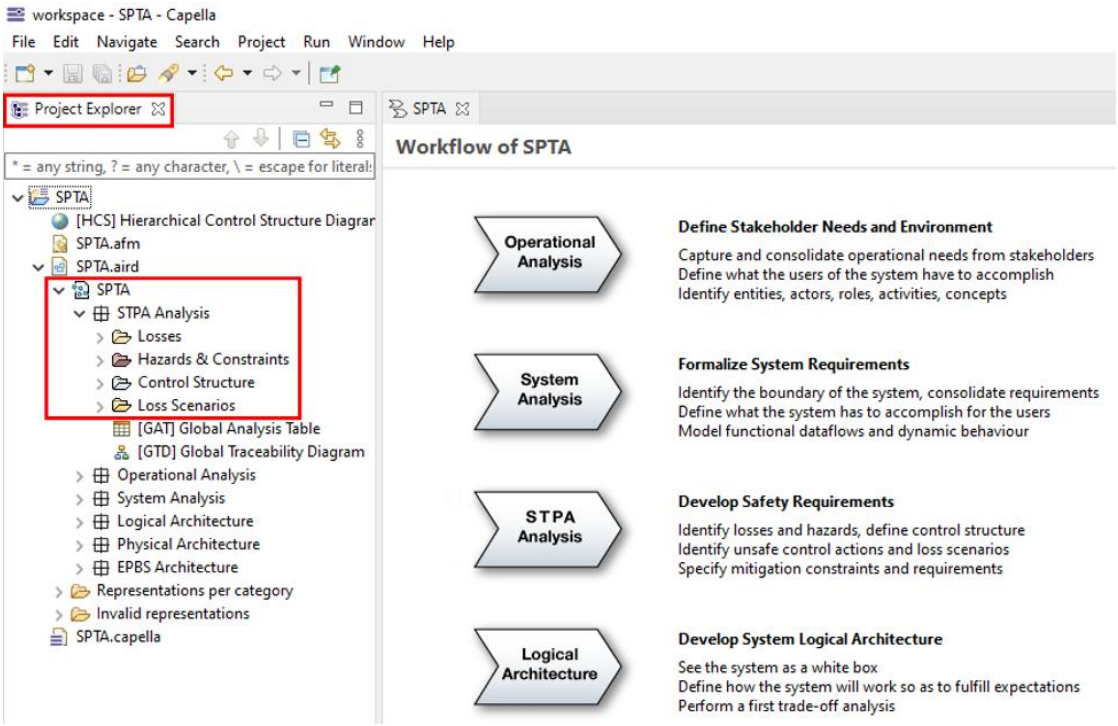
O software Capella é uma ferramenta de modelagem *Model-Based Systems Engineering* (MBSE) de código aberto que implementa o método Arcadia no ambiente de desenvolvimento Eclipse. A abordagem MBSE consiste em usar uma linguagem formal para especificar, projetar e analisar sistemas, garantindo rastreabilidade nesse processo. Ele possui um ecossistema de especialistas e provedores de tecnologia que oferecem suporte, integração e ferramentas complementares (*add-ons*) (Roques, 2016).

Uma das extensões do Capella é o STPA, disponível gratuitamente em Capella (Labs for Capella, [202-?]) por meio da plataforma GitHub. A Figura 23 apresenta o ambiente de trabalho desse software. Ao aplicar o método STPA, o usuário insere os dados específicos do STPA nos elementos do modelo Arcadia. Esses dados são organizados em uma seção dedicada do Capella, abaixo do elemento STPA *Analysis*, visível na guia *Project Explorer*.

Cada seção contém uma tabela que relaciona diferentes elementos do STPA, tais como perdas, perigos a nível de sistema, responsabilidades e ações de controle. A Figura 24 mostra a tabela de perdas adotada neste trabalho, relacionando com os valores da indústria e os perigos a nível de sistema.

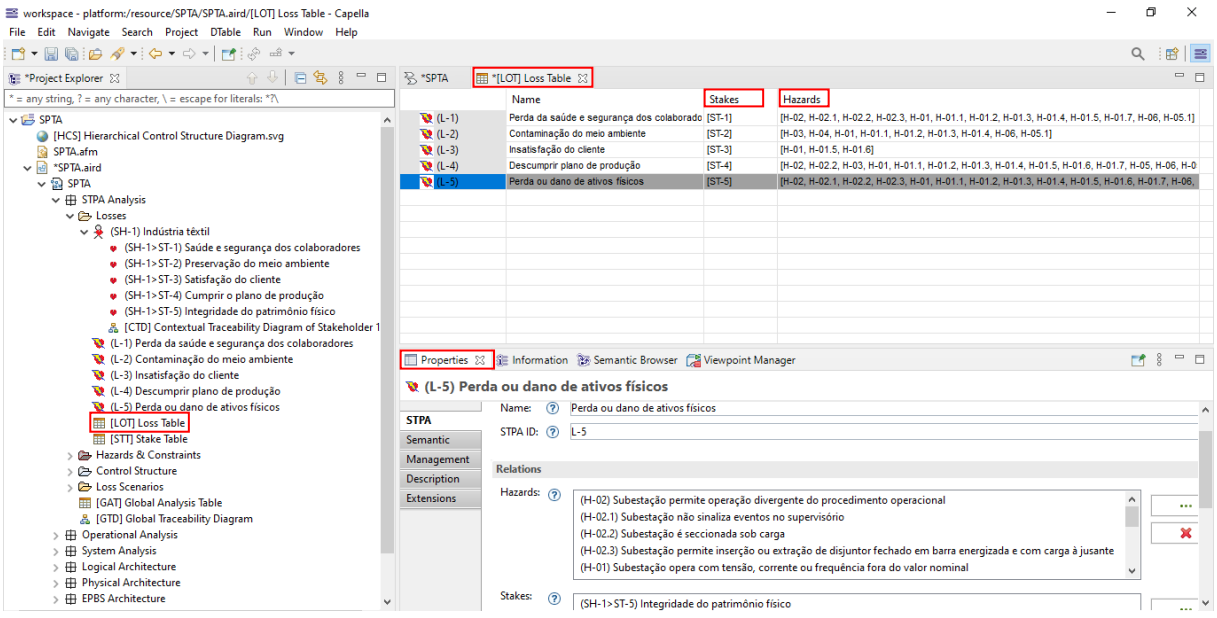
As informações de cada elemento do modelo devem ser inseridas na guia “Propriedades”, aberta quando um elemento é selecionado em uma tabela ou diagrama. A Figura 25 mostra um exemplo para inserção de dados referentes a um perigo a nível de sistema. Inicialmente, são inseridos nome e código de identificação para o elemento selecionado. Na sequência, há campos disponíveis para relacionar o elemento selecionado às demais entidades.

Figura 23 – Ambiente de modelagem do software Capella Eclipse.



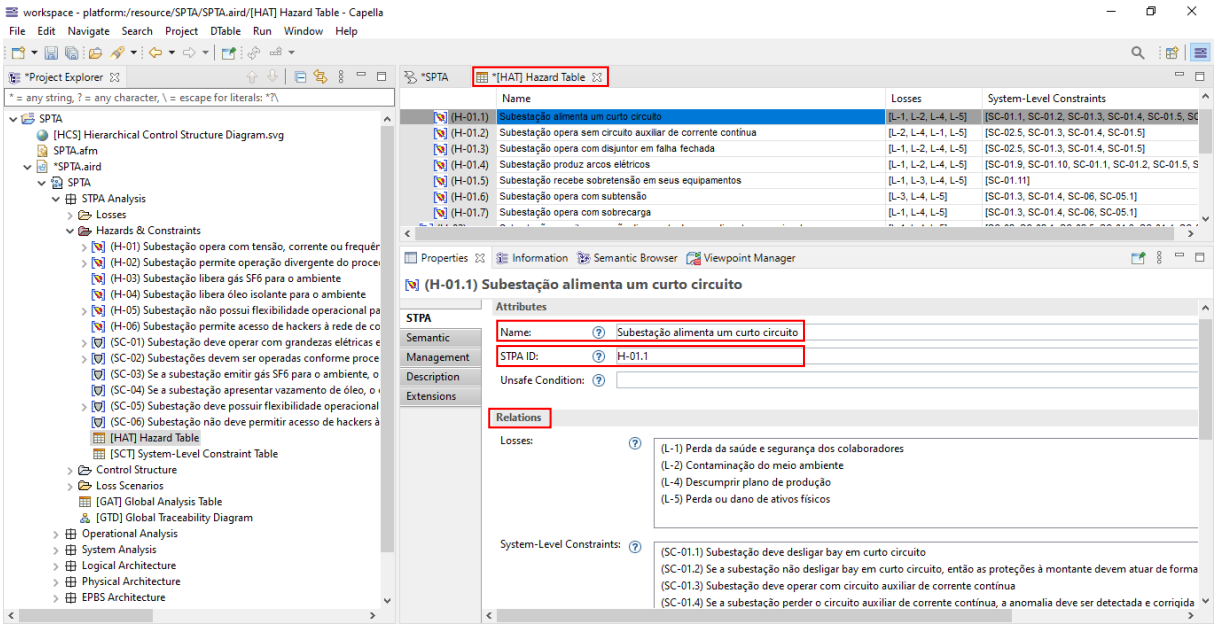
Fonte: Adaptado de Capella (versão 6.1, [202-?]).

Figura 24 – Tabela de perdas no software Capella.



Fonte: Adaptado de Capella (versão 6.1, [202-?]).

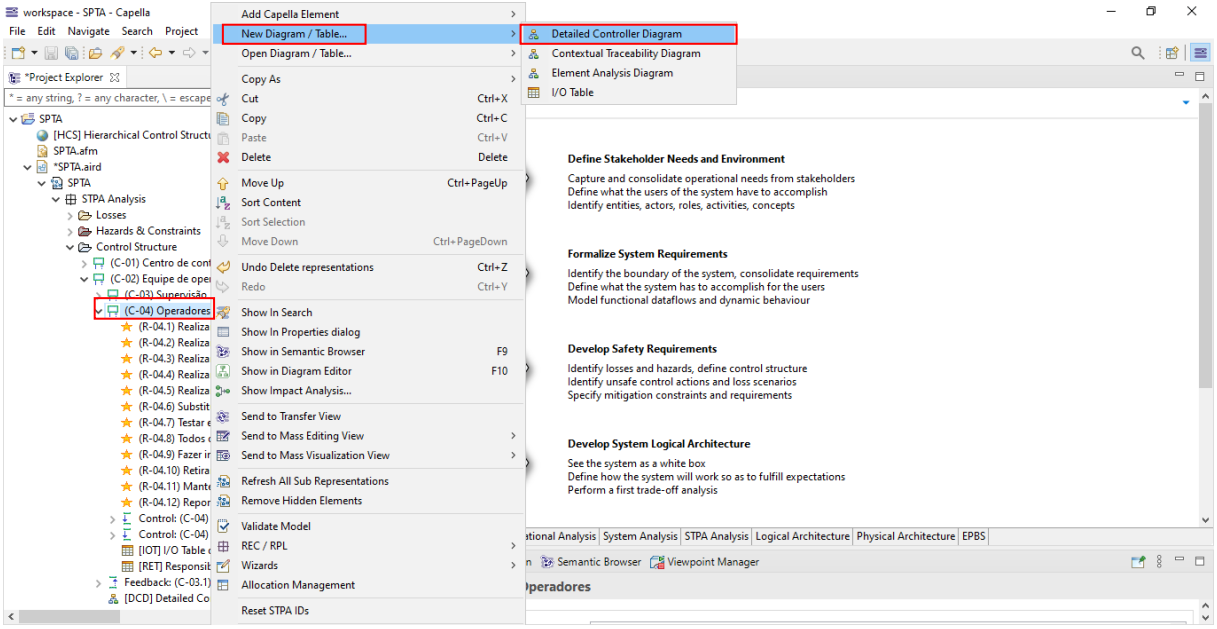
Figura 25 – Inserção de um perigo a nível de sistema no software Capella.



Fonte: Adaptado de Capella (versão 6.1, [202-?]).

É possível gerar um diagrama de controle detalhado para cada elemento do Capella, conforme Figura 26. Tais diagramas exibem de forma sintética os dados atribuídos ao elemento do modelo, tais como responsabilidades, modelos de processos, ações de controle e restrições a nível de controlador.

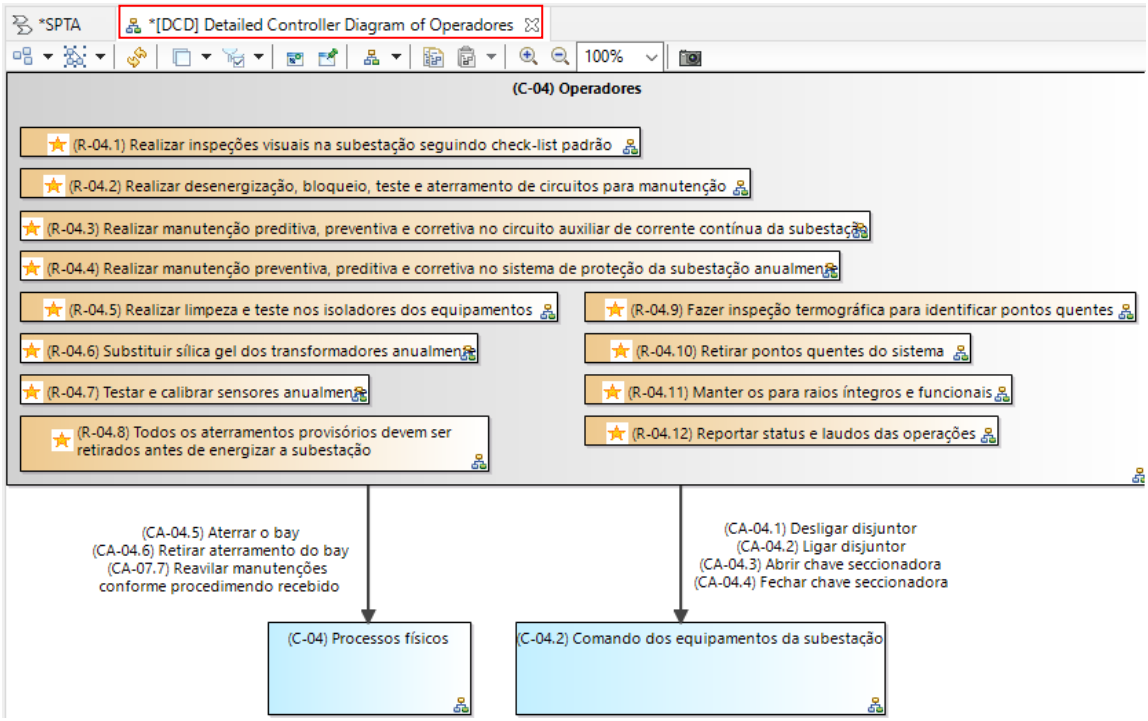
Figura 26 – Caminho para gerar um diagrama de controle detalhado no software Capella.



Fonte: Adaptado de Capella (versão 6.1, [202-?]).

A Figura 27 exemplifica o diagrama de controle detalhado elaborado para os operadores locais da subestação, destacando doze responsabilidades deste controlador, bem como as ações de controle que ele executa sob os processos físicos, como aterrar um bay, e sob o painel de comando dos equipamentos de campo, como desligar um disjuntor de forma local.

Figura 27 – Diagrama de controle detalhado para operadores locais no software Capella.



Fonte: Adaptado de Capella (versão 6.1, [202-?]).

3.3 Considerações finais

As quatro fases do STPA foram ilustradas por meio de fluxogramas, bem como o software Capella Eclipse, utilizado como ferramenta para aplicar o procedimento metodológico e avaliar, sob a perspectiva de segurança operacional, a proposta de digitalização de uma subestação industrial conforme padrão IEC 61850.

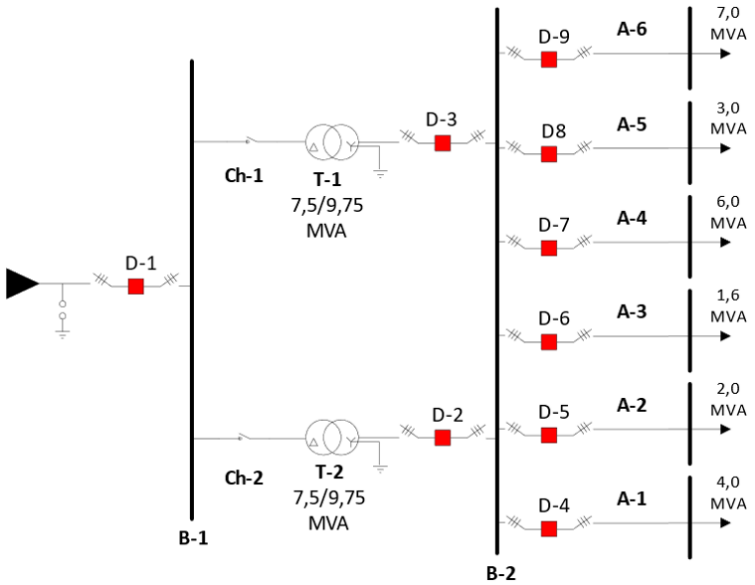
4 PROPOSTA DE AVALIAÇÃO DE SEGURANÇA EM SUSBESTAÇÃO DIGITAL UTILIZANDO SPTA

Este capítulo apresenta a subestação de uma indústria têxtil com filosofia de proteção cronométrica, destacando as limitações operacionais no âmbito de segurança. Na sequência, a proposta de digitalização é delineada para definir a amplitude do método STPA na avaliação de segurança da subestação. Por fim, o STPA é aplicado à proposta de digitalização das proteções da subestação a fim de evidenciar requisitos de segurança e motivar testes laboratoriais.

4.1 Cenário atual da subestação

O sistema elétrico escolhido para aplicação da metodologia deste trabalho é a subestação 69-13,8 kV de uma indústria têxtil. Tal subestação possui dois transformadores de 7,5/9,75 MVA. A Figura 28 apresenta o diagrama unifilar desta subestação.

Figura 28 – Diagrama unifilar simplificado da subestação industrial.



Fonte: Elaborado pelo autor.

A subestação é equipada com um disjuntor geral D-1 e duas chaves seccionadoras em 69 kV, uma para cada transformador de potência (T1 e T2), além de dois disjuntores, denominados de D-2 e D-3, em 13,8 kV. Os transformadores trabalham em paralelo de forma permanente. Além disso, há seis disjuntores, identificados de D-4 a D-9, todos operando em 13,8 kV, responsáveis por seccionar os alimentadores de A-1 a A-6.

As tecnologias empregadas nesta subestação se alinham parcialmente aos requisitos convencionais e, em parte, aos requisitos de um estágio inicial de digitalização, conforme classificação proposta por Santos et al. (2024) e sintetizada no Quadro 1.

O atual cenário de proteção e controle da subestação não possui rede de comunicação, apenas sinais analógicos emitidos por transformadores de instrumento convencionais via cabos de cobre. Embora a proteção seja realizada por IEDs, os dispositivos não são integrados à sistema SCADA. Tanto a coleta como a análise de dados são feitas de forma manual. A equipe operacional possui competências técnicas em eletromecânica e eletrônica, e realiza manutenções preventivas e corretivas.

As funções de proteção ANSI ativas nos relés limitam-se a sobrecorrente instantânea, função 50, e sobrecorrente temporizada, função 51. Os relés que realizam a proteção dos transformadores contam com a função diferencial 87T.

O estudo de coordenação e seletividade das proteções é de propriedade da indústria. Contudo, a Tabela 1 sintetiza os dados da Ordem de Ajuste das Proteções (OAP) para as funções de sobrecorrente de cada relé de proteção, tanto para fase quanto para neutro.

Tabela 1 – OAP para subestação industrial

Ordem de Ajuste das Proteções												
Equipamento	Tensão (kV)	RTC	I pick-up (A)	ANSI	Proteção	Fabricante/modelo	Regulação		Graduação			
							Temporizado	Instantaneo	Tape	Curva	Inst.	Tipo Curva
Relé RS1 Disjuntor D-1	69	600/5	150	50/51	FASE	ABB/REX521	(0,10 a 5,0) x In T - 0,05 a 15,0s	(0,10 a 40) x In T - 0,05 a 300s	0,25	0,5	5,24 (3144) T>>=0,1s	MI IEC
			6000	50/51N	NEUTRO		(0,01 a 5,0) x In T - 0,05 a 15,0s	(0,10 a 12) x In T - 0,05 a 300s	10	0,55	1,8 (1080) T>>=0,1s	MI IEC
Relé RS2 e RS3 Disjuntor D-2 e D-3	13.8	300/5	345	50/51	FASE	ABB/RET615	(0,05 a 5,0) x In T - 0,05 a 15,0s	(0,10 a 40) x In T - 0,04 a 200s	1,15	0,3	OFF	MI IEC
			105	50/51N	NEUTRO				0,35	0,6	3,5 (1065) T>>=0,08s	MI IEC
Relé RS4 e RS5 Disjuntor D-4 e D-5 (Saída 1 e 2)	13.8	300/5	330	50/51	FASE	ABB/REF610	(0,05 a 5,0) x In T - 0,05 a 15,0s	(0,10 a 40) x In T - 0,04 a 200s	1,1	0,35	12 (3600) T>>=0,08s	MI IEC
			102	50/51N	NEUTRO		(0,01 a 5,0) x In T - 0,05 a 15,0s	(0,10 a 40) x In T - 0,04 a 200s	0,34	0,55	3,6 (1080) T>>=0,07s	MI IEC
Relé RS6 Disjuntor D-6 (Saída 3)	13.8	400/5	80	50/51	FASE	ABB/REF610	(0,05 a 5,0) x In T - 0,05 a 15,0s	(0,10 a 40) x In T - 0,04 a 200s	0,2	0,9	2 (800) T>>=0,05s	MI IEC
			24	50/51N	NEUTRO		(0,01 a 5,0) x In T - 0,05 a 15,0s	(0,10 a 40) x In T - 0,04 a 200s	0,06	0,55	1 (400) T>>=0,05s	MI IEC
Relé RS7 e RS8 Disjuntor D-7 e D-8 (Saída 4 e 5)	13.8	300/5	330	50/51	FASE	ABB/REF610	(0,05 a 5,0) x In T - 0,05 a 15,0s	(0,10 a 40) x In T - 0,04 a 200s	1,1	0,45	12 (3600) T>>=0,08s	MI IEC
			102	50/51N	NEUTRO		(0,01 a 5,0) x In T - 0,05 a 15,0s	(0,10 a 40) x In T - 0,04 a 200s	0,34	0,55	3,6 (1080) T>>=0,07s	MI IEC
Relé RS9 Disjuntor D-9 (Saída 6)	13.8	300/5	460	50/51	FASE	ABB/REF610	(0,05 a 5,0) x In T - 0,05 a 15,0s	(0,10 a 40) x In T - 0,04 a 200s	0,92	0,26	5,5 (2750) T>>=0,08s	MI IEC
			120	50/51N	NEUTRO		(0,01 a 5,0) x In T - 0,05 a 15,0s	(0,10 a 40) x In T - 0,04 a 200s	0,24	0,39	1,8 (900) T>>=0,07s	MI IEC

Fonte: Elaborado pelo autor.

Uma forma de verificar se a coordenação está adequada é avaliar as curvas de atuação dos relés por meio de coordenogramas gráficos. Não deve haver interceptação entre as curvas e uma diferença de tempo entre elas deve ser adotada como margem de coordenação (Sharaf *et al.*, 2015).

Todas as curvas da OAP seguem o padrão IEC com tipo muito inverso. Em Sharaf *et al.* (2015), a função matemática para esse tipo de curva é dada pela Equação (4.1)

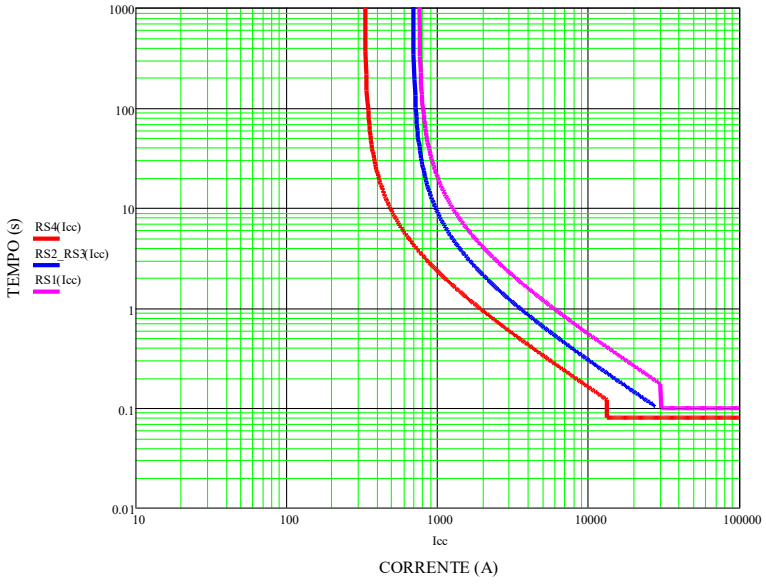
$$t = \frac{13{,}5}{\frac{I_{cc}}{I_{pk}} - 1} * DT \tag{4.1}$$

em que:

- t = tempo de atuação;
- Icc = corrente de curto-circuito;
- Ipk = corrente de *pick-up*;
- DT = múltiplo de tempo.

Nesse sentido, é elaborado o coordenograma das proteções que atuam na zona de proteção do alimentador A-1 com base na OAP fornecida. As curvas foram plotadas tendo como referência a barra de 13,8 kV e são exibidas na Figura 29. A zona de proteção do alimentador A-1 foi escolhida, pois supre a energia de um importante grupo de processos dessa indústria.

Figura 29 – Coordenograma dos relés conforme dados da OAP.



Fonte: Elaborado pelo autor.

A primeira curva, em vermelho, representa o relé RS4 associado ao disjuntor D-4, enquanto a segunda, em azul, representa uma síntese dos relés de saída de cada transformador de potência RS2-RS3. Já a terceira curva, em rosa, corresponde ao relé RS1 localizado na fronteira com a concessionária de energia. O ajuste de RS1 é determinado no estudo de coordenação e seletividade para que mantenha margem de coordenação mínima de 300 ms com o relé da concessionária de energia.

O nível de curto-circuito na barra B-2 é de 9,3 kA, conforme dados informados pela indústria têxtil em seu estudo de coordenação e seletividade. Esse valor pode ser referenciado para a barra B-1 dividindo-o pela relação de transformação dos transformadores de potência. Como os transformadores de potência são abaixadores de tensão, de 69 kV para 13,8 kV, a relação de transformação é igual a 5. Dessa forma, o curto-circuito na barra B-2 gera um fluxo de 1,86 kA na barra B-1. Essa corrente pode ser aplicada na Equação (4.1) em conjunto com os ajustes da OAP referentes ao relé RS1, a fim de encontrar o tempo de atuação do relé de entrada da subestação para uma falta na barra B-2. O resultado de tal aplicação pode ser observado em (4.2)

$$t = \frac{13{,}5}{\frac{1860}{150} - 1} * 0{,}5 = 0{,}592\ s. \tag{4.2}$$

Nesse mesmo cenário de curto-circuito, o valor de corrente percebida pelos relés dos transformadores é metade do valor observado na barra B-2, uma vez que os transformadores estão em paralelo e possuem a mesma impedância. Dessa forma, o tempo de atuação do relé RS2 e RS3 segue a Equação (4.3)

$$t = \frac{13{,}5}{\frac{4650}{345} - 1} * 0{,}3 = 0{,}325\ s. \tag{4.3}$$

Já para o RS4, o tempo de atuação é de 80 milissegundos para correntes de curto-circuito superiores a 3600 A, devido à atuação de sua função 50 instantânea. Curto-circuito na mufla dos cabos do alimentador A-1, por exemplo, geram níveis de curto equivalente ao curto da barra B-2, uma vez que não há impedância significativa entre esses pontos.

Portanto, no cenário de curto-circuito no início do alimentador A-1, com base na Tabela 1, é esperado que a proteção principal exercida por RS4 atue em 80 milissegundos. Caso

haja falha nesta proteção, o relé RS2 e RS3 atuarão como proteção de retaguarda em 325 milissegundos. Por fim, o relé RS1 aguardará 592 milissegundos para eliminação do defeito. Caso contrário, RS1 atua e desliga toda a subestação.

O responsável técnico assume tempo de 27 milissegundos para o sinal de comando chegar ao disjuntor, abertura do disjuntor em 240 milissegundos, devido a obsolescência dos equipamentos, compondo uma margem de coordenação de 267 milissegundos para realizar a coordenação entre os relés de entrada da subestação e dos transformadores.

4.2 Proposta de seletividade lógica padrão IEC 61850

Com a ascensão da Indústria 4.0, o setor elétrico adotou diversas tecnologias digitais que aprimoraram os processos de proteção dos sistemas elétricos. Esses avanços seguem os seis princípios fundamentais da quarta revolução industrial, a saber: interoperabilidade, Internet das Coisas (IoT), virtualização, coleta de dados em tempo real, descentralização e modularização (Hall; Schumacher; Bildstein, 2022).

O estado da arte das tecnologias de subestação é suficiente para inserir os conceitos da Indústria 4.0 em sistemas de energia. Para tanto, é proposto uso de IEDs conectados em rede de comunicação padrão IEC 61850, monitorados em tempo real por sistema SCADA com acesso remoto. Os transformadores de instrumentos podem ser mantidos. A equipe de operação precisa ser treinada em competências elétricas e de rede de computadores. Além disso, o plano de manutenção precisa englobar programações preditivas.

Com esses requisitos atendidos, torna-se viável funcionalidades como corte de cargas automático, detecção de falha de disjuntor e monitoramento remoto em tempo real dos status dos equipamentos e das grandezas elétricas.

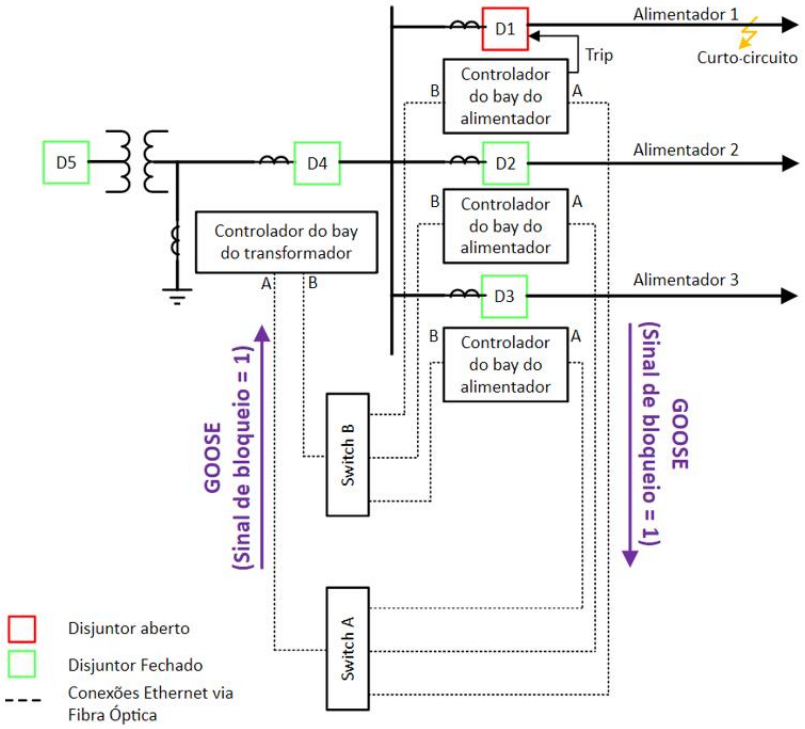
Nesse contexto, uma nova filosofia de proteção emerge, com o advento da IEC 61850, não mais baseado em tempo, e sim em lógicas de programação. Todos os sinais analógicos e digitais do sistema passam a ser disponibilizados na rede através dos IEDs. Informações como atuações de proteções intrínsecas dos transformadores de potência e status operacionais dos componentes da subestação são utilizados para projeto de restrições a nível de sistema, garantindo intertravamentos lógicos de segurança para a operação da subestação.

Um esquema de seletividade lógica tem como objetivo responder de forma rápida e coordenada a ocorrência de faltas em uma subestação. Essa abordagem não apenas melhora a segurança das equipes de trabalho, mas também minimiza os danos causados pela falta e prolonga o tempo de vida útil dos equipamentos da subestação (Kimura *et al.*, 2010).

Para implementar a seletividade lógica, cada proteção deve ser capaz de se comunicar com as proteções tanto a jusante quanto a montante por meio de um sinal digital, além de acionar o dispositivo de abertura do circuito. A comunicação entre os relés pode ser realizada por mensagens GOOSE, utilizando o protocolo IEC 61850. Dessa forma, quando um relé recebe a informação de que o relé a jusante está sensibilizado por uma falta, ele deve bloquear apenas a atuação de suas funções instantâneas. As funções temporizadas dos relés devem atuar como uma retaguarda da proteção do relé a jusante, em caso de falha no sistema de comunicação.

A Figura 30 ilustra a operação de um sistema de proteção com seletividade lógica padrão IEC 61850. Quando ocorre uma falta no alimentador A-1, o relé sensibilizado envia um sinal ao relé situado a montante que, caso também esteja sensibilizado, bloqueia a atuação de sua função instantânea.

Figura 30 – Seletividade lógica com comunicação baseada na IEC 61.850.

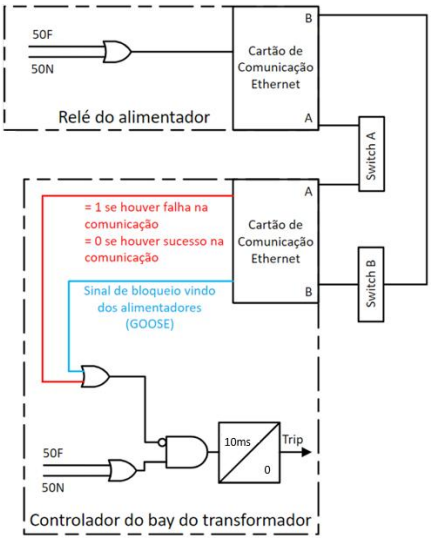


Fonte: Elaborado pelo autor.

A Figura 31 apresenta um diagrama do esquema de seletividade lógica com o uso da mensagem GOOSE. Nesse esquema, quando ocorre uma falta no alimentador, tanto o relé do alimentador quanto o controlador do *bay* do transformador são sensibilizados. Para garantir a coordenação, o controlador do transformador recebe dois sinais de comando: o sinal de bloqueio enviado pelo relé e o sinal de integridade da rede de comunicação. Se não houver sinal

de bloqueio, a rede de comunicação estiver íntegra e o controlador estiver sensibilizado, ocorrerá um sinal de *trip* após uma temporização de 10 milissegundos. Esse atraso de tempo na função instantânea garante o recebimento do sinal de bloqueio antes da atuação da proteção.

Figura 31 – Lógica do esquema de seletividade com uso de mensagem GOOSE.



Fonte: Elaborado pelo autor.

Ao implementar a IEC 61850 à subestação, todos os comandos e intertravamentos podem ser realizados de forma digital, além de executar operações de forma remota. Nesse novo cenário, a subestação assume a configuração de um sistema ciber-físico complexo. As interações entre equipes operacionais, equipamentos de potência, rede de comunicação e lógicas de proteção e controle dos IEDs geram novos cenários inseguros que precisam ser conhecidos e avaliados, a fim de garantir a segurança operacional do sistema.

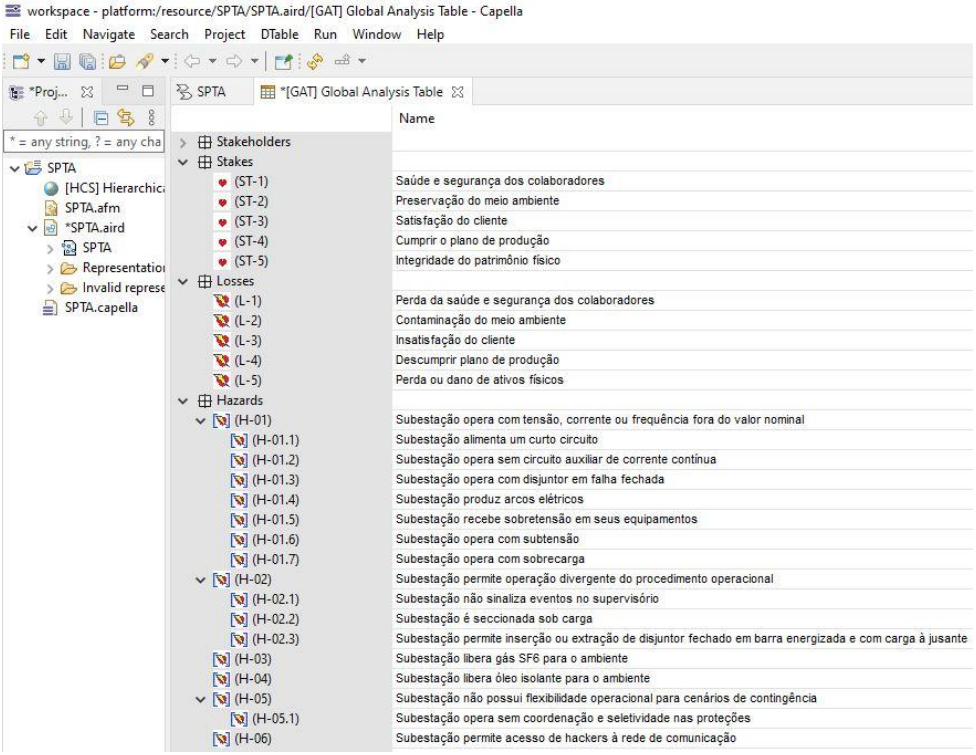
4.3 Uso de STPA em subestação digital

O STPA é aplicado à proposta de digitalização da subestação industrial por meio do software Capella versão 6.1. Os quatro passos do método são realizados, a saber: definição do propósito da análise, modelagem da estrutura de controle, especificação de ações de controle inseguras e identificação de cenários de perda (Leveson; Thomas, 2018).

O sistema é delimitado pela área física da subestação industrial 69/13,8 kV, compreendendo o pátio da subestação, onde ficam todos os equipamentos a montante da barra B-2, e a casa de comando, onde os cubículos de média tensão estão instalados junto com todos os relés.

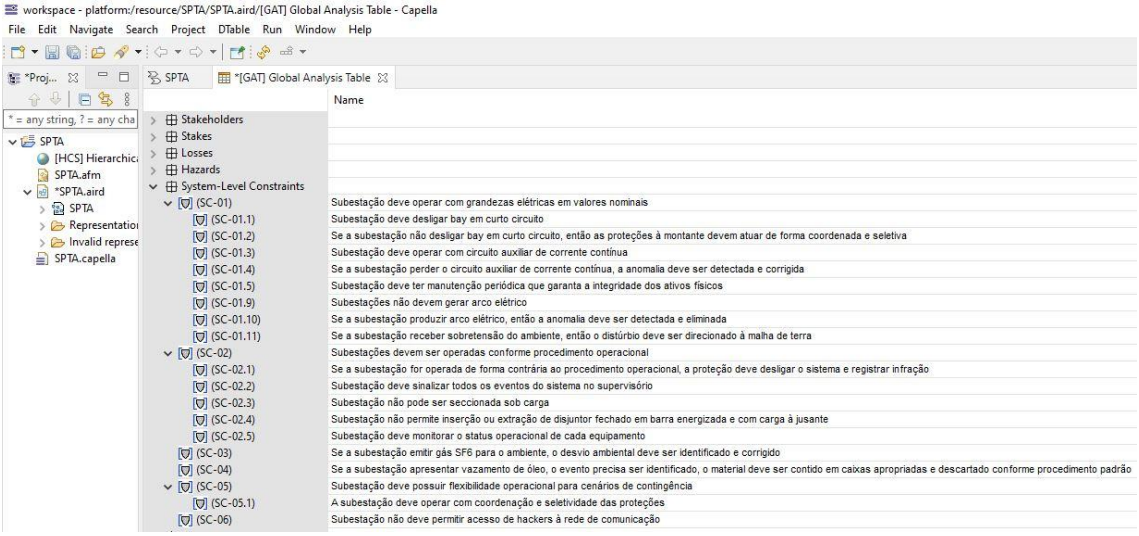
Para a definição do propósito da análise, os valores da empresa têxtil foram usados, tais como preservação do meio ambiente, perda de produção e integridade física dos colaboradores. A Figura 32 mostra os valores, perdas e perigos a nível de sistema inseridos no Capella. Já a Figura 33 apresenta as restrições a nível de sistema necessárias para evitar perdas. Essas informações são inseridas no software Capella para o início da modelagem.

Figura 32 – Definição das perdas e perigos a nível de sistema.



Fonte: Adaptado de Capella (versão 6.1, [202-?]).

Figura 33 – Definição das restrições a nível de sistema.



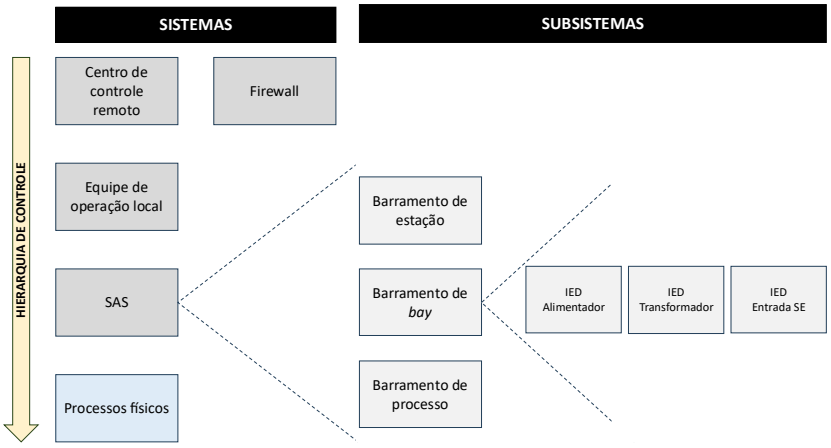
Fonte: Adaptado de Capella (versão 6.1, [202-?]).

Os perigos a nível de sistema e as restrições a nível de sistema são determinadas conforme taxonomia apresentada respectivamente na Figura 15 e Figura 16. Além disso, são mantidos prefixos em todos os elementos do modelo a fim de garantir a rastreabilidade do processo.

O prefixo “H” (do inglês, *Hazard*) é utilizado para perigos em nível de sistema, enquanto que “SC” (do inglês, *System-level Constraint*) é associado a restrições a nível de sistema. Outros prefixos são adotados, tais com “L” (do inglês, *Loss*), “R” para responsabilidades dos controladores, “FB” para *feedbacks*, “CA” (do inglês, *Control Action*) para ações de controle e “UCA” (do inglês, *Unsafe Control Actions*).

A construção da estrutura geral de controle da subestação começa com um grupo de processos controlados e quatro controladores abrangentes: centro de controle remoto, firewall, sistema de automação da subestação e equipe operacional. Nesse trabalho, a modelagem da estrutura de controle é restrita ao sistema de automação da subestação, enfatizando o barramento de interbay conforme ilustrado na Figura 34.

Figura 34 – Amplitude da aplicação do método STPA adotada no estudo de caso.

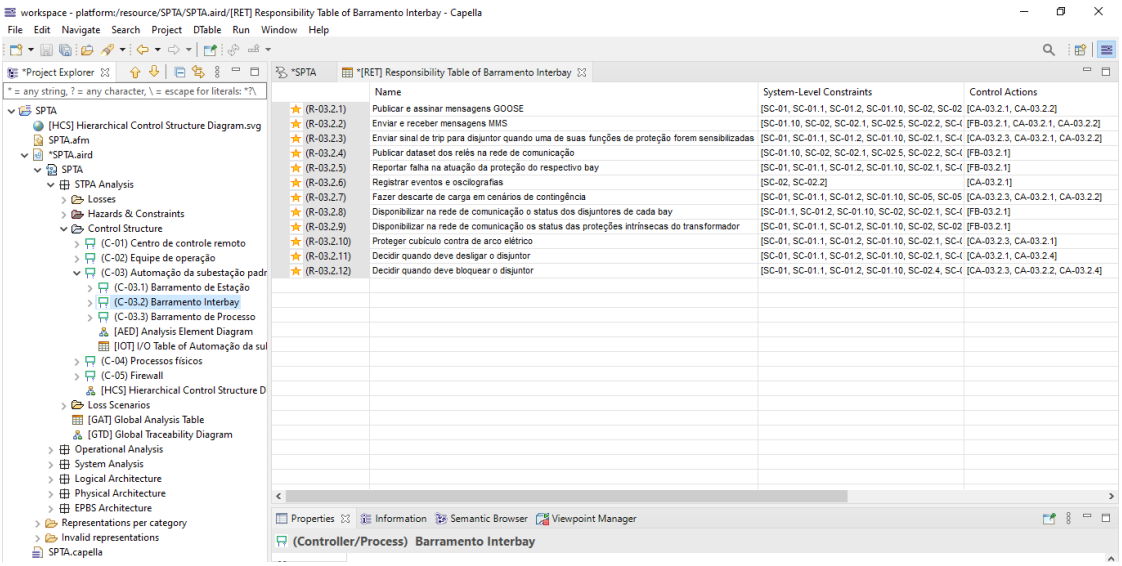


Fonte: Elaborado pelo autor.

Cada controlador recebe responsabilidades que precisam ser cumpridas para que juntas garantam as restrições em nível de sistema. A partir dessas responsabilidades, ações de controle são definidas para cada controlador, bem como o modelo de processo que eles precisam receber a fim de executar corretamente as ações de controle determinadas. Dessa forma, é gerado um diagrama detalhado de controle para cada controlador. Por fim, todas as ações de controle e *feedbacks* necessários para uma operação segura da subestação são ilustrados em um diagrama geral de controle construído conforme fluxograma apresentado na Figura 18.

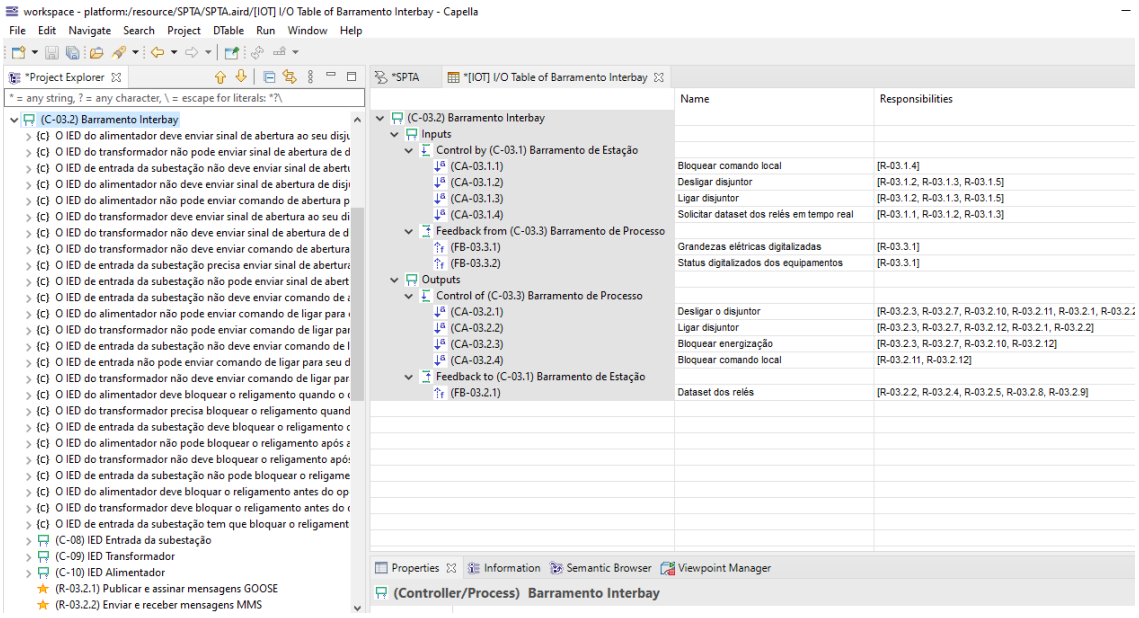
A Figura 35 apresenta as responsabilidades do barramento de *bay*. Para esse controlador, foram atribuídas doze responsabilidades, tais como publicar e assinar mensagens GOOSE, enviar e receber mensagens MMS e registrar oscilografias de eventos. Já na Figura 36, são mostradas as entradas e saídas desse subsistema. Vale salientar que esse controlador tanto recebe ações de controle e envia feedbacks para o barramento de estação, quanto envia ações de controle e recebe feedbacks do barramento de processos.

Figura 35 – Responsabilidades do barramento de bay no software Capella.



Fonte: Adaptado de Capella (versão 6.1, [202-?]).

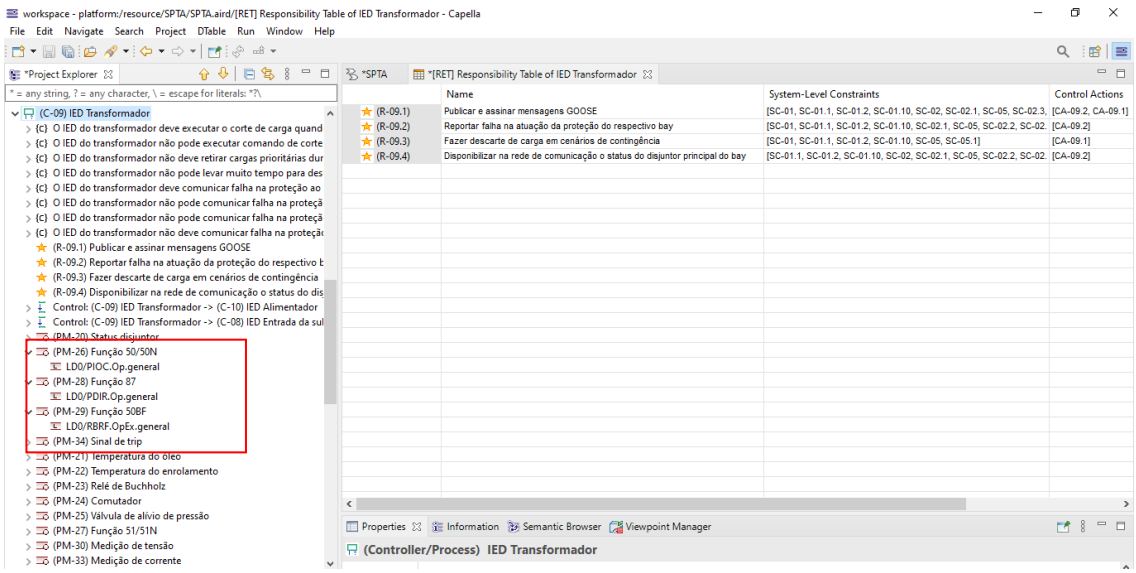
Figura 36 – Entradas e saídas do barramento de bay no software Capella.



Fonte: Adaptado de Capella (versão 6.1, [202-?]).

A Figura 37 ilustra as responsabilidades do IED do transformador com ênfase nas proteções e recursos operacionais. É destacado em vermelho os Modelos de Processos (MP) necessários para o funcionamento seguro desse controlador, de forma especial aquelas posteriormente implementadas na plataforma de testes, a saber: sobrecorrente instantânea, diferencial e falha disjuntor. Cada MP contém uma ou mais informações de processo. Essas informações foram associadas a caminhos de dados padrão IEC 61850, aproximando ainda mais a modelagem da implementação real da subestação digital.

Figura 37 – Responsabilidades do IED do transformador no software Capella.

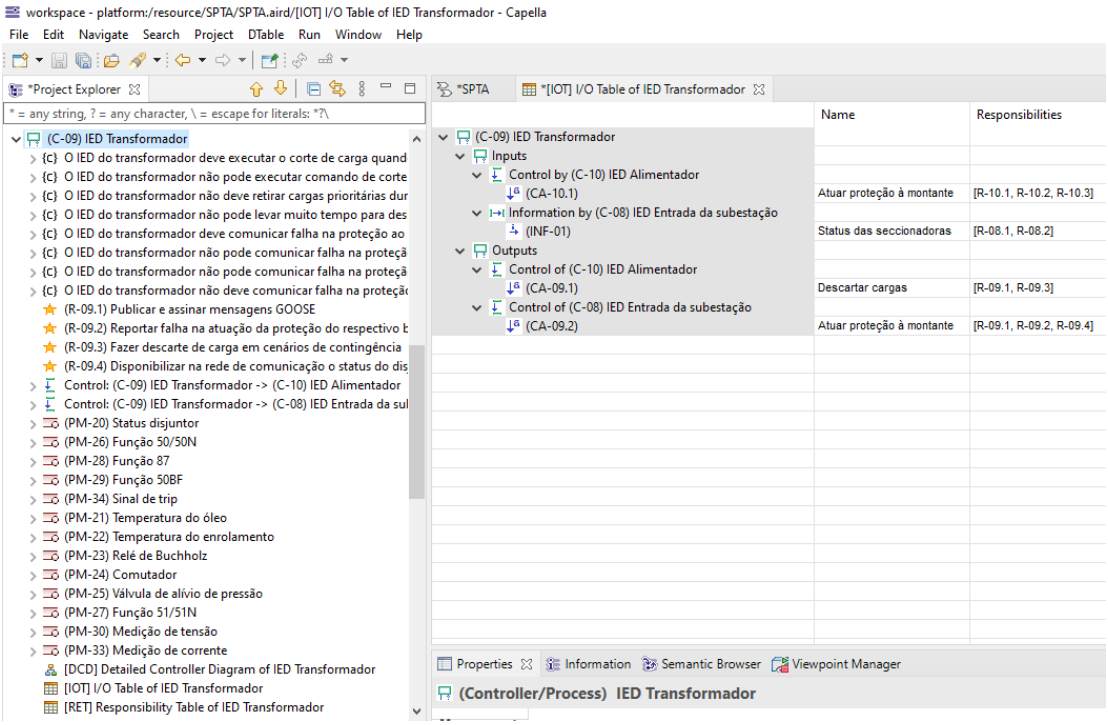


Fonte: Adaptado de Capella (versão 6.1, [202-?]).

A Figura 38 complementa a modelagem do IED do transformador ao exibir suas entradas e saídas. Esse controlador recebe e envia ação de controle ao IED do alimentador, seja atuando por falha no disjuntor do alimentador, seja comandando um descarte de cargas em cenário de contingência.

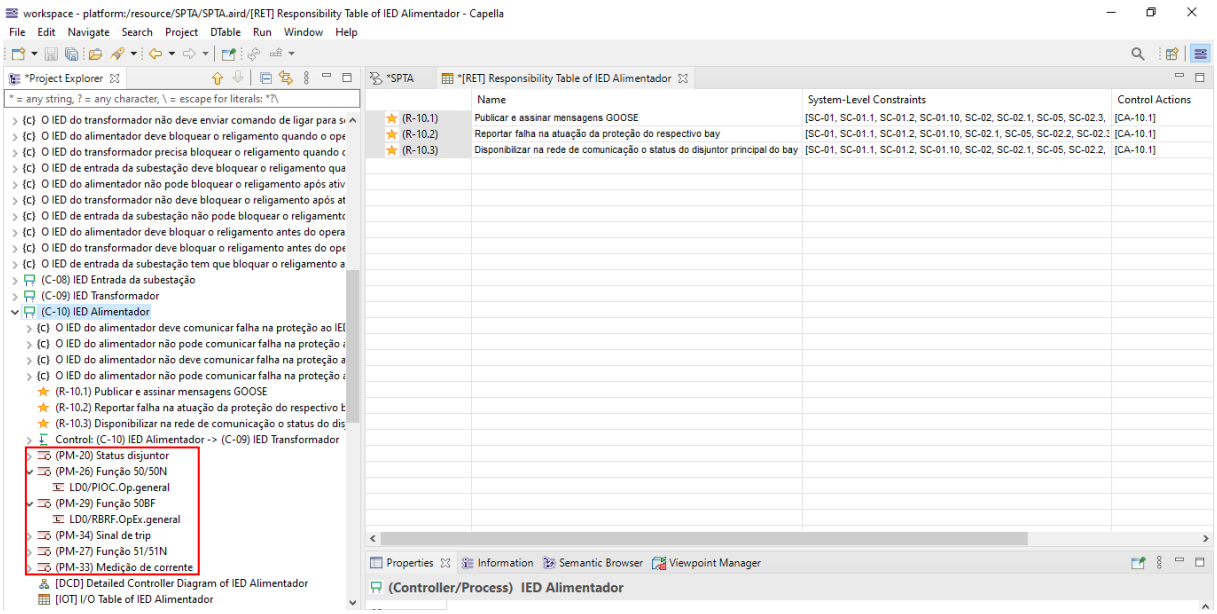
A Figura 39 mostra as três principais responsabilidades do IED do alimentador, destacando à esquerda os MPs necessários para sua atuação, enquanto a Figura 40 ilustra as entrada e saída desse controlador. O IED do alimentador recebe ação de controle para atuar em cenários de contingência quando sua carga não é prioritária para o processo produtivo, e envia ação de controle para o IED do transformador quando seu disjuntor falha em interromper uma falta em sua zona de proteção.

Figura 38 – Entradas e saídas do IED do transformador no software Capella.



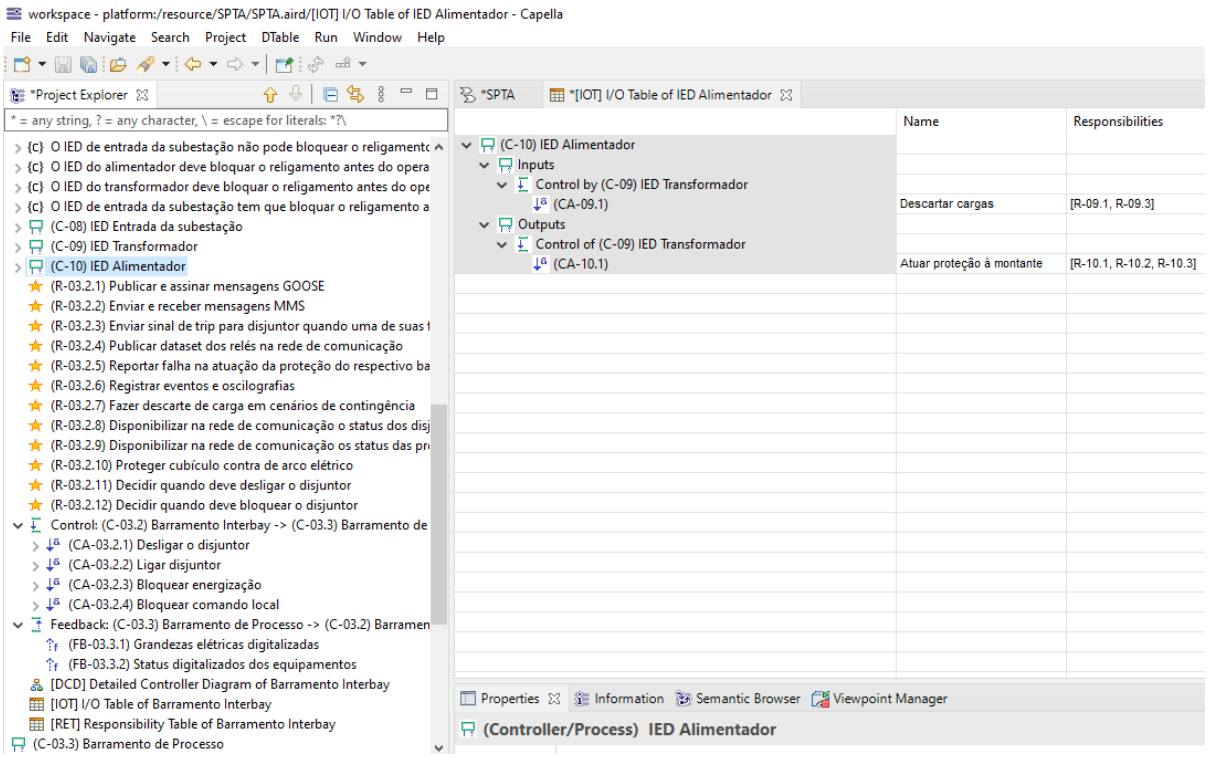
Fonte: Adaptado de Capella (versão 6.1, [202-?]).

Figura 39 – Responsabilidades do IED do alimentador no software Capella.



Fonte: Adaptado de Capella (versão 6.1, [202-?]).

Figura 40 – Entradas e saídas do IED do alimentador no software Capella.

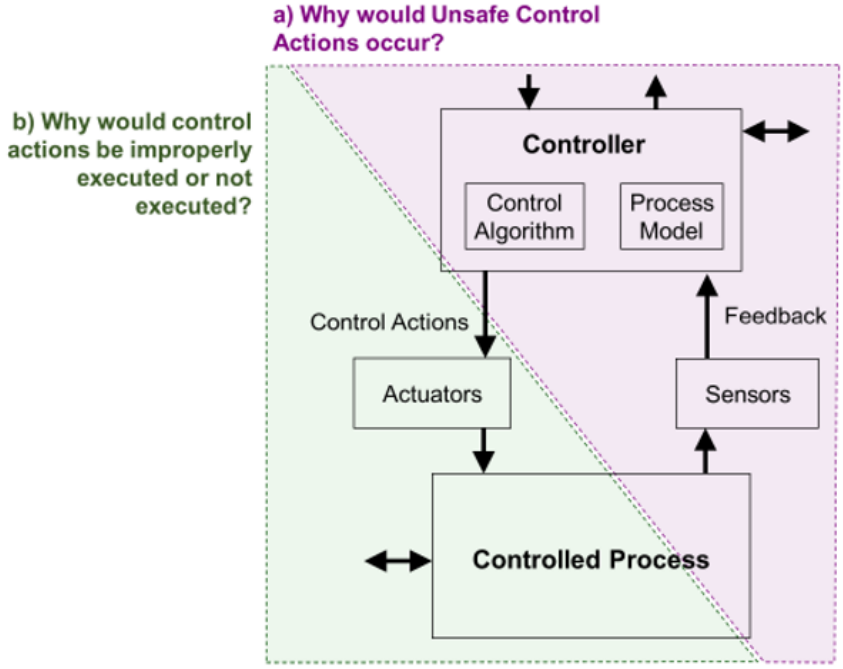


Fonte: Adaptado de Capella (versão 6.1, [202-?]).

Nesse trabalho, as ações de controle inseguras seguem a amplitude da estrutura de controle e são determinadas apenas para o barramento *interbay* do sistema de automação da subestação, conforme procedimento apresentado na Figura 22. Essa restrição visa limitar o escopo do trabalho e, dessa forma, tanto aprofundar a análise na filosofia de proteção proposta quanto explorar os conceitos da Indústria 4.0 na subestação.

Por fim, os cenários de perda são identificados, tanto aqueles que explicam a ocorrência de ações de controle inseguras, enfatizando sensores e controladores, quanto aqueles que tratam da execução inadequada ou ausência de ações de controle, considerando atuadores e o processo controlado. A Figura 41 ilustra o processo de investigação das causas que levam a cenários de perda.

Figura 41 – Investigação das causas dos cenários de perda.



Fonte: Leveson e Thomas (2018).

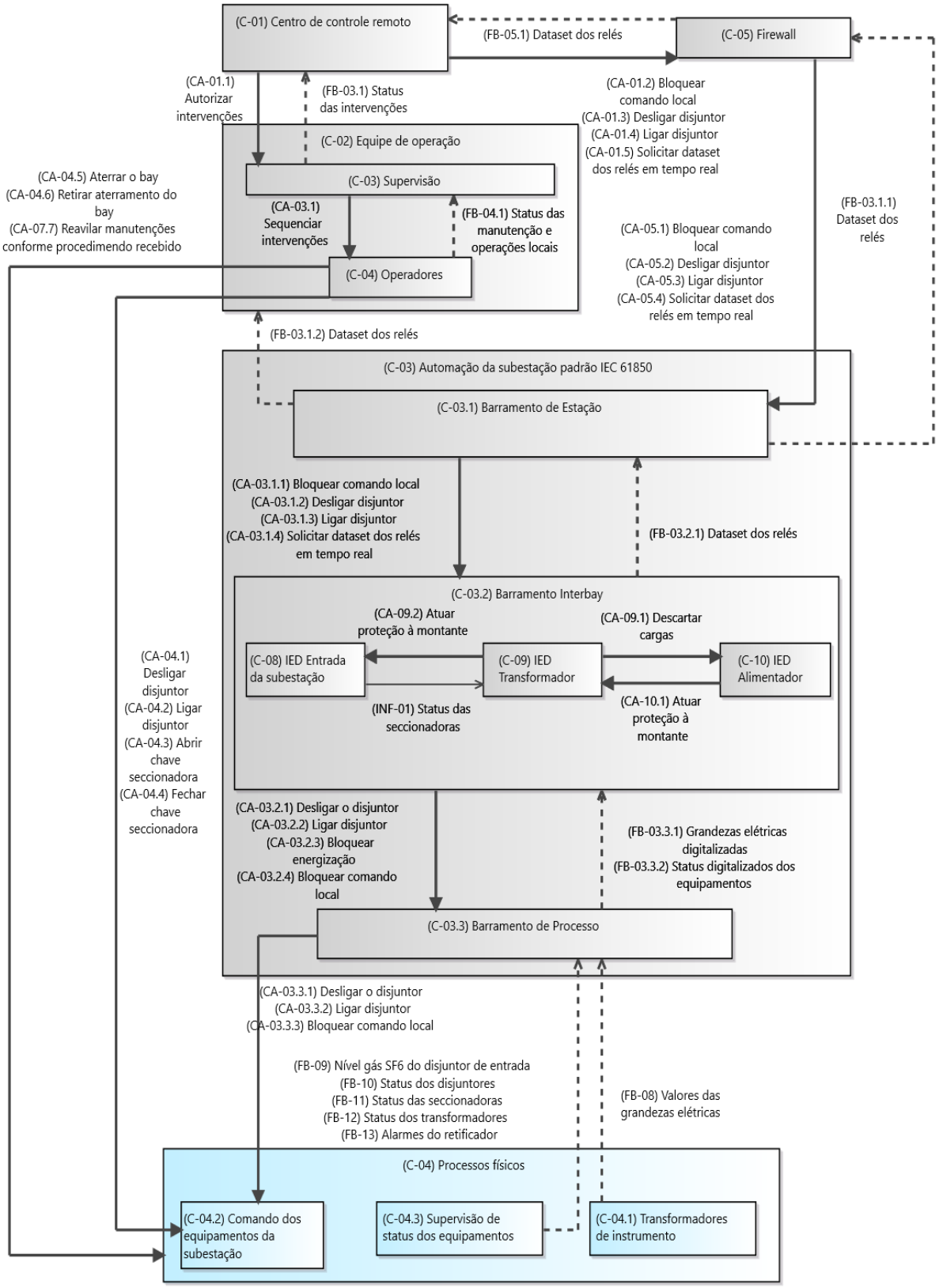
4.4 STPA aplicado à proposta de subestação industrial digital

A revisão da literatura realizada nesta Dissertação destacou os desafios associados às subestações digitais, como cibersegurança, controle em múltiplas camadas, capacitação técnica da equipe operacional e intertravamento lógico em IEDs, além dos modos de falha na comunicação de dados e nos níveis hierárquicos do SAS. A partir disso, foram identificados quatro sistemas que interagem entre si e controlam o funcionamento da subestação digital: centro de controle remoto, firewall, equipe de operação local e sistema de automação da subestação.

O método STPA é aplicado para a modelagem e avaliação das interações entre os controladores da subestação por meio de uma estrutura de controle hierárquica abrangente composta por circuitos de controle e feedback. A Figura 42 exibe a estrutura de controle obtida para a proposta de subestação digital industrial.

Antes de restringir a análise ao sistema de automação da subestação, uma compreensão global do sistema é necessária por meio da avaliação das interações entres os controladores. Observa-se que ações críticas do centro de controle remoto, localizado no topo da hierarquia de controle, estão intrinsecamente ligadas ao desempenho do *firewall*. Isso reforça a importância dos esforços direcionados a prevenir e mitigar ataques cibernéticos em subestações digitais.

Figura 42 – Diagrama geral da estrutura de controle da subestação.



Fonte: Adaptado de Capella (versão 6.1, [202-?]).

Outro ponto de destaque é a atuação da equipe local de forma coordenada e supervisionada pelo centro de controle remoto. Com essa estrutura, os procedimentos de segurança podem ser reforçados, uma vez que a validação de operações críticas, como a desenergização de *bay*, não ficará limitada às sinalizações de campo, mas passará por uma segunda avaliação da equipe de controle remoto, que pode validar as ações de campo por meio do sistema SCADA.

Adicionalmente, os comandos para ligar e desligar disjuntores podem partir do centro de controle remoto, da equipe de operação ou do sistema de automação. Em cenários críticos de segurança, como após a atuação de uma função de sobrecorrente, a função de bloqueio de comando local é crucial para evitar religamentos indesejados. Dessa forma, a equipe remota pode avaliar oscilografias dos relés e direcionar a atuação da equipe de manutenção de modo seguro.

O centro da tomada de decisão do sistema de automação da subestação está no barramento *interbay*. O diagrama detalhado de controle para esse subsistema é apresentado na Figura 43. São atribuídas doze responsabilidades e três ações de controle a esse barramento que contribuem para a imposição de restrições a nível de sistema. Além disso, são postas vinte e cinco restrições a nível de controlador advindas dos contextos que tornam ações de controle inseguras.

A Figura 44 exibe o diagrama detalhado de controle do IED do transformador. Dentre as responsabilidades inerentes ao barramento *interbay*, quatro itens relacionados as funções de proteção 50, 50BF e 87T foram destacadas. Além disso, são apresentados os modelos de processo com as respectivas informações, registradas conforme padrão IEC 61850, em caixas roxas. Esse controlador é encarregado de executar duas ações de controle, descarte de cargas sob o IED do alimentador e atuar a proteção à montante quando seu disjuntor falha.

A estrutura de controle detalhada do IED do transformador destaca a importância da sincronização das ações de controle e proteção, tais como a imposição um atraso no tempo de atuação da função 50BF em concordância com o tempo de abertura do respectivo disjuntor.

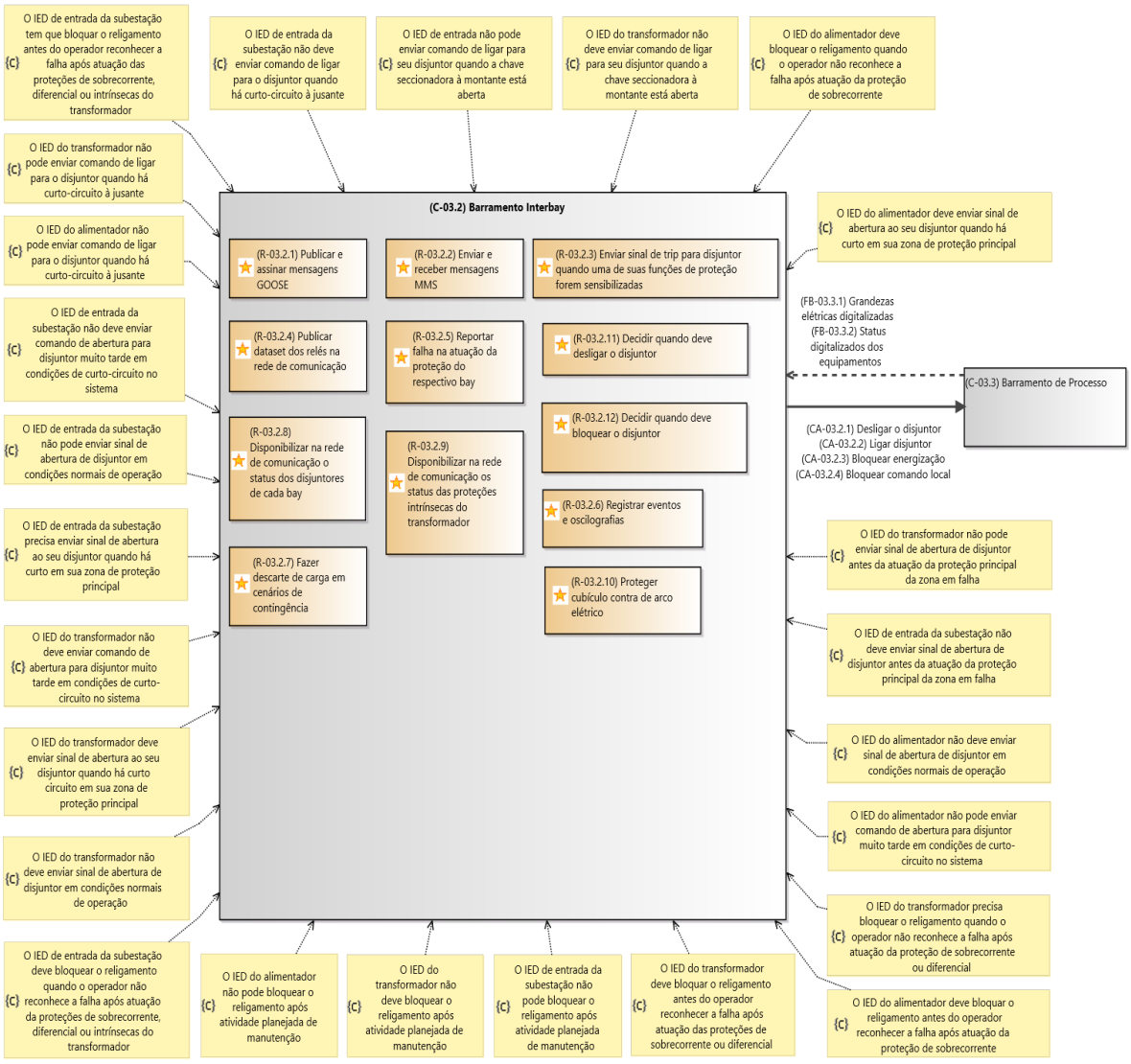
Além disso, o IED do transformador recebe a informação do status das chaves seccionadoras localizadas à montante do transformador. Isso possibilita a criação de uma lógica de segurança a fim de garantir que chaves seccionadoras não sejam comutadas sob carga.

Portanto, no primeiro movimento da chave seccionadora, o IED do transformador recebe a informação e comanda a abertura do seu disjuntor. Caso o disjuntor falhe, será comandado a abertura no disjuntor de entrada da subestação, garantindo integridade física do colaborador frente a uma operação errada na subestação.

Por sua vez, a Figura 45 mostra as informações necessárias para que o IED do alimentador desempenhe com segurança suas responsabilidades. São postas quatro restrições a nível de controlador que devem ser respeitadas durante o projeto da subestação digital.

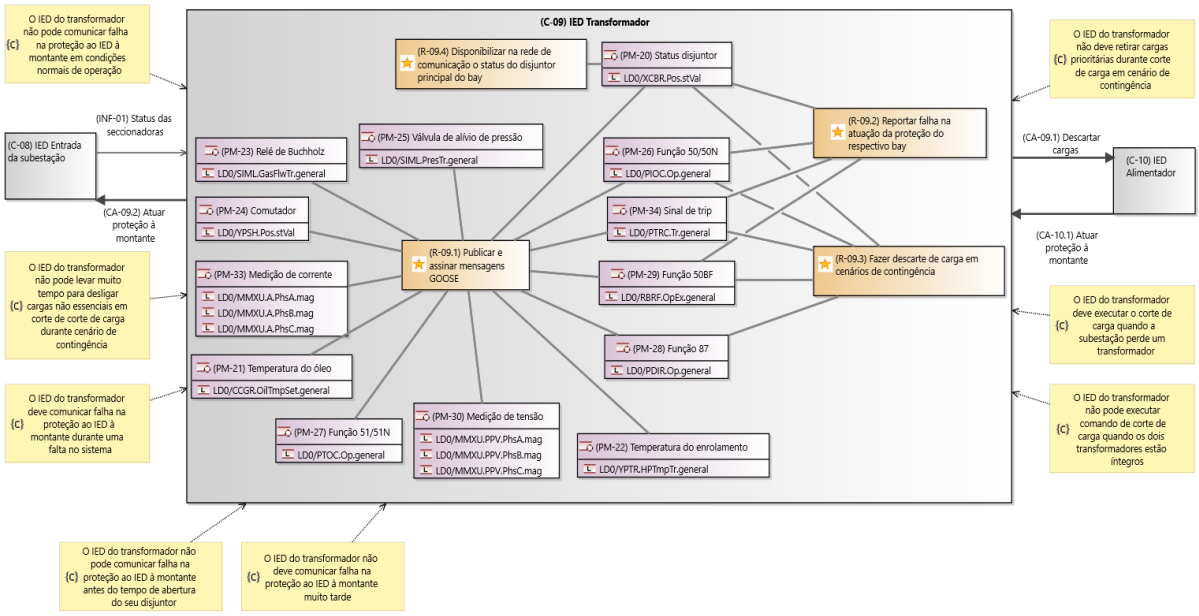
A modelagem da estrutura de controle foi tomada como base para determinar requisitos de projeto de proteção em subestações digitais, apoiando na criação de *datasets* com os dados que cada controlador precisa receber por meio de mensagens GOOSE.

Figura 43 – Diagrama detalhado de controle do barramento *interbay*.



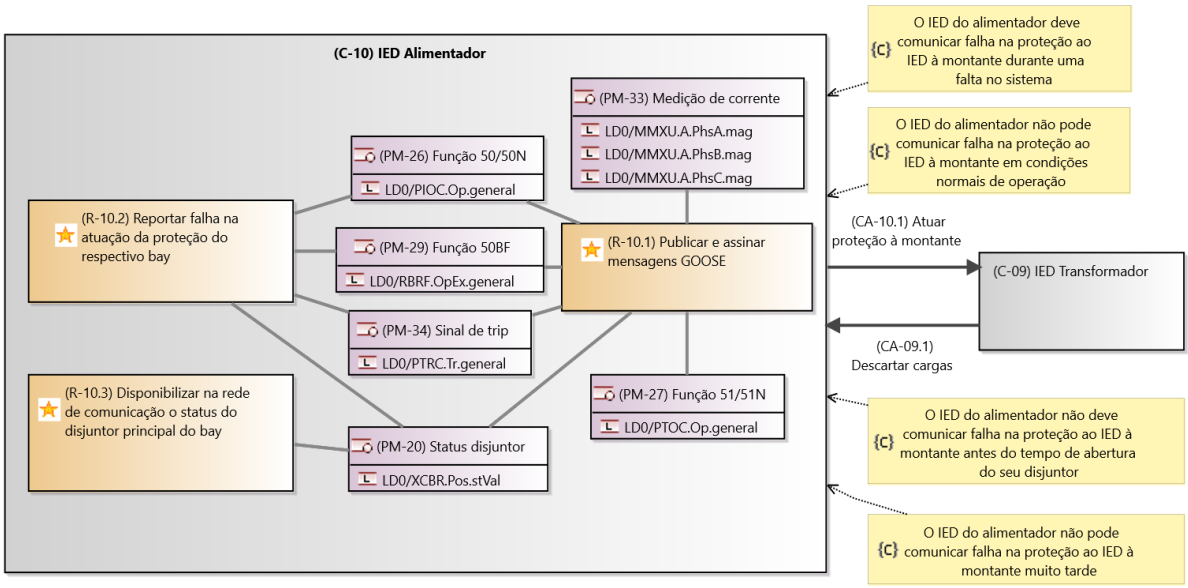
Fonte: Adaptado de Capella (versão 6.1, [202-?]).

Figura 44 – Diagrama detalhado de controle do IED do transformador.



Fonte: Adaptado de Capella (versão 6.1, [202-?]).

Figura 45 – Diagrama detalhado de controle do IED do alimentador.



Fonte: Adaptado de Capella (versão 6.1, [202-?]).

Dentre os cenários de perda obtidos pelo método STPA para as ações de controle sob responsabilidade dos IEDs do alimentador e do transformador, a Tabela 2 destaca aqueles que motivaram os testes laboratoriais, a fim de comparar o desempenho entre o atual cenário das proteções e a filosofia de proteção proposta.

Tabela 2 – Cenários de perda que motivaram testes laboratoriais.

Loss	Name	Control Action	Unsafe Control Action	Hazards
(LS-01)	O IED do alimentador não envia comando de abertura para a proteção à montante após seu disjuntor falhar em extinguir um curto-circuito ou sobrecarga no sistema, pois há falha na rede de comunicação.	CA-10.1 (IED Alimentador)	UCA-10.1	[H-01, H-01.1, H-01.4, H-05.1]
(LS-03)	O IED do alimentador não envia comando de abertura para a proteção à montante após seu disjuntor falhar em extinguir um curto-circuito ou sobrecarga no sistema, pois a função 50BF não está habilitada no relé.	CA-10.1 (IED Alimentador)	UCA-10.1	[H-01, H-01.1, H-01.4, H-05.1]
(LS-13)	O IED do transformador não executa o corte de carga quando a subestação perde um transformador, pois o grupo prioritário de cargas não foi definido no relé.	CA-09.1 (IED Transformador)	UCA-09.1	[H-01, H-01.7, H-05]
(LS-37)	O IED do alimentador não envia comando de abertura para a proteção à montante após seu disjuntor falhar em extinguir um curto-circuito ou sobrecarga no sistema, pois a rede de comunicação foi prejudicada por hackers.	CA-10.1 (IED Alimentador)	UCA-10.1	[H-01, H-01.1, H-01.4, H-05.1]

Fonte: Elaborado pelo autor.

4.5 Considerações finais

Este capítulo apresentou a subestação 69-13,8 kV de uma indústria têxtil e sua filosofia de proteção cronométrica. Na sequência, foi delineada a proposta de digitalização da subestação industrial e implementado o método STPA para avaliação de segurança. Após aplicar o STPA à proposta de digitalização da subestação, requisitos de segurança foram evidenciados, o que motivou a realização de testes em bancada.

5 PROPOSTA DE DIGITALIZAÇÃO DE SUBESTAÇÃO INDUSTRIAL

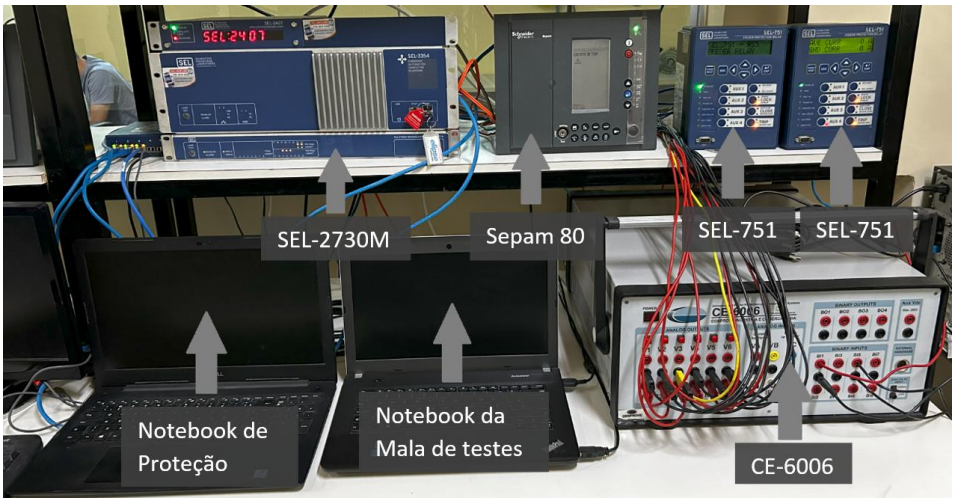
Este capítulo mostra a implementação e parametrização da plataforma de testes utilizada para validar o modelo proposto de digitalização da subestação industrial. São apresentados os equipamentos, softwares e o processos de configuração necessários para simular cenários operacionais. A validação do modelo proposto na bancada de testes é realizada por meio de experimentos que avaliam o desempenho das proteções da subestação nos contextos convencional e digital. Por fim, é verificado como a aplicação do padrão IEC 61850, em conjunto com os princípios da Indústria 4.0, pode otimizar os recursos operacionais da subestação.

5.1 Implementação da plataforma de teste

Após modelar um projeto de subestação digital padrão IEC 61850 por meio do método STPA, cenários de perda foram evidenciados. As perdas advindas de ações de controle inseguras do sistema de proteção e controle da subestação digital são confrontadas com a filosofia atual de proteção e controle da subestação industrial.

Para validar a inserção de princípios da Indústria 4.0 na subestação digital e avaliar o impacto do incremento de ações de controle propostas para essa subestação, as filosofias de proteção atual e proposta são testadas e validadas na plataforma de Proteção, Automação e Controle (PAC) padrão IEC 61850 do Laboratório de Redes Elétricas Inteligentes (LabREI), apresentada na Figura 46.

Figura 46 – Plataforma para testes em bancada.



Fonte: Elaborado pelo autor.

A plataforma PAC do LabREI é composta pela mala de testes Conprove CE-6006, dois relés de proteção SEL-751, um relé de proteção Schneider Sepam Series 80, um *switch* gerenciável SEL-2730M, dois notebooks, sendo um para comunicação com a mala de teste e outro para parametrização e configuração IEC 61850 dos relés de proteção.

O modelo da mala de teste adotada neste trabalho é o CE-6006, pois permite injeção de valores analógicos senoidais de corrente e tensão elétrica, medição de grandezas analógicas, controle de saídas e entradas digitais, além de suportar mensagens GOOSE conforme definido no padrão IEC 61850.

Durante os testes, foram habilitados seis canais para injeção de corrente elétrica e até duas entradas binárias para simular e monitorar, respectivamente, a atuação dos relés de proteção, interrompendo a injeção de corrente sempre que uma entrada binária muda de estado.

A fim de estabelecer a comunicação entre os notebooks, mala de testes e relés de proteção, é crucial empregar determinados softwares durante os procedimentos de teste. No que tange à mala de testes, é adotado o software Conprove Test Center (CTC) Quick ([202-?]), versão 2.02.162.

Já para os relés da marca SEL, são utilizados o software de parametrização *AcSELerator QuickSet*, versão 5.13.7.6, e o software de comunicação IEC 61850 *AcSELerator Architect*, versão 1.1.143.0 (Schweitzer Engineering Laboratories, [202-?]). O primeiro software permite o up-load e download da parametrização dos relés, sendo possível definir lógicas de atuação, selecionar protocolos de comunicação, ajustar funções de proteção, configurar indicações visuais por LEDs, além de outras funcionalidades típicas de IEDs. Já o segundo software possibilita a configuração de IEDs SEL para a edição ou assinatura de mensagens GOOSE de dispositivos SEL ou de terceiros e definição de reports padrão IEC 61850, baseados em atualização de valores analógicos. Além disso, permite a criação de Datasets com Logical Nodes selecionados pelo operador, os quais podem ser associados ao envio de mensagens GOOSE ou à transmissão de mensagens MMS para o SCADA.

Para os relés da Schneider, é usado o software de parametrização SFT2841, versão 17.4, e o software de comunicação IEC 61850 CET850, versão 4.6.0. O SFT2841 é adotado para parametrização do relé da série Sepam. Este software possibilita a parametrização e a transferência dos ajustes configurados no relé. Dentro desta interface, é possível estabelecer lógicas de atuação, selecionar o protocolo de comunicação do IED, ajustar as funções de proteção, configurar indicações visuais por LEDs, além de outras funcionalidades inerentes a IEDs. Por sua vez, o CET850 é utilizado para editar ou assinar mensagens GOOSE de dispositivos Schneider ou terceiros, criar datasets com logical nodes e vinculá-los ao envio de

mensagens GOOSE ou MMS, configurar reports, dentre outras configurações.

Esta seleção cuidadosa de softwares e versões é essencial para garantir a eficácia e confiabilidade das operações de teste e configuração dos dispositivos em questão.

5.2 Configuração da plataforma de Proteção, Automação e Controle (PAC)

A aplicação do método STPA em subestação digital resulta em um conjunto de restrições em nível de sistema que visam evitar ou mitigar cenários de perda. As restrições em nível de sistema, sob responsabilidade do sistema de automação, proteção e controle, que atuam em cenários de sobrecorrente, podem ser simuladas e validadas em bancada. Essas restrições são comparadas ao cenário atual das proteções da subestação, com o objetivo de identificar fragilidades na estrutura de controle existente e consolidar o modelo proposto como uma alternativa eficaz para as necessidades de segurança da subestação.

Primeiramente, são abordados os cenários de sobrecarga e curto-circuito, que são comuns em sistemas elétricos e exigem uma resposta imediata das proteções para evitar falhas catastróficas. Em seguida, são discutidos a falha na rede de comunicação e o corte de carga, destacando como esses eventos podem impactar a operação do sistema e a importância de mecanismos de recuperação e redundância na comunicação entre os dispositivos de proteção.

5.2.1 Cenários de sobrecarga e curto-circuito

Os testes têm como objetivo comparar os resultados das configurações atuais com as configurações propostas, avaliando se há ganhos de segurança no sistema com implementação da estrutura de controle e filosofia de proteção proposta.

Os relés da SEL foram ajustados conforme a OAP fornecida, e foram executados os testes de sobrecorrente temporizada e sobrecorrente instantânea. Em seguida, foi realizada a alteração da plataforma de testes a fim de simular a digitalização dos relés padrão IEC 61850. A mesma sequência de testes realizada para o cenário atual das proteções é repetida para o modelo proposto.

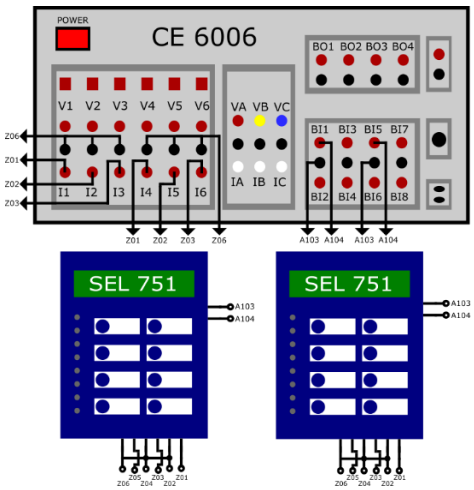
Inicialmente, os testes foram conduzidos sem simular uma falha no disjuntor D-4 e, posteriormente, com a simulação dessa falha no disjuntor, permitindo avaliar o comportamento do sistema tanto com a filosofia cronométrica quanto com a nova filosofia proposta.

A Figura 47 ilustra o *layout* das conexões elétricas realizadas na plataforma de testes, utilizando os 6 canais de corrente. Os canais I1 a I3 são destinados à entrada trifásica do relé

RS2, enquanto o BI1 monitora sua atuação. Já os canais I4 a I6 são destinados à entrada trifásica do relé RS4, com monitoramento de sua atuação via BI5.

O primeiro teste consiste na simulação de uma corrente de 650 A no alimentador A-1, com monitoramento do contato de trip do relé RS4 (principal). No segundo teste, a mesma corrente de 650 A é simulada no alimentador A-1, porém o monitoramento é do contato de trip do relé RS2 (retaguarda), simulando assim uma falha no disjuntor D-4. O terceiro teste simula uma corrente de 5000 A no alimentador A-1, com monitoramento do contato de trip do relé RS4 (principal). Já o quarto teste replica a mesma corrente de 5000 A no alimentador A-1, mas com monitoramento do contato de trip do relé RS2 (retaguarda), novamente simulando uma falha no disjuntor D-4.

Figura 47 – Layout das conexões elétricas da plataforma de teste para simulação de sobrecarga e curto-circuito.



Fonte: Elaborado pelo autor.

5.2.2 Falha na rede de comunicação e corte de carga

Uma forma de mitigar as perdas no contexto de falha na rede de comunicação da subestação é implementar a supervisão da integridade da rede, conforme ilustrado na Figura 31. Dessa forma, caso a rede de comunicação esteja comprometida, os relés voltam a coordenar por tempo.

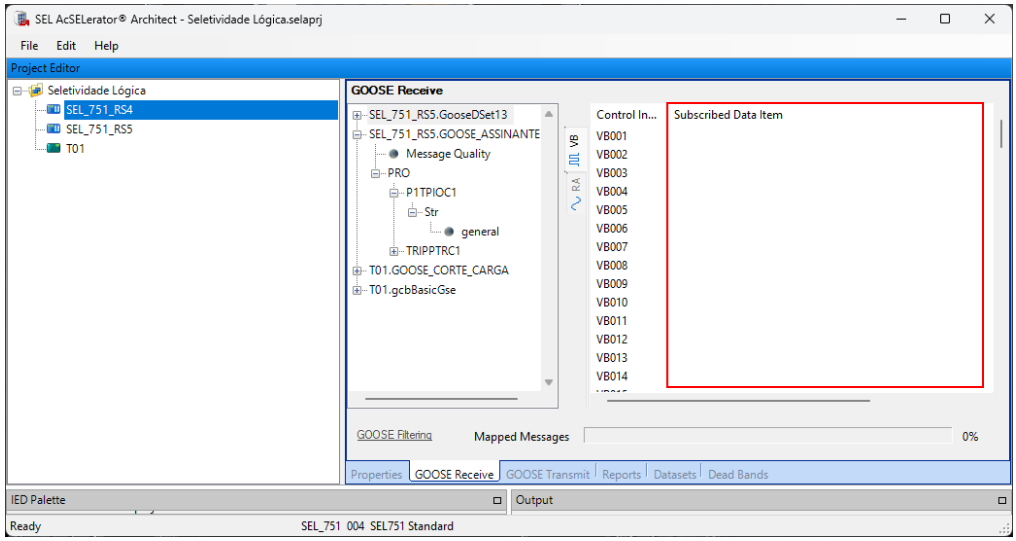
Atualmente, a subestação em estudo opera com dois transformadores de potência, e a falha de um desses transformadores resulta na paralisação de toda a indústria têxtil. O corte de carga surge como uma solução para esse problema, identificando e desconectando do sistema as cargas não essenciais, permitindo que a indústria continue operando com apenas um transformador.

O corte de carga só pode ser implementado de forma eficaz na subestação industrial mediante a substituição das chaves seccionadores por disjuntores no lado primário dos transformadores. Entretanto, por ser um recurso disponível no modelo de controle proposto e está intrinsecamente relacionada ao princípio de modularização da Industria 4.0, essa funcionalidade também é validada na plataforma de testes.

A função de proteção determinante para efetuar o corte automático de cargas é a proteção diferencial de corrente do transformador. Para essa aplicação, a função diferencial precisa da rede de comunicação para enviar mensagens GOOSE aos alimentadores de cargas não essenciais, comandando abertura de seus respectivos disjuntores. Essa etapa conta com relés de proteção de dois fabricantes, SEL e Schneider, sendo o relé Sepam Series 80 da Schneider responsável pela proteção 87T, enquanto os dois relés da SEL atuam como proteção dos alimentadores, um para cargas essenciais e outro para cargas não essenciais.

O relé RS4 é responsável pela proteção de cargas essenciais, enquanto o RS5 está associado ao grupo de cargas não essenciais que, portanto, deverão ser rejeitadas em cenários de contingência em um transformador. A Figura 48 evidencia que o relé RS4 não assina mensagens GOOSE, portanto não atuará para contingências em transformadores de potência.

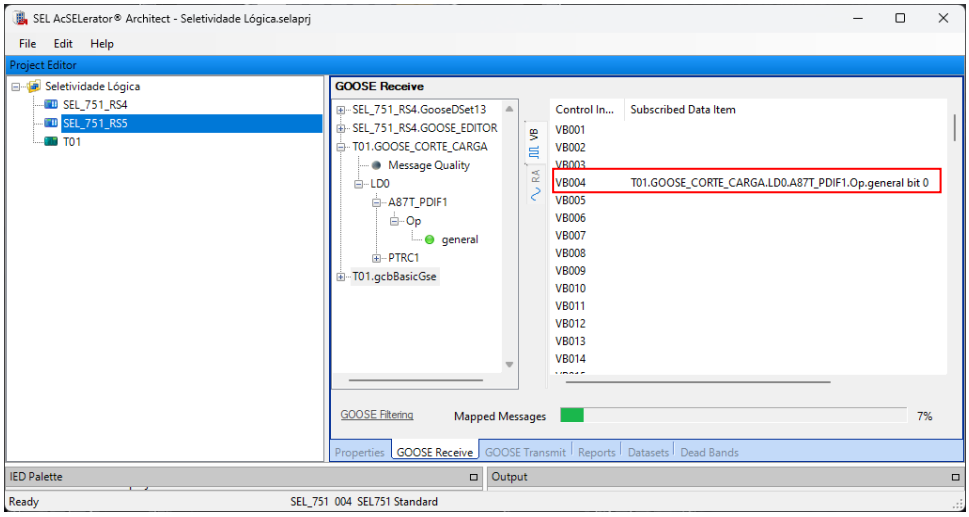
Figura 48 – Configuração IEC 61850 para RS4.



Fonte: Adaptado de Architect (versão 1.1.143.0).

Por outro lado, o relé RS5 assina a mensagem de operação da função 87T conforme mostrado na Figura 49. Portanto, RS5 comandará abertura do seu disjuntor quando houver uma contingência no transformador, conferindo a subestação o conceito de modularidade próprio da Indústria 4.0.

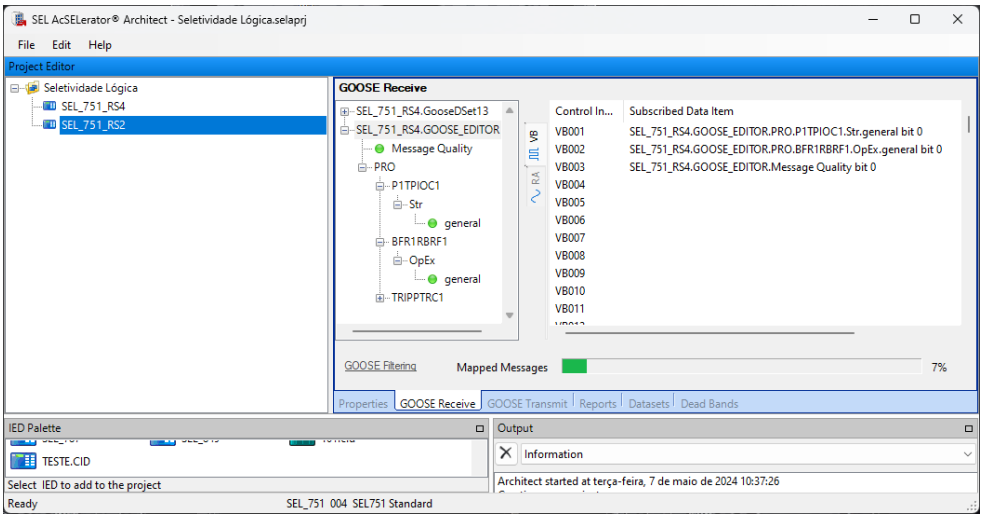
Figura 49 – Configuração IEC 61850 para RS5.



Fonte: Adaptado de Architect (versão 1.1.143.0).

Por sua vez, a Figura 50 apresenta as mensagens assinadas pelo relé RS2 responsável pela proteção do transformador. Esse dispositivo assina três mensagens: atuação da função 50 e 50BF do alimentador, e o bit de qualidade da mensagem GOOSE. Os três dados são fundamentais para atuação segura da proposta de seletividade lógica.

Figura 50 – Configuração IEC 61850 para RS2.

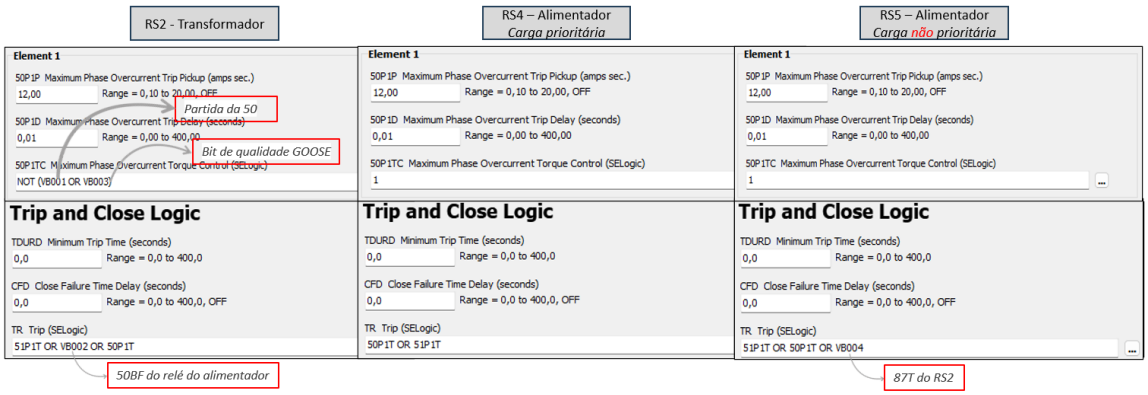


Fonte: Adaptado de Architect (versão 1.1.143.0).

Por fim, a Figura 51 apresenta uma síntese das configurações dos relés no arcabouço digital, destacando as informações recebidas nas portas virtuais dos relés (VB001 a VB004) e a construção da lógica de atuação. Vale destacar que o relé do alimentador envia sinal de trip para seu disjuntor quando suas funções de sobrecorrente atuam ou quando recebe mensagem de falha disjuntor de um alimentador. Além disso, sua função instantânea é bloqueada quando

o bit de qualidade da GOOSE ou a função 50 do alimentador assumem valor binário igual a um.

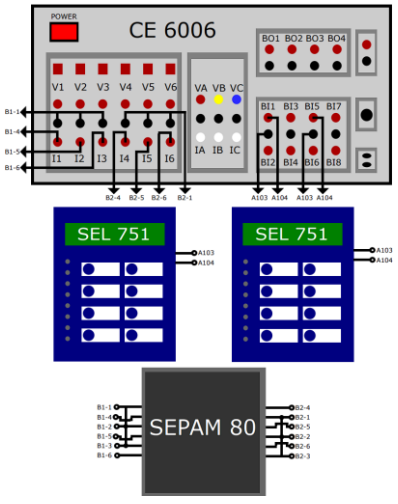
Figura 51 – Parametrização lógica dos relés.



Fonte: Adaptado de QuickSet (versão 5.13.7.6).

Para a realização do teste de corte automático de cargas, foi necessário um arranjo elétrico distinto em comparação ao teste de sobrecorrente. A Figura 52 ilustra as conexões elétricas realizadas para esse teste, incluindo a ligação dos seis canais analógicos de corrente da mala de testes ao Sepam Series 80 da Schneider e a monitoração da atuação dos relés RS4 e RS5 pelas entradas binárias BI1 e BI5 da mala de testes.

Figura 52 – Layout das conexões elétricas da plataforma de teste para simulação de interoperabilidade e rejeição de cargas.



Fonte: Elaborado pelo autor.

5.3 Validação do modelo proposto na bancada de teste

O Laboratório de Redes Elétricas Inteligentes, particularmente sua Plataforma de Automação e Controle (PAC), foi empregado para conduzir simulações destinadas à

implementação dos ajustes atualmente empregados na subestação, bem como das propostas de alterações na filosofia de proteção, em consonância com os avanços tecnológicos e os princípios da Indústria 4.0.

O principal objetivo dos testes é demonstrar os recursos de controle tanto do sistema de proteção atualmente em vigor, quanto da filosofia de proteção proposta, e a subsequente análise comparativa dos resultados obtidos para cada cenário.

Os resultados foram registrados para as simulações de sobrecorrente temporizada e instantânea, tanto em condições normais quanto com falha nos disjuntores. Para o cenário proposto, também é avaliado o comportamento do sistema quando há falha na comunicação e o recurso de corte automático de carga.

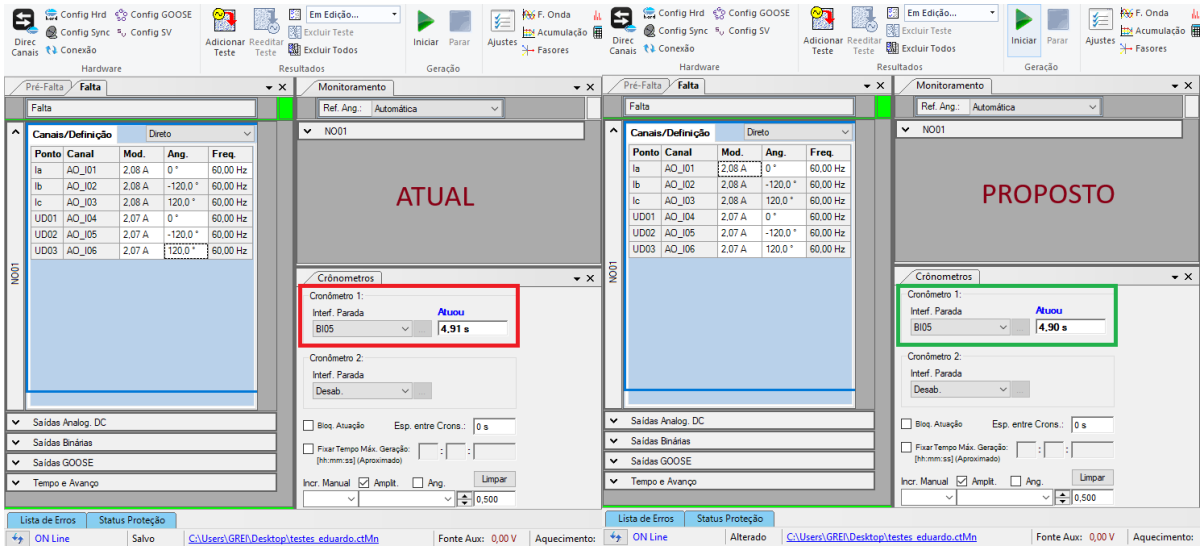
O primeiro teste foi conduzido impondo uma sobrecarga no alimentador A-1 de 650A e sem falha no disjuntor D-4. Na Figura 53, são apresentados os resultados do primeiro teste, com o cenário atual à esquerda e as modernizações propostas à direita. No cenário atual, é observado coordenação e seletividade com tempo de resposta de 4,91 segundos, dos quais 4,87 segundos correspondem à atuação da função de proteção 51 e 0,04 segundos ao tempo de processamento e recepção do sinal pela entrada binária da mala de testes. Quanto ao cenário proposto, não foram observadas mudanças em relação ao cenário atual.

Os resultados obtidos nesta fase são considerados satisfatórios, dado que a função de proteção 51 possui os mesmos ajustes em ambos os cenários e o valor de tempo obtido está coerente com o tempo calculado pela curva de atuação do relé, conforme Equação (5.1)

$$t = \frac{13{,}5}{\frac{650}{345} - 1} * 0{,}3 = 4{,}58\ s. \qquad (5.1)$$

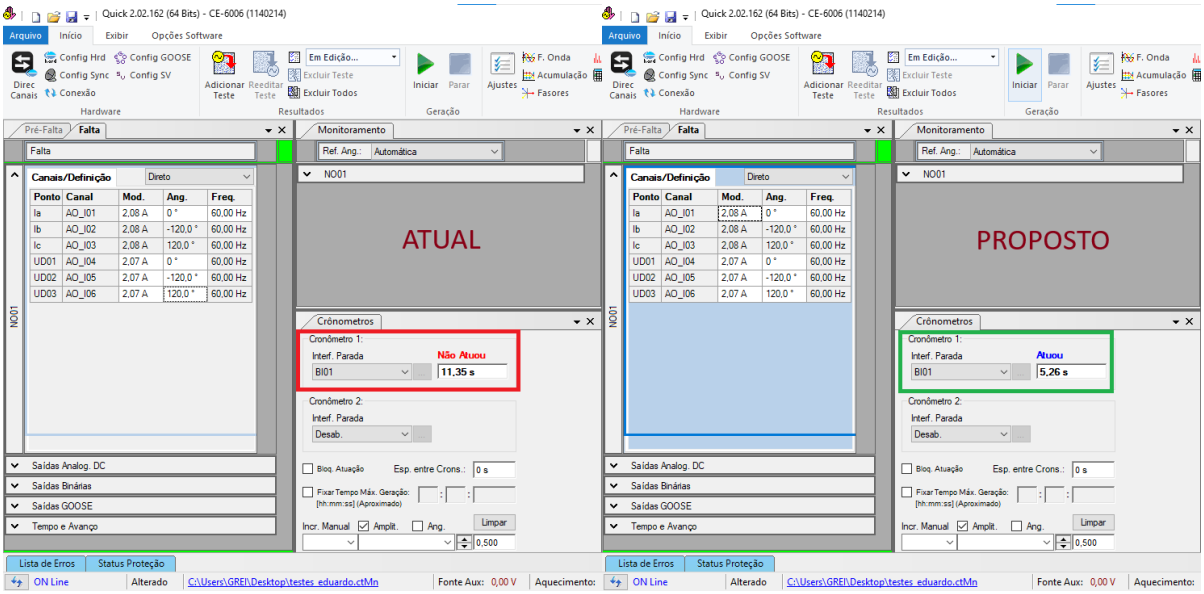
A segunda simulação considera além da sobrecarga de 650 A, a falha do disjuntor D-4. A Figura 54 mostra os resultados deste teste. Para o cenário atual das proteções, a falha não foi eliminada do sistema, indicando uma vulnerabilidade nesta subestação. Por outro lado, no cenário proposto, a falha foi eliminada por meio do envio da mensagem de falha do disjuntor. O tempo de resposta para a filosofia digital foi de 5,26 segundos, dos quais 4,90 segundos correspondem ao tempo previsto na curva de atuação do relé RS4, 0,34 segundos ao envio da mensagem de falha do disjuntor e 0,02 segundos ao tempo de processamento e recepção do sinal pela entrada binária da mala de testes. Este resultado valida a restrição a nível de sistema imposta pela seletividade lógica com atuação da proteção de retaguarda.

Figura 53 – Comparação de desempenho das filosofias de proteção para sobrecarga no alimentador A-1 de 650A sem falha no disjuntor D-4.



Fonte: Adaptado de Quick (versão 2.02.162).

Figura 54 – Comparação de desempenho das filosofias de proteção para sobrecarga no alimentador A-1 de 650A com falha no disjuntor D-4.

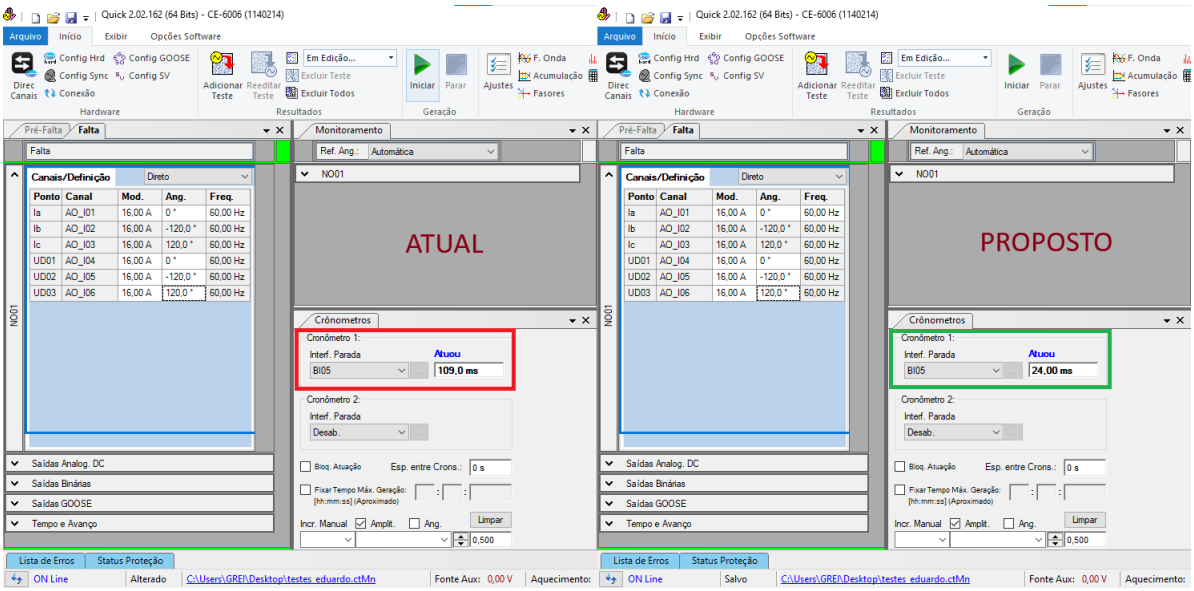


Fonte: Adaptado de Quick (versão 2.02.162).

O terceiro experimento foi realizado sob condição de curto-circuito no alimentador A-1 no nível de 3500A, sem falha no disjuntor D-4. A Figura 55 exibe os resultados dessa etapa. No cenário atual, a coordenação e seletividade é alcançada. O teste é considerado satisfatório, com um tempo de resposta de 0,109 segundos, dos quais 0,08 segundos correspondem ao atraso na atuação da função 50, conforme OAP, e 0,029 segundos ao tempo de processamento e recepção do sinal pela entrada binária da mala de testes.

No cenário proposto, a coordenação e seletividade também foram observadas, mas com um tempo de atuação inferior ao tempo de atuação do cenário atual. O tempo total de resposta foi de 24,00 milissegundos. A redução do tempo de atuação é alcançada devido a coordenação não ser realizada por atrasos de tempo, e sim por intertravamento lógico.

Figura 55 – Comparação de desempenho das filosofias de proteção para curto-circuito no alimentador A-1 sem falha no disjuntor D-4.



Fonte: Adaptado de Quick (versão 2.02.162).

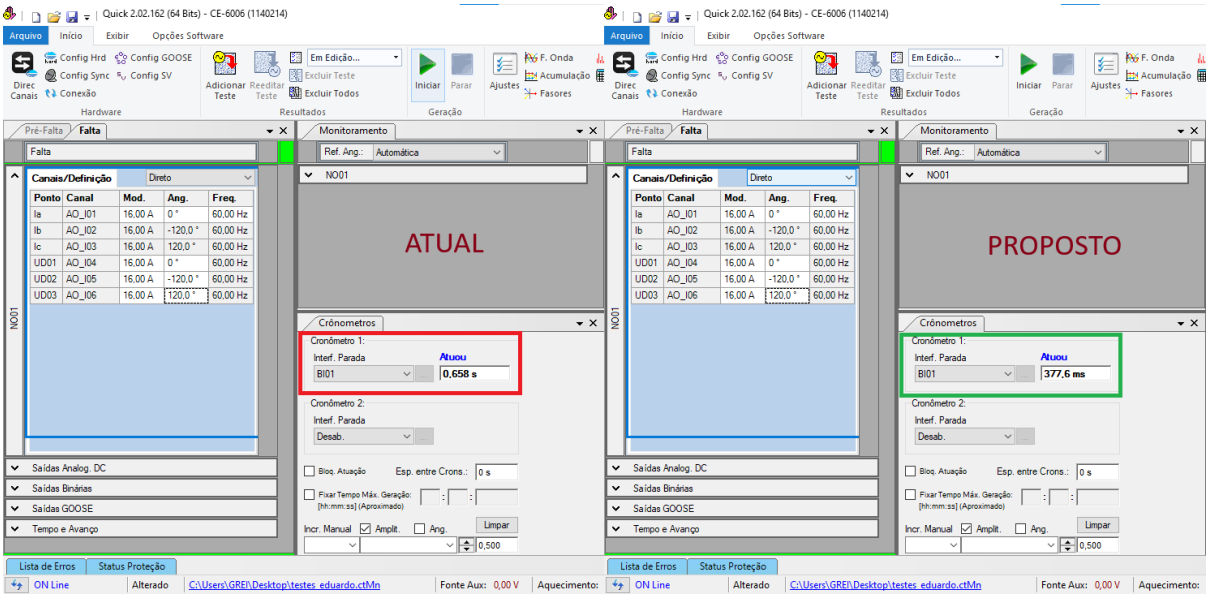
A quarta avaliação implementa além da corrente de curto-circuito de 3500 A, a falha no disjuntor D-4. Os resultados são expressos na Figura 56. A coordenação e seletividade são mantidas para o cenário atual. O tempo de resposta foi de 0,658 segundos, dos quais 0,63 segundos correspondem à atuação da função de proteção 51 e 0,028 segundos ao tempo de processamento e recepção do sinal pela entrada binária da mala de testes. O tempo de resposta foi elevado em relação à corrente de falta injetada no sistema, pois a função 50 está desabilitada no dispositivo RS2 conforme OAP.

Já para o cenário proposto, o tempo de atuação é menor, atingindo 377,6 milissegundos, dos quais 340 milissegundos correspondem ao envio da mensagem de falha do disjuntor, 10 milissegundos ao atraso de tempo aplicado no dispositivo RS2 e 27,76 milissegundos ao tempo de processamento e recepção do sinal pela entrada binária da mala de testes. Portanto, o cenário proposto também possui vantagem operacional nessa etapa.

É importante ressaltar que para o pleno funcionamento da estrutura de controle proposta, é imprescindível contar com uma infraestrutura de comunicação robusta, capaz de garantir a integridade do processo. A falha no sistema de comunicação na subestação representa

um perigo a nível de sistema. Portanto, é necessário estabelecer restrições a nível de sistema que assegurem o funcionamento das proteções em um contexto de interrupção na rede de comunicação.

Figura 56 – Comparação de desempenho das filosofias de proteção para curto-circuito no alimentador A-1 com falha no disjuntor D-4.



Fonte: Adaptado de Quick (versão 2.02.162).

O quinto teste visa simular uma falha de comunicação no sistema de proteção proposto. A Figura 57 expõe os resultados da atuação das proteções em caso de falha na rede de comunicação. Notavelmente, o tempo de resposta é semelhante ao encontrado no quarto teste para o cenário atual. Quando ocorre a perda de comunicação no sistema, a lógica implementada no novo cenário detecta essa indisponibilidade, desabilita a seletividade lógica e mantém a coordenação cronométrica.

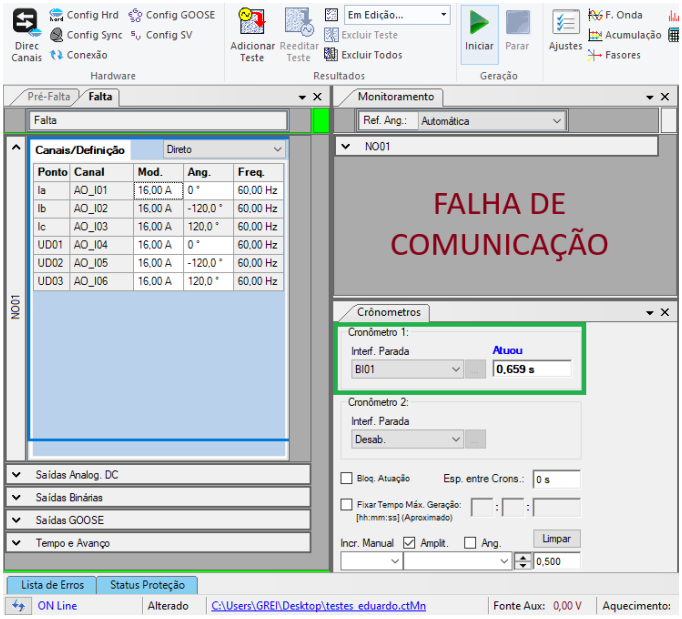
O último teste visa validar a inserção de três princípios da Indústria 4.0 na subestação industrial digitalizada conforme IEC 61850, a saber: interoperabilidade, modularização e descentralização.

Para verificar a interoperabilidade, relés de fabricantes diferentes foram utilizados para simular o sistema. O relé Sepam T87 da Schneider é utilizado como relé do *bay* do transformador, enquanto os relés da SEL são utilizados para proteção de alimentadores. A modularização é obtida quando a subestação é capaz de se reconfigurar automaticamente por meio do corte de cargas a fim de se adequar a um cenário de contingência.

Tal adequação é limitada a atuação das equipes operacionais no cenário atual da estrutura de controle da subestação. Para o modelo proposto, essa decisão é descentralizada. As

cargas prioritárias são definidas previamente pelas partes interessadas e o sistema atua de modo a manter o suprimento de energia para essas cargas. Vale salientar que para o funcionamento pleno desse recurso operacional, é necessário substituir as seccionadoras, localizadas no primário dos transformadores, por disjuntores.

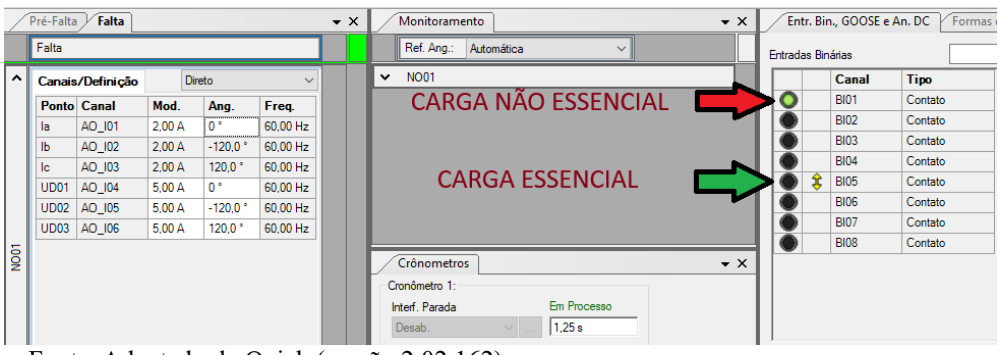
Figura 57 – Desempenho da filosofia de proteção proposta para curto-circuito no alimentador A-1 e falha na rede de comunicação.



Fonte: Adaptado de Quick (versão 2.02.162).

O corte automático de carga depende da comunicação entre os três relés de proteção presentes na bancada. A Figura 58 mostra a injeção de corrente no relé da Schneider associado a T01, que é responsável pela função 87T, e o descarte automático das cargas. A atuação da função 87T é sinônimo de perda de potência de suprimento na subestação, uma vez que o transformador em falha será desconectado do sistema.

Figura 58 – Desempenho da filosofia de proteção proposta para cenário de contingência.



Fonte: Adaptado de Quick (versão 2.02.162).

5.4 Considerações finais

Este capítulo apresentou a estrutura dos testes laboratoriais, identificando os equipamentos necessários, os softwares de configuração correspondentes e a parametrização da plataforma de testes. Além disso, são exibidos os resultados de cinco experimentos laboratoriais, que fundamentam as discussões sobre o desempenho operacional das proteções da subestação industrial nos cenários convencional e digital. Por fim, é mostrado como a adoção do padrão IEC 61850, em conjunto com os princípios da Indústria 4.0, agrega recursos operacionais à subestação.

6 DISCUSSÃO

Este capítulo discute os resultados obtidos a partir da aplicação do método STPA em subestação digital, destacando os requisitos operacionais necessários para a segurança da subestação e de seus operadores. Além disso, o desempenho das proteções da subestação nos cenários convencional e digital são comparados, evidenciando os ganhos em segurança proporcionados pela digitalização com o padrão IEC 61850, assim como os ganhos operacionais resultantes da adoção dos princípios da Indústria 4.0.

6.1 Aplicação do STPA em subestações digitais

O método STPA direcionou a modelagem da estrutura de controle da subestação digital proposta, destacando as ações de controle necessárias a cada controlador para operação segura da subestação. Além disso, o STPA possibilita a avaliação das ações de controle e os contextos em que essas ações podem levar a perdas.

Inicialmente, são verificados impactos no sistema pela ausência de cada ação de controle em contextos adversos de operação. Ao avaliar a ação de controle “Atuar proteção à montante”, um cenário inseguro foi observado para a filosofia cronométrica. Caso o disjuntor D-4 falhe, a ação de controle é executada somente se o relé a montante for sensibilizado, uma vez que não há comunicação entre os relés.

No entanto, para correntes no sistema que estejam acima do pick-up da função 51 do RS4 e abaixo do pick-up da função 51 do RS2, da ordem de 650 A, o perigo não será controlado no contexto de falha do disjuntor D-4, o que pode levar a perdas. Portanto, esse perigo a nível de sistema não possui ação de restrição para o contexto de falha no disjuntor no âmbito da subestação convencional.

Para mitigar os impactos da ausência de ação de controle na proteção de sobrecorrente, foi criada uma restrição a nível de sistema no âmbito digital, onde o IED deve comunicar a falha de atuação da proteção ao IED à montante.

A medida de controle proposta é a implementação de seletividade lógica entre os relés, com envio de mensagem de falha de disjuntor. Se o disjuntor D-4 falhar ao eliminar uma falta no alimentador A-1, uma mensagem GOOSE, conforme o padrão IEC 61850, será enviada pela rede de comunicação e detectada pelo relé RS2. A solução é implementada na PAC por meio da função 50BF.

Ações de controle executadas em contextos inadequados também podem levar a

perdas. Isso foi evidenciado dentro das responsabilidades da equipe operacional. Durante as manutenções, a equipe deve aterrar o *bay* antes de executar suas tarefas. Contudo, essa ação de controle levará a uma perda caso seja realizada com o *bay* ainda energizado. Para superar esse perigo, uma restrição a nível de sistema é imposta aos operadores, sendo necessário autorização das ações pelo centro de controle remoto antes da execução. A digitalização da subestação permite habilitar essa restrição, uma vez que as grandezas elétricas do sistema são monitoradas em tempo real.

O STPA também expõe os perigos associados as ações de controle realizadas de forma inadequada, como muito cedo, muito tarde ou fora de ordem. Dessa forma, foi possível identificar a necessidade de retardar a função de proteção 50BF, a fim de coordenar com a função de sobrecorrente instantânea, pois quando a função 50 atua, há um tempo mínimo necessário para acionamento mecânico do disjuntor. Sem o retardo de tempo na função 50BF, não haveria seletividade na atuação das funções de sobrecorrente e falha disjuntor.

As ações de controle mantidas por muito tempo ou interrompidas precocemente também podem gerar perdas, como por exemplo, o sinal de *trip* enviado ao disjuntor. A manutenção desse sinal sobre a bobina de abertura do disjuntor resultará em queima da bobina. Por tanto, é necessária uma restrição a nível de controlador para que o sinal de *trip* cesse quando o disjuntor abrir ou se a função 50BF acionar a proteção de retaguarda.

Adicionalmente, o método evidenciou o perigo de executar o comando de abertura da chave seccionadora no contexto de um circuito em carga. Para mitigar esse perigo, é necessário incluir um intertravamento entre a chave seccionadora e o circuito de abertura do disjuntor à jusante. Dessa forma, ao tentar abrir a chave seccionadora com carga, o disjuntor será aberto primeiro. Além disso, o relé não deve enviar o comando de fechamento para o disjuntor quando a chave seccionadora à montante estiver aberta. Para garantir essa condição, é necessário inserir o contato auxiliar da chave seccionadora no circuito de fechamento do disjuntor

As restrições a nível de controlador expostas por meio do método STPA podem subsidiar decisões de projeto da subestação digital, tais como definições de hardware para relés e intertravamentos lógicos necessários para operação segura. Por outro lado, o método gera uma grande quantidade de cenários de perda com descrição textual longa, dificultando o gerenciamento desses cenários. Tendo em vista os demais controladores da subestação que deverão ser modelados em trabalhos futuros, torna-se imperativo a busca por outros métodos e ferramentas capazes de abordar melhor os cenários de perda.

6.2 Desempenho das proteções em subestações tradicional e digital

A comparação entre as proteções em sistemas digitais e convencionais foi realizada por meio de uma série de testes laboratoriais, focando em cenários de sobrecarga e curto-circuito. Nos testes de sobrecarga de 650 A sem falha do disjuntor D-4, ambas as abordagens mostraram coordenação e seletividade adequadas, com um tempo de resposta similar.

No entanto, quando a sobrecarga ocorreu com falha do disjuntor, a filosofia convencional não atuou a proteção de retaguarda, mantendo a falha no sistema. Por outro lado, as proteções no âmbito digital eliminaram o defeito em 5,26 segundos, dos quais 4,90 segundos correspondem ao tempo previsto na curva de atuação do relé RS4. Isso evidencia um perigo a nível de sistema sem restrição a nível de sistema para a filosofia de proteção convencional que foi mitigado pela proposta de digitalização da subestação.

A seletividade lógica proposta também superou a filosofia de proteção convencional em um cenário de curto-circuito no alimentador A-1. Nesse teste, o tempo de atuação das proteções digitais foi 78% abaixo do tempo de atuação da proteção convencional. Essa eficiência é atribuída à capacidade da filosofia digital de realizar coordenação por intertravamentos lógicos, em vez de depender de atrasos temporais.

Para um curto-circuito no mesmo alimentador, mas com falha do disjuntor, seletividade lógica proposta superou novamente a filosofia de proteção convencional. Nesse teste, o tempo de atuação das proteções digitais foi 43% abaixo do tempo de atuação da proteção convencional.

Por sua vez, o quinto teste avaliou o desempenho da subestação digital quando a rede de comunicação está indisponível. Foi evidenciado que para contingência na rede de comunicação, as proteções atuam seguindo a filosofia convencional. Para garantir esse comportamento, as funções de sobrecorrente temporizada dos relés devem permanecer habilitadas e parametrizadas conforme OAP.

Esses resultados comprovam a eficiência do sistema proposto para esse cenário de falha, eliminando defeitos no sistema elétrico de forma mais rápida e, consequentemente, preservando o patrimônio físico da empresa.

Além do desempenho das proteções na proposta de digitalização da subestação, é importante ressaltar a possibilidade de implementar redundância nos intertravamentos de segurança, tanto de forma física quanto digital. Os intertravamentos físicos oferecem uma segurança robusta, mas são suscetíveis a falhas mecânicas. Por outro lado, os intertravamentos digitais proporcionam flexibilidade, monitoramento em tempo real e uma resposta mais rápida

a condições operacionais adversas. Por exemplo, no arcabouço digital, o intertravamento entre a chave seccionadora e o disjuntor à jusante incluirá um intertravamento físico, realizado pelo circuito de abertura e fechamento do disjuntor, e um intertravamento digital, por meio da assinatura de mensagens GOOSE que indicam o status da seccionadora.

Os resultados de cinco experimentos laboratoriais discutidos, confirmam que a implementação da nova filosofia de proteção, baseada na norma IEC 61850 e nos princípios da Indústria 4.0, traz melhorias significativas em termos de eficiência, segurança e agilidade operacional.

6.3 Adoção de recursos operacionais da Indústria 4.0

Os resultados obtidos demonstram que a filosofia de proteção proposta, com adoção de seletividade lógica conforme IEC 61850, em conjunto com a função 50BF, está alinhada aos princípios da Indústria 4.0, uma vez que reduz o tempo necessário para a tomada de decisão e fortalece a agilidade operacional da subestação.

Além disso, os conceitos de interoperabilidade, modularização e descentralização, inerentes a Indústria 4.0, foram observados no último teste. Os relés Sepam T87 e SEL 751, respectivamente dos fabricantes Schneider e SEL, foram utilizados para simular a reconfiguração do sistema elétrico em cenários de contingência.

A interoperabilidade é garantida uma vez que os equipamentos utilizados seguem o padrão IEC 61850. A modularização foi constatada ao ser realizado o corte de cargas não essenciais após a perda de um transformador da subestação. A reconfiguração do sistema acontece sem interferência da equipe operacional. A descentralização desta ação deve-se a definição prévia das cargas prioritárias e assinatura das mensagens GOOSE associadas à contingência no transformador.

Embora a implementação em bancada tenha atribuído o corte de carga a atuação da função 87 do IED do transformador, a restrição a nível de controlador não limita esse recurso operacional a função diferencial. A perda de um transformador pode ocorrer pela atuação de uma das suas proteções intrínsecas, como sobreaquecimento, que está associada ao modelo de processo PM-22 e disponível na rede de comunicação da subestação.

A aquisição de dados e a execução de comandos de forma remota em subestações digitais são pilares fundamentais para a implementação da Indústria 4.0 no setor elétrico. As condições ambientais e o status operacional dos equipamentos são exemplos de dados que podem ser coletados em tempo real, digitalizados pelos relés e disponibilizados na rede padrão

IEC 61850.

Além disso, a capacidade de enviar comandos de controle remotamente permite uma resposta rápida a eventos adversos, como sobrecargas e falhas, garantindo a continuidade da operação. Essa conectividade remota reduz a necessidade de intervenção humana direta, diminuindo os riscos operacionais e facilitando a implementação de estratégias de manutenção preditiva.

Por outro lado, à medida que a subestação migra para um arcabouço digital e incorpora recursos operacionais da Indústria 4.0, sua vulnerabilidade a ciberataques aumenta. Nesse contexto, o desempenho do firewall se torna crucial para a segurança cibernética, pois monitora e filtra o tráfego de dados, bloqueando acessos não autorizados e detectando atividades suspeitas. Embora esse sistema de segurança tenha sido incluído no modelo STPA da subestação digital proposta neste trabalho, não foi abordado em detalhes. Assim, surge uma oportunidade para novos estudos sobre a aplicação de firewalls avançados, juntamente com sistemas de detecção de intrusão e respostas automáticas, que possam ser implementados em subestações digitais.

6.4 Considerações finais

Neste capítulo, foi possível identificar a relevância do método STPA na avaliação de segurança em subestações digitais, destacando os requisitos operacionais que garantem a integridade da operação e a proteção dos operadores. A comparação entre os desempenhos das proteções nos cenários convencional e digital evidenciou que a digitalização, com o uso do padrão IEC 61850, proporciona ganhos expressivos em segurança. Além disso, a integração dos princípios da Indústria 4.0 demonstrou uma clara melhoria nos recursos operacionais, tornando o sistema mais eficiente e adaptável às demandas fabris.

7 CONCLUSÃO E TRABALHOS FUTUROS

Este trabalho apresentou a avaliação de segurança de uma proposta de digitalização de uma subestação industrial 69/13,8 kV no contexto de uma empresa têxtil, empregando uma metodologia unificada para analisar a transição do sistema de proteção convencional para um quadro digital, conforme o padrão IEC 61850, com a integração dos princípios da Indústria 4.0.

O método STPA foi utilizado em conjunto com o software Capella Eclipse versão 6.1 para a modelar uma proposta de digitalização de subestação industrial padrão IEC 61850, a fim de avaliar de forma qualitativa a segurança das camadas de controle e suas interações. A modelagem da subestação digital possibilitou estabelecer requisitos de segurança e introduzir conceitos da Indústria 4.0, integrando uma filosofia de proteção baseada em seletividade lógica.

O modelo digital proposto integra à subestação recursos operacionais inerentes a Indústria 4.0, como modularização e interoperabilidade. A implementação e comparação do desempenho das filosofias de proteção, juntamente com a validação dos recursos operacionais integrados no contexto digital, foram testados em bancada experimental em laboratório, a fim de validar os benefícios da filosofia de proteção proposta em comparação com o atual nível de automação da subestação industrial.

Os resultados obtidos permitem concluir que a aplicação do método STPA por meio do software Capella Eclipse é promissor para avaliação de segurança em subestações digitais. Destaca-se a identificação e controle de um ponto inseguro de operação da subestação através desse método. A aplicação da IEC 61850 mostrou-se eficaz não apenas para atribuir conceitos da Indústria 4.0, mas também para impor restrições de segurança à subestação digital.

Ao comparar a implementação da seletividade lógica com o atual cenário das proteções da subestação industrial, observa-se que o arcabouço digital reduz até 78% o tempo para eliminar falhas no sistema elétrico. O uso da mensagem de qualidade da GOOSE apresenta-se como uma solução viável para habilitar a seletividade lógica apenas quando a rede de comunicação estiver íntegra.

Em cenários de falha na rede, as proteções retornam à filosofia cronométrica. A validação da interoperabilidade para o cenário proposto, com a atuação conjunta de IEDs de fabricantes diferentes, reforça a inserção de princípios da Indústria 4.0 na subestação. Portanto, a transformação digital da subestação baseada na IEC 61850 e adoção da seletividade lógica são fortemente recomendadas.

7.1 Trabalhos futuros

Embora os resultados do presente estudo forneçam percepções significativas sobre a avaliação de segurança em subestações digitais no contexto da Indústria 4.0 por meio do método STPA, é crucial reconhecer suas limitações. Uma das principais restrições é a dificuldade de gerenciamento dos diversos cenários de perdas resultantes do STPA. Embora a IEC 61850 viabilize a implementação de diversas ações de controle, quanto maior o número de controladores da subestação, mais complexa será a avaliação dos cenários de perda por meio dessa metodologia.

Além disso, questões de segurança cibernética no contexto de subestações digitais precisam ser exploradas. Essas limitações inerentes destacam a necessidade de trabalhos futuros que incorporem métodos de gerenciamento aos cenários de perda do STPA. Além disso, modelar outros controladores da subestação digital de forma abrangente e integrá-los ao modelo proposto pode ser uma alternativa para melhor compreensão dos desafios de segurança em subestações digitais.

REFERÊNCIAS

ABRAHAM, Doney *et al*. Cyber Attack Simulation and Detection in Digital Substation. In: INTERNATIONAL CONFERENCE ON SECURE CYBER COMPUTING AND COMMUNICATIONS (ICSCCC), 3., 2023, [S. l.]. **Anais** [...]. [S. l.]: IEEE, 2023. p. 762–768. Disponível em: https://ieeexplore.ieee.org/document/10176955. Acesso em: 25 mar. de 2025.

AFTAB, Mohd Asim *et al*. IEC 61850 based substation automation system: A survey. **International Journal of Electrical Power and Energy Systems**, [s. l.], v. 120, 2020. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0142061520304646. Acesso em: 25 mar. de 2025.

AKBARZADEH, Aida *et al*. Attacking IEC 61850 Substations by Targeting the PTP Protocol. **Electronics**, [s. l.], v. 12, p. 2596, 2023. Disponível em: https://www.mdpi.com/2079-9292/12/12/2596/htm. Acesso em: 21 maio 2024.

ALKARAAN, Fadi *et al*. Corporate transformation toward Industry 4.0 and financial performance: The influence of environmental, social, and governance (ESG). **Technological Forecasting and Social Change**, [s. l.], v. 175, 2022. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0142061520304646. Acesso em: 25 mar. de 2025.

ALSAADI, Naif. Modeling and Analysis of Industry 4.0 Adoption Challenges in the Manufacturing Industry. **Processes**, [s. l.], v. 10, p. 2150, 2022. Disponível em: https://www.mdpi.com/2227-9717/10/10/2150. Acesso em: 25 mar. de 2025.

ARAVINTHAN, Visvakumar *et al*. Reliability Modeling Considerations for Emerging Cyber-Physical Power Systems. In: INTERNATIONAL CONFERENCE ON PROBABILISTIC METHODS APPLIED TO POWER SYSTEMS (PMAPS), 2018, [S. l.]. **Anais** [...]. [S. l.]: IEEE, 2018. p. 1–7. Disponível em: https://ieeexplore.ieee.org/document/8440331. Acesso em: 25 mar. de 2025.

BARBIERI, Giacomo; ESPAÑA, Adriana; SANCHEZ-LONDOÑO, David. A Taxonomy for Levels of Automation based on the Industrial Revolutions. In: IFAC-PAPERSONLINE, 2022, [S. l.]. **Anais** [...]. [S. l.]: Elsevier B.V., 2022. p. 368–373. Disponível em: https://www.sciencedirect.com/science/article/pii/S2405896322015506. Acesso em: 25 mar. de 2025.

BERTALANFFY, Ludwig von. **General System Theory**: Foundations, Development, Applications. [S. l.: s. n.], 1968.

BORGES, Sarah Francisca De Souza *et al*. Systems Theoretic Process Analysis (STPA): a bibliometric and patents analysis. **Gestão & Produção**, [s. l.], v. 28, n. 2, p. e5073, 2021. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0104-530X2021000200212&tlng=en. Acesso em: 20 maio 2024.

BOSOVSKA, Myroslava *et al*. Models of the Industrial Revolution 5.0. In: INTERNATIONAL CONFERENCE ON MODERN ELECTRICAL AND ENERGY SYSTEM (MEES), 4., 2022, [S. l.]. **Anais** [...]. [S. l.]: IEEE, 2022. p. 1–4. Disponível em: https://ieeexplore.ieee.org/document/10005761. Acesso em: 25 mar. de 2025.

CABRAL, Eduardo Almeida *et al*. Reliability assessment applied in the design of an industrial substation in the context of Industry 4.0. **Electric Power Systems Research**, [s. l.], v. 231, p. 110365, 2024. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0378779624002530. Acesso em: 25 mar. 2025.

CAPELLA. **CAPELLA MBSE Tool versão 6.1**. [S. l.: s. n.], [202-?]. Disponível em: https://mbse-capella.org/download.html. Acesso em: 20 maio 2024.

CAPELLA. **CAPELLA MBSE Tool**. [S. l.: s. n.], [202-?]. Disponível em: https://mbse-capella.org/arcadia.html. Acesso em: 19 maio 2024.

CHEN, Simin; SONG, Yu; GAO, Peng. Environmental, social, and governance (ESG) performance and financial outcomes: Analyzing the impact of ESG on financial performance. **Journal of Environmental Management**, [s. l.], v. 345, 2023. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0301479723016171. Acesso em: 25 mar. de 2025.

FREITAS, Claudivan Domingos de. **Plataforma de proteção, automação e controle de sistemas elétricos com IEDS físicos e virtuais padrão IEC 61850 orientada à aprendizagem baseada em projetos**. 2022. Dissertação (Mestrado em Engenharia) – Universidade Federal do Ceará, Fortaleza, 2022. Disponível em: http://repositorio.ufc.br/handle/riufc/74175. Acesso em: 20 maio 2024.

GHOLAMI, Mohammadreza; GHOLAMI, Alireza; MOHAMMADTAHERI, Meysam. Cyber-physical power system reliability assessment considering multi-state independent components. **Electric Power Systems Research**, [s. l.], v. 217, 2023. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0378779623000305. Acesso em: 25 mar. de 2025.

GROUMPOS, Peter P. A critical historical and scientific overview of all industrial revolutions. In: IFAC-PAPERSONLINE, 2021, [S. l.]. **Anais** [...]. [S. l.]: Elsevier B.V., 2021. p. 464–471. Disponível em: https://www.sciencedirect.com/science/article/pii/S2405896321019297. Acesso em: 25 mar. de 2025.

HAGSTRÖM, Malin Hane; BERGSJÖ, Dag; WAHRÉN, Henrik. Barriers from a socio-technical perspective to implement digitalisation in industrial engineering processes - a literature review. In: INTERNATIONAL CONFERENCE ON ENGINEERING DESIGN (ICED), 2023, [S. l.]. **Anais** [...]. [S. l.]: Cambridge University Press, 2023. p. 737–745. Disponível em: https://www.cambridge.org/core/journals/proceedings-of-the-design-society/article/barriers-from-a-sociotechnical-perspective-to-implement-digitalisation-in-industrial-engineering-processes-a-literature-review/E593C2F8C02DF9DC52E546C2E9A16752. Acesso em: 25 mar. de 2025.

HALL, Roland; SCHUMACHER, Simon; BILDSTEIN, Andreas. Systematic Analysis of Industrie 4.0 Design Principles. In: PROCEDIA CIRP, 2022, [S. l.]. **Anais** [...]. [S. l.]: Elsevier B.V., 2022. p. 440–445. Disponível em: https://www.sciencedirect.com/science/article/pii/S2212827122002888. Acesso em: 25 mar. de 2025.

HUSSAIN, Shahbaz *et al*. Vulnerabilities and countermeasures in electrical substations. **International Journal of Critical Infrastructure Protection**, [s. l.], v. 33, 2021. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1874548220300706. Acesso em: 25 mar. de 2025.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61850-7-1**: Communication networks and systems in substations, Part 7-1: Basic communication structure for substation and feeder equipment-Principles and models. [S. l.]: IEC, 2003. Disponível em: https://www.iec.ch/searchpub. Acesso em: 25 mar. de 2026

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61850-7-3**: Communication networks and systems in substations, Part 7-3: Basic communication structure for substation and feeder equipment-Common data classes. [S. l.]: IEC, 2003. Disponível em: https://www.iec.ch. Acesso em: 25 mar. 2026.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **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. [S. l.]: IEC, 2004. Disponível em: https://www.iec.ch/searchpub. Acesso em: 25 mar. 2026.

JIANG, Siwei *et al*. Complex and Intelligent Systems in Manufacturing. **IEEE Potentials**, [s. l.], v. 35, n. 4, p. 23–28, 2016. Disponível em: https://ieeexplore.ieee.org/document/7517444. Acesso em: 25 mar. 2026.

KAPIL, Vivek; PRASAD, Sheetla. Application of Industry 4.0 Technology and Internet of Things in Power Transmission Protection, Monitoring and Asset Management. In: GLOBAL CONFERENCE FOR ADVANCEMENT IN TECHNOLOGY (GCAT), 3., 2022, [S. l.]. **Anais** [...]. [S. l.]: IEEE, 2022. p. 1–8. Disponível em: https://ieeexplore.ieee.org/document/9972004. Acesso em: 25 mar. 2026.

KARANTAEV, V. G.; KARPENKO, V. I. Relevance of the Use of Combined Methods for Calculating the Reliability of the RPA of the Digital Substation in the Mass Use of ICT, Taking into Account the Impact of Cyber Attacks. In: INTERNATIONAL YOUTH SCIENTIFIC AND TECHNICAL CONFERENCE RELAY PROTECTION AND AUTOMATION (RPA), 5., 2022, [S. l.]. **Anais** [...]. [S. l.: s. n.], 2022. Disponível em: https://ieeexplore.ieee.org/document/9950784. Acesso em: 22 maio 2024.

KAUR, Harpreet *et al*. Preparing to Teach IEC 61850 Digital Substations: A Laboratory Approach. In: NORTH AMERICAN POWER SYMPOSIUM (NAPS), 2022, [S. l.]. **Anais** [...]. [S. l.]: IEEE, 2022. p. 1–6. Disponível em: https://ieeexplore.ieee.org/document/10012255. Acesso em: 25 mar. 2026.

KIMURA, Sergio *et al*. Aplicação do IEC 61850 no Mundo Real: Projeto de Modernização de 30 Subestações Elétricas. In: ANNUAL PROTECTION, AUTOMATION AND CONTROL WORLD CONFERENCE, 1., 2010, [S. l.]. **Anais** [...]. [S. l.: s. n.], 2010. Disponível em: https://www.iec.ch/searchpub. Acesso em: 25 mar. 2026.

KOPEINIG, Jacob; WOSCHANK, Manuel; OLIPP, Nadine. Industry 4.0 Technologies and their Implications for Environmental Sustainability in the Manufacturing Industry. In: PROCEDIA COMPUTER SCIENCE, 2024, [S. l.]. **Anais** [...]. [S. l.]: Elsevier B.V., 2024. p.

2777–2789. Disponível em: https://www.sciencedirect.com/science/article/pii/S1877050924002722. Acesso em: 25 mar. 2026.

KUMAR, Shantanu *et al*. Review of the Legacy and Future of IEC 61850 Protocols Encompassing Substation Automation System. **Electronics**, [s. l.], v. 12, n. 15, p. 3345, 2023. Disponível em: https://www.mdpi.com/2079-9292/12/15/3345. Acesso em: 25 mar. 2026.

LABS FOR CAPELLA. **GitHub - labs4capella/stpa-capella**: STPA Viewpoint for Capella. [S. l.], 2024. Disponível em: https://github.com/labs4capella/stpa-capella. Acesso em: 20 maio 2024.

LAZAROVA-MOLNAR, Sanja; MOHAMED, Nader. Reliability assessment in the context of industry 4.0: Data as a game changer. In: PROCEDIA COMPUTER SCIENCE, 2019, [S. l.]. **Anais** [...]. [S. l.]: Elsevier B.V., 2019. p. 691–698. Disponível em: https://www.sciencedirect.com/science/article/pii/S187705091930554X. Acesso em: 25 mar. 2026.

LEVESON, Nancy G. **Engineering a safer world**: Systems thinking applied to safety. [S. l.]: The MIT Press, 2011. Disponível em: https://direct.mit.edu/books/oa-monograph/2908/Engineering-a-Safer-WorldSystems-Thinking-Applied. Acesso em: 25 mar. 2026.

LEVESON, Nancy G.; THOMAS, John P. **STPA Handbook**. [S. l.: s. n.], 2018.

LEVESON, Nancy. A new accident model for engineering safer systems. **Safety Science**, [s. l.], v. 42, n. 4, p. 237–270, 2004. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S092575350300047X. Acesso em: 25 mar. 2026.

LIN, Chuan; XU, Qifeng. Risk Assessment of Substation Integrated Anti-Misoperation System Considering Human Reliability. **IEEE Transactions on Power Delivery**, [s. l.], v. 38, n. 3, p. 2022–2033, 2023. Disponível em: LIN, Chuan; XU, Qifeng. Risk Assessment of Substation Integrated Anti-Misoperation System Considering Human Reliability. Acesso em: 25 mar. 2026.

LOZANO, Juan C *et al*. Digital Substations and IEC 61850: A Primer. **IEEE Communications Magazine**, [s. l.], p. 28–34, 2023. Disponível em: https://escholarship.org/content/qt5kp7n3cn/qt5kp7n3cn_noSplash_d8abb0678703a222d93facc0549085e4.pdf?t=s0zkki. Acesso em: 25 mar. 2026.

MIT. **STAMP Tools**: MIT Partnership for Systems Approaches to Safety and Security (PSASS). [S. l.], [202-?]. Disponível em: https://psas.scripts.mit.edu/home/stamp-tools/. Acesso em: 22 maio 2024.

MOSCHKO, Lukas; BLAŽEVIĆ, Vera. Managing digitization of industrial incumbents through innovation-oriented leadership. **Industrial Marketing Management**, [s. l.], v. 113, p. 232–242, 2023. Disponível em: https://www.sciencedirect.com/science/article/pii/S0019850123001177. Acesso em: 25 mar. 2026.

MULAZZANI, M. Reliability Versus Safety. **IFAC Proceedings Volumes**, [s. l.], v. 18, n. 12, p. 141–146, 1985. Disponível em: https://www.sciencedirect.com/science/article/pii/S1474667017600971. Acesso em: 21 maio 2024.

NAGY, Judit *et al*. The role and impact of industry 4.0 and the internet of things on the business strategy of the value chain-the case of hungary. **Sustainability**, [s. l.], v. 10, p. 3491, 2018. Disponível em: https://www.mdpi.com/2071-1050/10/10/3491. Acesso em: 25 mar. 2026.

QUICK. **Software Quick** versão 2.02.162. [S. l.: s. n.], [202-?]. Disponível em: https://conprove.com/en/atributo/ctc/software-quick/. Acesso em: 23 maio 2024.

ROQUE, Acássio Matheus. **Considerações sobre avaliação de risco e resiliência eletromagnética em sistemas elétricos e eletrônicos**. 2022. Trabalho de Conclusão de Curso (Especialização) – Universidade de São Paulo, São Paulo, 2022. Disponível em: https://repositorio.usp.br/item/003135632. Acesso em: 25 mar. 2026.

ROQUES, Pascal. MBSE with the ARCADIA Method and the Capella Tool. In: EUROPEAN CONGRESS ON EMBEDDED REAL TIME SOFTWARE AND SYSTEMS (ERTS), 8., 2016, [S. l.]. **Anais** [...]. [S. l.: s. n.], 2016. Disponível em: https://hal.science/hal-01258014. Acesso em: 20 maio 2024.

ROSS, Alan. Reliability and safety of electric power systems: Copyright Material IEEE Paper No. ESW2021-14. **IEEE IAS Electrical Safety Workshop**, [s. l.], v. 2021-March, 2021. Disponível em: https://ieeexplore.ieee.org/document/9461505/. Acesso em: 21 maio 2024.

SAMPAIO, Raimundo Furtado. **Sistema de automação distribuído**: uma abordagem baseada em multiagente aplicada a sistemas de distribuição de energia elétrica em média tensão. 2017. Tese (Doutorado em Engenharia) – Universidade Federal do Ceará, Fortaleza, 2017. Disponível em: https://repositorio.ufc.br/handle/riufc/28423. Acesso em: 25 mar. 2026.

SANTOS, Gabriel Rodrigues *et al*. From conventional to smart substations: A classification model. **Electric Power Systems Research**, [s. l.], v. 226, 2024. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0378779623007757. Acesso em: 25 mar. 2026.

SCHWEITZER ENGINEERING LABORATORIES. **ACSELERATOR Architect Software** versão 1.1.143.0. [S. l.: s. n.], [202-?]. Disponível em: https://selinc.com/products/5032/. Acesso em: 23 maio 2024.

SCHWEITZER ENGINEERING LABORATORIES. **SEL-5030 Software ACSELERATOR QuickSet** versão 5.13.7.6. [S. l.: s. n.], [202-?]. Disponível em: https://selinc.com/pt/products/5030/. Acesso em: 23 maio 2024.

SEN, Aishwarya; BAKKA, Sowmya. A Study of Wireless Communication for Substation Automation. In: INTERNATIONAL CONFERENCE ON TRENDS IN ELECTRONICS AND INFORMATICS (ICOEI), 5., 2021, [S. l.]. **Anais** [...]. [S. l.]: IEEE, 2021. p. 606–612. Disponível em: https://ieeexplore.ieee.org/iel7/9452735/9452736/09452985.pdf. Acesso em: 25 mar. 2026.

SHARAF, Hebatallah Mohamed *et al*. A proposed coordination strategy for meshed distribution systems with DG considering user-defined characteristics of directional inverse time overcurrent relays. **International Journal of Electrical Power and Energy Systems**, [s. l.], v. 65, p. 49–58, 2015. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0142061514005791. Acesso em: 25 mar. 2026.

SHIKHIN, Vladimir; TRUTNEVA, Olga. Development of a comprehensive cybersecurity solution for an automated process control system of a digital substation. In: INTERNATIONAL YOUTH CONFERENCE ON RADIO ELECTRONICS, ELECTRICAL AND POWER ENGINEERING (REEPE), 5., 2023, [S. l.]. **Anais** [...]. [S. l.]: IEEE, 2023. p. 1–6. Disponível em: https://ieeexplore.ieee.org/document/10086782/. Acesso em: 25 mar. 2026.

SINGH, Pooja; SINGH, Lalit Kumar. Reliability and Safety Engineering for Safety Critical Systems: An Interview Study with Industry Practitioners. **IEEE Transactions on Reliability**, [s. l.], v. 70, n. 2, p. 643–653, 2021. Disponível em: http://ieeexplore.ieee.org/iel7/24/9448244/09353567.pdf. Acesso em: 25 mar. 2026.

SMITH, Paul *et al*. Towards a Systematic Approach for Smart Grid Hazard Analysis and Experiment Specification. In: IEEE INTERNATIONAL CONFERENCE ON INDUSTRIAL INFORMATICS (INDIN), 2020, [S. l.]. **Anais** [...]. [S. l.]: IEEE, 2020. p. 333–339. Disponível em: https://arxiv.org/abs/2309.07629. Acesso em: 25 mar. 2026.

SYED, Rizwan R.; HOIDALEN, Hans K. A Review on Reliability Analysis: Approaches and Tools for Digital Substation. In: INTERNATIONAL CONFERENCE ON FUTURE ENERGY SOLUTIONS (FES), 2023, [S. l.]. **Anais** [...]. [S. l.]: IEEE, 2023. p. 1–6. Disponível em: https://ieeexplore.ieee.org/document/10182937. Acesso em: 25 mar. 2026.

TAMASCELLI, Nicola *et al*. Artificial Intelligence for safety and reliability: A descriptive, bibliometric and interpretative review on machine learning. **Journal of Loss Prevention in the Process Industries**, [s. l.], v. 90, 2024. Disponível em: https://www.sciencedirect.com/science/article/pii/S0950423024001013. Acesso em: 25 mar. 2026.

WAN, Guochao *et al*. Hotspots and trends of environmental, social and governance (ESG) research: a bibliometric analysis. **Data Science and Management**, [s. l.], v. 6, n. 2, p. 65–75, 2023. Disponível em: https://www.sciencedirect.com/science/article/pii/S2666764923000097. Acesso em: 25 mar. 2026.

WATERSON, Patrick *et al*. Defining the methodological challenges and opportunities for an effective science of sociotechnical systems and safety. **Ergonomics**, [s. l.], v. 58, n. 4, p. 565–599, 2015. Disponível em: https://pubmed.ncbi.nlm.nih.gov/25832121/. Acesso em: 25 mar. 2026.

ZHANG, Zhaoyang *et al*. Composite Evaluation Method of Substation Reliability Suitable for Digital Handover Scenarios. In: ASIA CONFERENCE ON POWER AND ELECTRICAL ENGINEERING (ACPEE), 7., 2022, [S. l.]. **Anais** [...]. [S. l.: s. n.], 2022. p. 869–873. Disponível em: https://ieeexplore.ieee.org/document/9783886. Acesso em: 25 mar. 2026.

ZHAO, Zihao. Presentation of Real-time Risk Assessment Results of Substations Based on Three-color Diagrams. In: ASIA CONFERENCE ON POWER AND ELECTRICAL ENGINEERING (ACPEE), 8., 2023, [S. l.]. **Anais** [...]. [S. l.]: IEEE, 2023. p. 2201–2206. Disponível em: https://ieeexplore.ieee.org/document/10135871. Acesso em: 25 mar. 2026.