UNIVERSIDADE DE SÃO PAULO
ESCOLA DE ENGENHARIA DE SÃO CARLOS

Nilson Tinassi Peres

Uma abordagem de segurança cibernética em sistemas elétricos de potência

São Carlos

2019

Nilson Tinassi Peres

Uma abordagem de segurança cibernética em sistemas elétricos de potência

Trabalho de Conclusão de Curso apresentado à Escola de Engenharia de São Carlos, da Universidade de São Paulo
Curso: Engenharia Elétrica
Orientador: Ivan Nunes da Silva

São Carlos

2019

Ficha catalográfica elaborada pela Biblioteca Prof. Dr. Sérgio Rodrigues Fontes da EESC/USP com os dados inseridos pelo(a) autor(a).

Peres, Nilson Tinassi
P434u Uma abordagem de segurança cibernética em sistemas elétricos de potência / Nilson Tinassi Peres; orientador Ivan Nunes da Silva. São Carlos, 2019.

Monografia (Graduação em Engenharia Elétrica com ênfase em Sistemas de Energia e Automação) -- Escola de Engenharia de São Carlos da Universidade de São Paulo, 2019.

1. Segurança Cibernética. 2. Sistemas Elétricos. 3. Automação de Energia. 4. Infraestrutura Crítica. I. Título.

Eduardo Graziosi Silva - CRB - 8/8907

FOLHA DE APROVAÇÃO

Nome: Nilson Tinassi Peres

Título: "Uma abordagem de segurança cibernética em sistemas elétricos de potência"

Trabalho de Conclusão de Curso defendido e aprovado em 11/06/2019,

com NOTA 10,0 (DEZ, ZERO), pela Comissão Julgadora:

Prof. Titular Ivan Nunes da Silva - Orientador - SEL/EESC/USP

Prof. Dr. Danilo Hernane Spatti - SSC/ICMC/USP

Mestre Rafael Guedes Lang - Doutorando - SEL/EESC/USP

Coordenador da CoC-Engenharia Elétrica - EESC/USP:
Prof. Associado Rogério Andrade Flauzino

Esse trabalho é dedicado especialmente à minha família: Nilson Vieira Peres, Rosana Tinassi Peres e Luana Soares, que sempre acreditaram em mim e que sempre me apoiaram. Eu não teria conseguido sem vocês. Adicionalmente, dedico aos meus bons amigos Tiago, Gustavo, José e Álvaro que foram meus grandes parceiros nesses anos.

Agradecimentos

Agradeço primariamente a Jeová, nosso Deus e criador, sem o qual eu não estaria aqui e nem mesmo seria capaz de tal obra. Só ele merece toda honra, glória e poder (Apocalipse 4:11, Bíblia Sagrada).

Adicionalmente agradeço ao professor Dr. Ivan Nunes da Silva por ter me dado a oportunidade de desenvolver esse trabalho sob sua orientação. Espero que este trabalho o agrade e seja relevante para as futuras gerações.

Também e de igual importância, agradeço aos meus companheiros de trabalho da Siemens Jundiaí. Paulo Antunes por ter confiado em mim para desempenhar inúmeras tarefas no programa de desenvolvimento de talentos (PDT) da Siemens, entre elas participar do grande projeto de atualização e criação de um padrão global de segurança cibernética para subestações de energia. Destaco aqui, em particular, meus companheiros André Franceschett, que acompanhou de perto meu trabalho e me deu incontáveis dicas valiosas, sempre me apoiando; Fábio Barros que possui um conhecimento de redes e arquitetura de subestações inigualável e Alexandre Onça que muito me motivou a continuar lutando todos os dias "porque não existe almoço grátis".

Agradeço aos meus pais Nilson e Rosana pelo suporte que me deram nesses anos. Eu sei o quanto eles se esforçaram e se sacrificaram, física, emocional e financeiramente para me dar um lugar pra descansar, conforto pra viver e apoio para que eu nunca desistisse. Vocês são incríveis e eu me orgulho de vocês.

E agradeço à minha amada e noiva, Luana Soares. Obrigado por existir, por me amar e por me apoiar. Nenhum único dia que estive longe deixei de sonhar com quando finalmente poderíamos estar juntos, definitivamente. Obrigado por ser compreensiva e por lutar comigo as minhas batalhas. Prometo estar ao seu lado sempre e lutar contigo suas batalhas.

Finalmente, agradeço a todos os companheiros e amigos que tive e formei nesses anos, a pessoa que eu me tornei carrega um pouquinho de cada um de vocês e as nossas histórias estarão sempre guardadas no meu coração.

Obrigado a todos, que vocês encontrem a felicidade e o sucesso que merecem.

"Let's think the unthinkable, let's do the undoable. Let us prepare to grapple with the ineffable itself, and see if we may not eff it after all. Don't Panic." - Douglas Adams

Resumo

Peres, N. (2019). **Uma abordagem de segurança cibernética em sistemas elétricos de potência**. Trabalho de conclusão de curso - Departamento de Engenharia Elétrica e Computação - Escola de Engenharia de São Carlos, Universidade de São Paulo.

Esse trabalho foi motivado pela relativa fragilidade dos sistemas de automação de subestação (SAS) e pelos recentes incidentes cibernéticos em sistemas elétricos de potência (SEP), que resultaram na indisponibilidade de serviços básicos que atendem às necessidades humanas. Os objetivos desse trabalho são propor recomendações de medidas que tornem as subestações ciberneticamente mais seguras e incentivar a pesquisa na área por ser um dos poucos trabalhos acadêmicos que discutem segurança cibernética em sistemas elétricos. Os métodos utilizados são baseados em técnicas e ferramentas desenvolvidas para o ambiente de tecnologia da informação, mas que são também válidas para o ambiente de tecnologia de operação com as devidas adaptações, conforme orientado pelos manuais desenvolvidos pela Siemens para aplicação de segurança cibernética em subestações de energia. Alguns dos métodos considerados envolvem o desenvolvimento de uma arquitetura de rede segura, a redução das vulnerabilidades através da aplicação de técnicas de *hardening*, a aplicação de *softwares* que protejam contra *malwares* e uso de *backups* para recuperação em caso de incidentes. Os materiais utilizados foram cedidos pelas Siemens e consistem em computadores (estação de controle, estação de engenharia e interface homem-máquina), equipamentos de rede (*switch*, roteador e servidor NTP) e equipamentos de campo de subestação (relés digitais), além do laboratório de proteção e controle aplicado a subestações e dos *softwares* que foram necessários para execução dos testes. Os resultados obtidos consistem em uma série de recomendações e explicações baseados nos testes realizados no laboratório com auxílio da bancada de testes. Na conclusão discute-se quanto à praticidade de aplicação dessas medidas, quais são as expectativas futuras e como esse trabalho mostra-se importante para o aprendizado e para a literatura.

Palavras-chave: Segurança Cibernética. Sistemas Elétricos. Automação de Energia. Infraestrutura Crítica.

Abstract

Peres, N. (2019). **An approach of cybersecurity in electrical power systems**. Undergraduate thesis - Department of Electrical Engineering and Computing SEL - São Carlos School of Engineering, University of São Paulo.

This work was motivated by the relative weakness of substation automation systems (SAS) and recent cybernetic incidents in power electrical systems (SEP), which resulted in the unavailability of basic services that meet human needs. This work objectives are to propose recommendations of measures that make substations cybernetically safer and to encourage research in the area by being one of the few academic papers that discuss cyber security in electrical systems. The methods used are based on techniques and tools developed for the information technology environment, but are also valid for the operational technology environment with the appropriate adaptations, as guided by the manuals developed by Siemens for the application of cybernetic security in substations of energy. Some of the methods considered involve the development of a secure network architecture, the reduction of vulnerabilities through the application of hardening techniques, the application of softwares that protect against malware and the use of backups for recovery in case of incidents. The materials used were provided by Siemens and consist of computers (station controller, engineering workstation and human-machine interface), network equipment (switch, router and NTP server) and substation field equipment (digital relays), Siemens also provided the laboratory of protection and control applied to substations and all the software that was necessary to execute the tests. The obtained results consist of a series of recommendations and explanations based on the tests carried out in the laboratory with the aid of the test bench. In conclusion, the practicality of these measures is discussed, what are the future expectations and how this work is important for learning and for the literature.

Keywords: Cybersecurity. Power Systems. Energy Automation. Critical Infrastructure.

Lista de ilustrações

Lista de tabelas

Sumário

1 Introdução

O uso de soluções digitais para otimizar os sistemas existentes têm se tornado cada vez mais comum e parece um caminho sem volta.

Essa evolução constante no uso de tecnologias também afeta o sistema elétrico, onde a interconexão entre os sistemas exige uma comunicação confiável para que o serviço esteja sempre disponível.

Mas, a evolução tecnológica pode trazer junto de si algumas vulnerabilidades até então desconhecidas ou ignoradas que podem levar a resultados desastrosos.

Nesse capítulo, serão introduzidos pontos importantes desse trabalho tais como a importância da segurança cibernética em sistemas elétricos de potência, a motivação por trás do desenvolvimento desse trabalho, quis objetivos ele se propõe alcançar e como os textos desse trabalho estão organizados.

1.1 A Importância da Segurança Cibernética no SEP

Um reconhecido psicólogo americano escreveu em seu trabalho sobre a hierarquia de necessidades humanas (MASLOW; GREEN, 1943), ele subdividiu as necessidades humanas quanto à sua importância em secundárias e primárias.

As secundárias envolvem: necessidades sociais, necessidades de estima e necessidades de auto realização. Porém, mais importantes do que as necessidades secundárias, existem as necessidades primárias que segundo Maslow são a base da vida. Ele as definiu como sendo as necessidades fisiológicas e as necessidades de segurança.

Para satisfazer as necessidades primárias da humanidade, cada nação investe em setores que se tornam responsáveis por providenciar os bens e serviços que atendam essas necessidades.

As instalações, serviços e bens que compõem esses setores são de tamanha importância que a interrupção de suas operações resultaria em sério impacto social, econômico e político, comprometendo diretamente as necessidades primárias do ser humano.

Por esse motivo, esses setores são conhecidos como Setores de Infraestrutura Crítica e são responsáveis por garantir a operação contínua da provisão de bens e serviços à população em cada país. Alguns setores de infraestrutura crítica são: Setor de comunicações, setor químico, setor manufatura, setor de agricultura, setor financeiro e setor elétrico (DHS, 2019).

Portanto, pode-se afirmar que o Sistema Elétrico de Potência é um setor de

infraestrutura crítica, sendo um dos principais responsáveis por dar condições para que a população satisfaça suas necessidades primárias básicas. A interrupção de suas operações seria responsável por uma desastrosa reação em cadeia, afetando os demais setores de infraestrutura crítica e comprometendo toda a nação.

Por ser tão importante na manutenção dos serviços e operações de uma nação e capaz de consequências tão desastrosas, o setor elétrico é um dos maiores alvos de ataques realizados por organizações criminosas do setor cibernético. Mas, algumas empresas cientes da vulnerabilidade desse setor têm começado a investir na mudança desse cenário.

1.2 Ataques Cibernéticos Direcionados ao Setor Elétrico

Ataques cibernéticos em setores de infraestrutura crítica podem acontecer em qualquer nação e, por isso, todas devem investir em segurança.

Para destacar a importância de tornar os ambientes de sistemas elétricos mais seguros contra ataques cibernéticos serão considerados 3 ataques direcionados realizados na Ucrânia: *BlackEnergy*, *Industroyer* e *GreyEnergy*.

1.2.1 *BlackEnergy*, Ucrânia, 2015

O *BlackEnergy* foi um ataque que utilizou um *malware* primeiramente identificado em meados de 2007 com objetivo de executar ataques DDOS (Distributed Denial of Service), porém alguns anos foram suficientes para que esse *malware* evoluísse e se tornasse uma ferramenta poderosa e perigosa (KASPERSKY, 2017).

Às vésperas do Natal de 2015, no dia 23 de dezembro, o *BlackEnergy* foi responsável por um apagão de 6 horas afetando cerca de 230 mil pessoas na Ucrânia após comprometer importantes centros de distribuição de energia.

Esse ataque cibernético se tornou um marco na história da segurança cibernética voltada para sistemas elétricos de potência, sendo o principal responsável por atrair as atenções das empresas, organizações e instituições parte do setor. Finalmente, o setor elétrico começou a investir tempo e recursos em análises, estudos, técnicas, ferramentas e infraestrutura de segurança.

1.2.2 *Industroyer*, Ucrânia, 2016

O ataque anterior não foi um incidente isolado. Após o apagão de 2015, quase um ano depois, em dezembro de 2016 um ataque similar ocorreu, novamente na Ucrânia. Premeditado e com altos níveis de privilégio, o ataque foi orquestrado por um grupo de criminosos com bastante conhecimento sobre infraestrutura de sistemas elétricos de potência. (POLITYUK; VUKMANOVIC; JEWKES, 2017)

Esse ataque mostrou-se ainda mais preocupante para todos os órgãos e empresas envolvidas por se tratar de um ataque calculado e direcionado. Sendo executado através de um *malware* desenvolvido com características únicas do sistema elétrico, tais como a capacidade de fazer uso de protocolos de comunicação específicos do setor (IEC 101, IEC 104, IEC 61850 e OPC DA) (OSBORNE, 2017).

O setor elétrico, caracterizado por uma engenharia única e especializada e com protocolos exclusivos não estava blindado dos ataques cibernéticos. Pelo contrário, a reincidência através de um *malware* tão sofisticado e único reforçou que os sistemas elétricos de potência seriam a cada dia um alvo mais atraente para os criminosos, um alvo tão importante que esforços e recursos não seriam medidos para comprometer a operação desse setor de infraestrutura crítica.

1.2.3 *GreyEnergy*, Ucrânia e Polônia, 2016-2018

Os ataques acima citados atraíram a atenção de inúmeros profissionais e empresas de segurança cibernética. Uma de suas principais descobertas se deu com o *malware* *GreyEnergy*.

Esse software malicioso foi desenvolvido para operar sem causar danos ao sistema, projetado para ser executado discretamente e passar despercebido por todas as camadas de proteção. Nesse caso, os criminosos investiram seus esforços com outros objetivos e motivações: fazer reconhecimento, mapeamento e espionagem dentro do sistema, adquirindo informações de funcionamento e operação. Essas ações não causam danos nem falhas no setor elétrico e poderiam nunca ter sido descobertas, porém o aumento dos investimentos em segurança e infraestrutura revelou uma série de companhias de energia já infectadas pelo *GreyEnergy* por toda Ucrânia e Polônia.

Através de informações críticas de funcionamento e comportamento do sistema elétrico, os desenvolvedores do *GreyEnergy* seriam capazes de realizar um ataque ainda maior e mais prejudicial, afetando direta ou indiretamente todos os setores de infraestrutura crítica no país e dezenas de milhões de pessoas.

Esse *malware* é mais uma evidência de que os criminosos continuam à procura de vulnerabilidades e, ainda mais, continuam arquitetando seus ataques visando aumentar os danos e consequências por eles causados, reafirmando as preocupações concernentes a segurança cibernética em sistemas de infraestrutura crítica (CHEREPANOV; LIPOVSKY, 2018).

1.2.4 Resumo dos Ataques e Motivação

Brevemente se recapitulou nessa seção alguns ataques cibernéticos que aconteceram nos últimos anos, a figura 1 traz um resumo dos 3 ataques abordados e permite uma

análise e comparação entre eles.

Figura 1 – Resumo dos Ataques: *BlackEnergy*, *Industroyer* e *GreyEnergy*

BlackEnergy	Industroyer	GreyEnergy
Local		
Ucrânia	Ucrânia	Ucrânia Polônia
Consequências		
- Tipo: Apagão - Alcance: 230 mil pessoas - Duração: 6 horas	- Tipo: Apagão - Alcance: ~2,5 millhões de pessoas - Duração: 1 hora	- Tipo: Espionagem - Alcance: Não se aplica - Duração: Não se aplica
Características		
- Spearphishing (email) usado para infecção, arquivos de Excel infectavam computadores através das macros - Roubo de senhas, screenshots, roubo de privilégios de acesso - Controle remoto e destruição de discos de armazenamento.	- Desenvolvido para afetar redes de energia, infiltrado na rede através da exploração de um relé de proteção - Usado como backdoor para expor o sistema a ataques - Foco em DJ e relés, com comunicação IEC 104, IEC 61850 e OPC DA (protocolos especificos)	- Spearphishing para infecção: Web Servers contaminados para disseminar na rede local - Uso de técnicas de espionagem - Uso de técnicas de camuflagem - Roubo de senhas, informações, screenshots, entre outros

Fonte: Autoria Própria.

Esses ataques introduzem e reforçam a necessidade de investimentos (tempo, recursos e mão de obra qualificada) em segurança cibernética voltada para sistemas de infraestrutura crítica, como o Sistema Interligado Nacional (SIN).

Os ataques citados não são pontuais e de baixa complexidade, eles são ataques modernos e bem planejados que desenvolvem técnicas e ferramentas para comprometer a infraestrutura e interromper os serviços.

A motivação desse trabalho se deu a partir do estudo detalhado de casos de ataques cibernéticos em sistemas de infraestrutura crítica como o sistema elétrico de potência. No Brasil, o assunto ainda é pouco discutido pelas partes interessadas (concessionárias de energia, empresas de engenharia, órgãos reguladores, entre outros) e também é pouco tratado no meio acadêmico. Além disso, existe pouca literatura sobre o assunto em português, dificultando o acesso a informação e a capacitação de profissionais.

O setor elétrico é de extrema importância para assegurar as necessidades da humanidade, ele está em risco e existem poucas iniciativas para mudar esse cenário. Tais foram os fatores motivacionais no desenvolvimento desse trabalho.

1.3 Investimentos em Segurança Cibernética

Empresas mundialmente começaram a levar em consideração a vulnerabilidade do setor elétrico após os ataques comentados e, a partir de então, investimentos começaram a ser destinados a melhoria da segurança cibernética no setor elétrico

Uma das empresas que têm investido bastante nesse setor é a Siemens, umas das maiores empresas de engenharia do mundo e fornecedora de equipamentos utilizados na infraestrutura do sistema elétrico de potência.

Dentre as ações da Siemens voltadas para melhorias de segurança cibernética no setor elétrico, destaca-se o desenvolvimento e atualização de um padrão normativo

internacional que pode ser aplicado nas subestações por ela comercializadas.

No final de 2018, a matriz alemã da Siemens juntamente com sua filial nacional publicaram internamente uma série de manuais que totalizam mais de 1000 páginas de conteúdo com descrições, explicações e recomendações de técnicas e ferramentas que devem ser aplicadas em uma subestação digital para que ela atenda aos requisitos mínimos de segurança cibernética.

Esse trabalho de conclusão de curso foi desenvolvido com base nesse material, sendo respeitadas as leis de propriedade intelectual e industrial. Assim, esse trabalho só foi possível devido aos investimentos da Siemens e ao desenvolvimento de tal documentação completa e prática voltada para subestações digitais.

1.4 Objetivos do Trabalho

O tema abordado compreende duas áreas de bastante complexidade e abrangência, porém que através de um estudo conjunto resultam em conclusões interessantes. Assim, para desenvolvimento desse tema com base na motivação e no problema definidos, são determinados objetivos específicos e objetivos gerais que serão detalhados na sequência.

1.4.1 Objetivos Gerais

Os 2 objetivos gerais desse trabalho são:

- Propôr Recomendações: Através da documentação disponível, das hipóteses consideradas e dos resultados obtidos na bancada de testes, são propostas recomendações de técnicas e ferramentas que podem ser utilizadas em subestações digitais pertencentes ao sistema elétrico de potência;
- Incentivar a Pesquisa: Oferecer através desse trabalho, conteúdo de qualidade e relevante no idioma nacional (português) para incentivar futuros trabalhos e pesquisas que resultem na melhoria continua das soluções de segurança cibernética voltadas para aplicações nos setores de infraestrutura crítica.

1.4.2 Objetivos Específicos

Através dos objetivos gerais, definem-se alguns objetivos específicos que oferecem uma visão mais detalhada do que se deseja alcançar:

- Revisão Bibliográfica: As duas áreas grandes compreendidas por esse trabalho são Segurança da Informação e Sistemas Elétricos de Potência, assim para desenvolver o tema com qualidade um dos objetivos é estudar com maior profundidade essas áreas e obter uma visão mais sólida do assunto;

- Adquirir Experiência Profissional: O tema a ser desenvolvido está em pauta de discussão de muitas empresas envolvidas no setor elétrico, dessa forma um objetivo desse trabalho é aproximar pesquisa e mercado de trabalho, proporcionando e enriquecendo a experiência profissional e habilidades desejáveis para o mercado de trabalho como relacionamento interpessoal e competências comportamentais;

- Revisar Documentos: As preocupações com segurança cibernética são, de certa forma, recentes. Porém, em empresas como a Siemens já haviam sido desenvolvidas algumas recomendações de segurança em sistemas elétricos de potência. Assim, ao estudar a documentação antiga e desatualizada tem-se por objetivo determinar quais caminhos de desenvolvimento podem ser seguidos e quais devem ser evitados;

- Conhecimento Prático: Grande parte do desenvolvimento do tema envolve leituras e pesquisas, porém para determinar se uma medida ou recomendação foi eficaz devem ser realizados testes. Assim, outro dos objetivos foi a aprendizagem prática através da aplicação das recomendações desenvolvidas e de testes para análise dos resultados;

- Preparação de um Cenário de Testes: A aplicação das medidas e das recomendações deve atender algumas premissas básicas, dentre essas a mais importante é que esse ambiente seja uma reprodução mínima do ambiente real de uma subestação de maneira que os resultados tenham sentido e possam ser replicados em maior escala. Dessa forma, outro objetivo desse trabalho é preparar a bancada de testes;

- Elaboração de Relatórios: Através da aplicação prática dos procedimentos na bancada de testes, define-se como outro objetivo a elaboração de relatórios técnicos que descrevam como as medidas foram aplicadas e quais resultados de tal aplicação;

1.5 Organização do Texto

Definidas a motivação e os objetivos, esse trabalho está organizado através de capítulos e seções de acordo com a seguinte estrutura: Introdução, Embasamento Teórico, Materiais e Métodos, Resultados e Conclusão.

O capítulo 1 Introdução se propõe a discutir os pilares que foram base desse trabalho. Nela se discute a motivação do trabalho através da consideração de alguns ataques cibernéticos relevantes ocorridos em sistemas elétricos de potência. Também são apresentados quais objetivos o trabalho propõe satisfazer e qual a importância desse trabalho para o cenário de segurança cibernética em sistemas elétricos de potência.

O Embasamento Teórico se dá através de dois importantes capítulos que tratam de áreas distintas, mas que juntas consistem na base desse trabalho. Essas duas áreas são: Sistemas Elétricos de Potência e Sistemas de Tecnologia da Informação.

O capítulo 2 Subestações em SEP introduz os conhecimentos básicos de sistemas elétricos de potência (SEP), subestações de energia (SE) e automação de subestações (SAS). Esses conceitos são importantes para que se entenda claramente onde serão aplicadas as recomendações de segurança cibernética e porque essas medidas são necessárias. Esse capítulo utiliza como literatura base os livros Sistemas Elétricos de Potência - Automação (JARDINI, 1997) e Equipamentos de Alta Tensão - Prospecção e Hierarquização de Inovações Tecnológicas (FRONTIN, 2013). Também parte do embasamento teórico, o capítulo 3 Segurança Cibernética: Conceitos, Técnicas e Ferramentas introduz os conhecimentos de tecnologia da informação que são necessários nas aplicações de segurança cibernética em sistemas elétricos de potência. Para esse capítulo, se utiliza o livro de Computadores 5ª Edição (TANENBAUM; WETHERALL, 2011) como literatura base.

Para introduzir os materiais e métodos utilizados no desenvolvimento do trabalho utiliza-se o capítulo 4 Configuração do *Test-Bed*.

A seguir são apresentados os resultados, que consistem em uma série de comentários e recomendações, no capítulo 5 Aplicação de medidas de Segurança Cibernética em Subestações de Energia e, finalmente, no capítulo 6 Conclusão se discute se os objetivos do trabalho foram atendidos e como ele foi importante para dentro do escopo no qual se insere.

2 Subestações em SEP

Subestações de energia (figura 2) são a interface entre os sistemas de geração, transmissão e distribuição em sistemas elétricos de potência. Elas são compostas por uma série de equipamentos elétricos e podem ter diferentes objetivos como conversão (AC/DC), transformação (de níveis de tensão) e chaveamento (entre linhas de transmissão) (DONEV, 2018).

Figura 2 – Exemplo de Subestação de Energia

Fonte: (DONEV, 2018)

As subestações têm papel chave no setor elétrico e são a base dos estudos desse trabalho.

Esse capítulo introduz conceitos e equipamentos utilizados em subestações de energia, além de apresentar alguns parâmetros considerados em projetos de subestação.

Finalmente, o grande objetivo deste capítulo é introduzir a subestação digital e conceitos de automação de subestação, que envolvem os sistemas de controle e proteção e a arquitetura de rede estabelecida entre suas partes.

2.1 História das Subestações

Os primeiros projetos de subestação de energia foram desenvolvidos a mais de 100 anos e eram muito diferentes do que se vê hoje. A ABB, empresa de engenharia voltada a soluções no setor elétrico, foi uma das precursoras no desenvolvimento desses projetos que utilizavam sistemas de controle e proteção complexos e extremamente caros. Os disjuntores eram volumosos e as subestações requisitavam supervisão ininterrupta (24/7/365 - 24 horas por dia, 7 dias por semana, 365 dias do ano) e manutenção custosa constante. A maioria das operações eram executadas manualmente e havia grandes preocupações envolvendo a segurança física dos operadores envolvidos no processo.

Apesar das condições desestimulantes, as grandes empresas de engenharia reconheciam a necessidade das subestações e, por isso, fizeram altos investimentos em pesquisa e desenvolvimento para obterem melhores soluções para os problemas do sistema elétrico de potência.

Os resultados alcançados ao longo dos anos envolvem um grande aumento na capacidade de atendimento dos consumidores (maior potência), melhoria na disponibilidade do serviço e redução da necessidade de constante manutenção. Soluções para automação das operações surgiram e a velocidade dos processos aumentou significantemente (ESON; LEJDEBY, 2009).

Conforme também apontado na revista O Setor Elétrico: "Alguns desses desenvolvimentos e inovações levaram ao lançamento, nos anos 1960, do painel de manobra isolado a gás (GIS). Esses painéis, menores e mais compactos, reduziram as dimensões de uma subestação convencional com isolamento a ar em quase 90%. Nos anos 1970, a proteção eletromecânica convencional foi substituída pela proteção estática (amplificadores operacionais) e inovações adicionais resultaram nos sistemas atuais de proteção e controle numérico, incorporando múltiplas funções e tarefas, que se comunicam com outros sistemas por meio da tecnologia digital"(ESON; LEJDEBY, 2009).

As empresas de engenharia que atuam no setor elétrico garantiram que as tecnologias utilizadas em subestações de energia acompanhassem a revolução digital dos últimos 20 anos, tendo como resultado sistemas de proteção e controle inovadores que caracterizam a digitalização nos sistemas elétricos de potência, permitindo monitoramento (até mesmo remotamente) eficiente e atuação otimizada dos sistemas de controle e proteção.

2.2 Parâmetros de Subestações de Energia

A construção e comissionamento de uma subestação de energia requer grandes investimentos em recursos, tempo e mão-de-obra. Assim, projetos de subestação devem ser cautelosamente desenvolvidos para atender todos os requisitos de operação e segurança.

O escopo de atuação das subestações tem base na definição de seus parâmetros de projeto, de forma que esses parâmetros delimitam a escolha dos equipamentos e técnicas que serão utilizadas.

Alguns parâmetros de projeto que caracterizam uma subestação são:

- Tipo: Em geral subestações ser classificadas entre 3 tipos de acordo com os níveis de tensão (CSANYI, 2019):

  - Subestação de Transmissão: Em sistemas de transmissão costumam ser utilizados níveis de transmissão acima de 138kV, dessa forma as subestações de transmissão podem aumentar a tensão recebida de sistemas de subtransmissão ou de distribuição para os níveis de tensão do sistema de transmissão, ou operar a ação contrária.

  - Subestação de Subtransmissão: Atua como mediadora entre sistemas de transmissão (acima de 138kV) e sistemas de subtransmissão (entre 33kV e 138kV).

  - Subestação de Distribuição: Responsável por entregar os níveis de tensão apropriados para aplicações residenciais e/ou industriais, variando entre 11kV e 400V (os níveis de tensão entregues aos consumidores não são padronizados internacionalmente, podendo variar entre os países).

- Ação: O projeto de uma subestação depende basicamente do objetivo pelo qual ela será construída, esse objetivo pode ser determinado com base em 3 diferentes ações (ARCHANA, 2017) que podem ser executadas por uma subestação (e que podem ser combinadas), sendo elas:

  - Transformação: As subestações podem atuar como abaixadoras ou elevadoras. As abaixadoras transformam altos níveis de tensão em níveis menores e geralmente são posicionadas próximas aos centros de consumo. Por outro lado, as elevadoras transformam níveis mais baixos de tensão em altos níveis para que a transmissão seja realizada com menos perdas e, em geral, são posicionadas próximas de centros de geração de energia (termelétricas, hidrelétricas ou outros centros geradores).

  - Conversão: As tensões geradas podem ser subdivididas entre tensões de corrente contínua (DC) e tensões de corrente alternada (AC), dependendo basicamente das técnicas de geração utilizadas na unidade geradora. Porém, para meios de transmissão e distribuição, em alguns casos é mais apropriado transmitir em corrente alternada e em outros é mais apropriado transmitir em corrente contínua, por isso existem subestações cujo objetivo é converter entre AC/DC.

  - Chaveamento: A ação mais básica pela qual uma subestação pode ser projetada é para permitir um chaveamento seguro entre linhas de transmissão.

- Localização: A localização da subestação é muito importante visto que está diretamente ligada à sua utilidade e eficiência no setor elétrico (LAYTON, 2015). As empresas buscam garantir que o investimento milionário não somente traga bons

resultados, mas que traga os melhores resultados possíveis. Assim, ao escolher a localização da subestação é importante considerar alguns pontos tais como:

- Localização atual e futura dos centros de carga;

- Localização atual e futura das fontes geradores de energia;

- Existência de linhas e circuitos de distribuição e transmissão que viabilizem a subestação;

- Características do solo;

- Segurança pública;

- Segurança física da infraestrutura na localidade (contra furtos, vandalismo, sabotagem, condições climáticas, entre outros).

Conhecer alguns dos parâmetros de projeto de subestações de energia é importante para melhor entender o papel das subestações no setor elétrico e a necessidade de garantir a segurança física e digital de seus componentes.

A definição da arquitetura base desse trabalho nos capítulos seguintes será feita através de alguns dos parâmetros de projeto aqui introduzidos. A escolha dos parâmetros reduz a complexidade da arquitetura, porém garante que os aspectos segurança cibernética sejam abordados com maior clareza, sem impedir que eles sejam aplicados de forma mais abrangente.

2.3 Automação de Subestações

Segundo definido no livro Sistemas Elétricos de Potência - Automação (JARDINI, 1997), o sistema digital de automação de uma subestação tem o objetivo de prover meios para operação e manutenção desta. Esse sistema pode ser dividido em duas partes:

- Nível 1: Interface com Processo e Aquisição de Dados
  Nesse nível estão localizadas as Unidades de Aquisição de Dados (UACs) e equipamentos como relés de proteção (digitais ou não), controladores, equipamentos de oscilografia, entre outros;
- Nível 2: Comando e Supervisão (Sistema Central)
  O Sistema Central é responsável pela execução de funções como medições, monitoramento da proteção, sincronização, oscilografia, geração de relatórios, alarmes e notificações, entre outros. Esse sistema é composto por vários microcomputadores e estações de trabalho interligados através da rede.

Algumas funções básicas das subestações de energia que podem ser automatizadas através do uso de relés eletromecânicos e de sistemas lógicos são o comando de disjuntores e chaves da sala de controle, e os intertravamentos na operação de equipamentos.

Através da digitalização (transformação de dados analógicos em digitais) as subestações convertem todos os dados de supervisão, proteção e controle em saídas digitais que podem ser processadas, analisadas e aplicadas na operação. Assim, novas técnicas e funções foram desenvolvidas.

A evolução das técnicas permitiu que o controle e a proteção evoluíssem reduzindo danos sobre a infraestrutura e aumentando a disponibilidade do serviço (JARDINI, 1997).

2.4 Infraestrutura de uma Subestação de Energia

Uma subestação de energia é composta por sua infraestrutura civil, elétrica e digital.

Algumas responsabilidades referentes à infraestrutura civil de uma subestação envolvem, mas não estão limitadas à, a preparação do terreno, a construção dos prédios e salas de operação, supervisão e manutenção e o posicionamento das torres de energia (por onde passam as linhas de transmissão e distribuição).

Apesar de ser de ser importante, a infraestrutura civil não faz parte do escopo desse trabalho. Por outro lado, a infraestrutura elétrica e digital da subestação, que envolvem componentes utilizados nesses dois segmentos, devem ser introduzidos com maiores detalhes para claro entendimento dos capítulos seguintes.

2.4.1 Unidades de Aquisição e Controle - UACs

São os equipamentos responsáveis pela coleta de dados e pela realização de medidas. Esses dados são encaminhados para os centros de supervisão, controle e proteção, aonde através da análise dos dados são executadas as ações para garantir a disponibilidade dos serviços. Também, conforme bem colocado em Sistemas de Automação de SEs (SENGER, 2015), as UAC são também algumas vezes chamadas de Unidades Terminais Remotas.

Em geral os dados da UAC são obtidos através de:

- Entrada de Dados Analógica: Responsáveis pela aquisição das variáveis referentes à parâmetros físicos. Alguns exemplos são: tensão instantânea, corrente instantânea e temperatura;
- Entrada de Dados Digital: Responsável pela aquisição das variáveis de estado. Alguns exemplos são: estado de operação (em funcionamento ou inoperante) e posição (aberto ou fechado) dos equipamentos (disjuntores, relés de proteção, chaves seccionadoras, entre outros);
- Saída de Dados Analógica: Ajuste dos valores de referência (*set point*) dos componentes que podem ser definidos pelo sistema de controle. Alguns exemplos são: ajuste

do valor de saída em um regulador de tensão e ajuste da velocidade de um gerador;

- Saída de Dados Digital: Comando para ações em componentes que recebem como entrada variáveis de estado. Como exemplo têm-se o chaveamento entre aberto/fechado de equipamentos como chaves seccionadoras e disjuntores.

Os dados gerados são destinados ao sistema de controle local ou ao sistema de controle remoto referente à localidade. Devido à alta quantidade de dados gerada, apenas as informações mais importantes obtidas através desses dados são encaminhadas aos centros de controle superiores (SCADA), tais como: o estado dos disjuntores das linhas, geradores e transformadores, as potências ativas e reativas em cada elemento, e a tensão nos vários trechos de barra.

As UACs são compostas por módulos:

- Fonte: Responsável por alimentar eletricamente a UAC, é importante na definição dos níveis de tensão aceitos por suas entradas e saídas;
- Borneira: Módulo no qual estão conectadas as entradas e saídas através da fiação proveniente do campo. Essa ligação é realizada através de circuitos optoacopladores;
- Processador: Dotado da unidade central de processamento (CPU) da UAC, é responsável por realizar todas as operações e cálculos com os valores de entrada e saída.

Apesar da importância das UAC na aquisição dos dados, existem outros dispositivos inteligentes que também são muito importantes nessa tarefa, tais como os IEDs.

2.4.2 Dispositivos Eletrônicos Inteligentes - IEDs

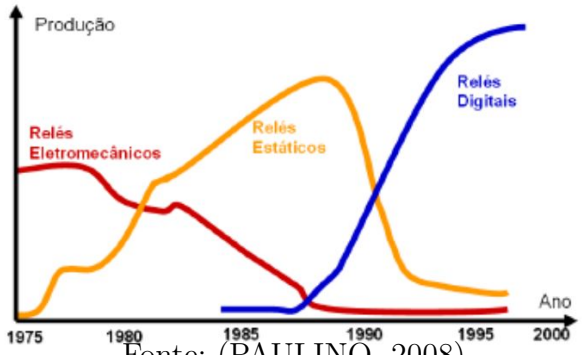
OS IEDs são dispositivos multifuncionais com funções de proteção, controle, automação, medição e monitoramento de sistemas elétricos e permitem que sejam concebidas lógicas de intertravamento e bloqueio. Em outras palavras, as IEDs são a evolução dos relés de proteção e controle eletromecânicos e estáticos.

Cada IED traz a possibilidade de expansão do sistema de proteção, essa proteção é ampliada ainda mais com a norma IEC 61850, cuja plataforma baseada em protocolos abertos e garantindo que os investimentos não sejam em vão e acompanhem o avanço da tecnologia (SANTOS; PEREIRA, 2007a).

O uso de IEDs têm aumentado continuamente nas aplicações em subestações de energia à medida que recebem mais funções, visto que dessa forma custos de implementação e manutenção são reduzidos e até mesmo a quantidade de componentes auxiliares fica menor (cabos e equipamentos adjacentes). A figura 3 traz uma visualização do cenário de produção de relés no ano de 2008, onde segundo os dados, os relés digitais haviam substituído quase completamente o uso de relés eletromecânicos e estáticos naquele ano.

Nenhum substituto para os relés digitais foi desenvolvido até o momento, porém as funções desses relés têm evoluído bastante, mantendo-os como a solução mais utilizada em subestações de energia (PAULINO, 2008).

Figura 3 – Evolução das tecnologias de relés aplicadas em função do tempo



Fonte: (PAULINO, 2008)

Também, esses dispositivos proporcionam trocas de informações mais rápidas e em maior quantidade, permitindo uma comunicação segura e sincronizada entre todos os componentes do sistema (LACERDA; CARNEIRO, 2010).

As principais funções desempenhadas pelos relés de proteção em subestações de energia são descritas no trabalho Avaliação de Desempenho de Relés de Proteção Digitais (SILVA, 2012). Para exemplificar, conheça as funções 50, 87 e 58:

- Função 50 - Proteção de Sobrecorrente Instantânea:
  Configura-se o relé para monitorar a corrente e atuar caso ela ultrapasse o valor ajustado $I_{\text{ajuste do relé}}$ (*set point*). Conforme a equação (2.1), o valor ajustado $I_{\text{ajuste do relé}}$ será maior do que a corrente nominal de operação do circuito I_{nominal}, porém será menor do que qualquer corrente de curto circuito resultante de faltas I_{CC}. A recomendação é que a corrente de ajuste seja configurada conforme a equação (2.2) para evitar acionamento da proteção em função de transitórios na rede;

$$I_{\text{nominal}} \leq I_{\text{ajuste do relé}} \leq I_{\text{CC minimo}} \tag{2.1}$$

$$I_{\text{ajuste do relé}} = 1.5 \times I_{\text{nominal}} \tag{2.2}$$

- Função 87 - Proteção Diferencial:
  A proteção diferencial monitora os valores de corrente entrando e saindo pela área delimitada pela proteção. A partir desses valores, calcula-se a diferença entre entrada e saída e verifica-se se esse valor excede o *set point* configurado para acionar a proteção;

- Função 58 - Proteção de Sobretensão:
  Análoga à proteção de sobrecorrente, essa função monitora os valores de tensão e verifica se eles excedem o valor de referência ajustado. Algumas das ações que podem

ser executadas são: envio de notificações e disparo de alarmes, chaveamento de banco de capacitores e comandos de abertura de disjuntores.

Os relés de proteção (IEDs) oferecem outras funções de similar importância, porém maior complexidade, que não serão abordadas nesse trabalho. Algumas de suas funções básicas foram aqui destacadas para oferecerem através do exemplo um entendimento mais claro de como as subestações de energia são protegidas e controladas.

2.4.3 Transformadores de Corrente - TC

Os relés citados anteriormente, bem como outros dispositivos (medidores e unidades de aquisição e controle) precisam ser alimentados pelas fontes apropriadas.

Então, para medir a corrente alternada e permitir a execução das funções a ela relacionadas, faz-se necessário utilizar o transformador de corrente (TC).

A corrente alternada que flui pelo sistema de distribuição ou transmissão em geral atinge níveis relativamente elevados. Por isso, essa corrente não pode ser utilizada diretamente como entrada (*input*) de dispositivos eletrônicos e digitais responsáveis pelo controle e processamento dos valores medidos. A injeção de altos valores de correntes em qualquer desses dispositivos resultaria em danos ao mesmo.

Assim, a necessidade dos transformadores de corrente é real. Eles são, na verdade, instrumentos de medição, que recebem como entrada a corrente alternada do sistema que em geral atinge níveis bastante elevados e opera reduzindo esses altos níveis de corrente para níveis apropriados que podem ser usados como entrada (*input*) nos demais dispositivos e controladores eletrônicos (tais como as IEDs) (FRONTIN, 2013).

Para haver precisão, os valores de saída e os valores de entrada são proporcionais através da relação de transformação do transformador. Dessa forma, por exemplo, os relés leem os valores reduzidos, mas através da relação de transformação podem obter os valores reais de corrente do sistema (conforme equação (2.3)).

$$I_{\text{real}} = \alpha \times I_{\text{saída TC}} \tag{2.3}$$

Os transformadores de corrente são um dos componentes mais importantes do sistema elétrico de potência, porém suas funcionalidades são basicamente físicas e elétricas, de maneira que não oferecem brechas de segurança que poderiam ser aproveitadas por criminosos cibernéticos.

A figura 4 traz um exemplo de TC da ABB do tipo *top core*, esse instrumento de medição pode operar recebendo tensões entre 40,5kV e 550kV, os valores de corrente do primário não podem ultrapassar 4000A.

Figura 4 – Transformador de Corrente da ABB: LVB/IMT (40,5-550 kV)

Fonte: (ABB, 2019b)

Essa seção foi baseada no Capítulo 8 (escrito por Francisco M. Salgado Carvalho) do livro Equipamentos de Alta Tensão (FRONTIN, 2013), que oferece uma análise detalhada do funcionamento dos transformadores de corrente.

2.4.4 Transformadores de Potencial - TP

Assim como o TC, os transformadores de potencial (TPs) têm como uma de suas funções dividir o circuito entre primário e secundário, sendo o primeiro deles o circuito oficial de transmissão/distribuição com os valores nominais, e o secundário sendo a alternativa desenvolvida para obter menores níveis de corrente ou tensão que possam ser utilizados nos dispositivos de medição, controle e proteção.

O transformador de potencial é dessa forma um instrumento de medição e recebe como entrada os níveis de tensão referentes ao sistema de distribuição/transmissão que, em geral, são mais altos do que os níveis de tensão permitidos para a maioria dos dispositivos eletrônicos utilizados em uma subestação digital (FRONTIN, 2013).

Através também da relação de transformação, porém agora aplicada para tensão, o transformador de potencial entrega em sua saída um valor de tensão reduzido, porém proporcional ao medido no circuito primário.

Apesar de também serem elementos essenciais em subestações de energia, assim como os TCs, os TPs são complexos física e eletricamente, mas também não oferecem funcionalidades digitais que façam deles alvos de ataques cibernéticos.A figura 5 permite

observar um modelo de TP da ABB, esse instrumento de medição pode operar recebendo tensões entre 72kV a 800kV.

Figura 5 – Transformador de Potencial da ABB: CPB (72-800 kV)

Fonte: (ABB, 2019a)

Essa seção foi baseada no Capítulo 9 (escrito por Ary D'Ajuz e Jonas de Oliveira e Silva Pinto) do livro Equipamentos de Alta Tensão (FRONTIN, 2013), que oferece uma análise detalhada do funcionamento dos transformadores de potencial.

2.4.5 GPS

O GPS ou sistema de posicionamento global foi uma das ferramentas mais importantes já desenvolvidas pelo homem e é largamente utilizado para determinação de localizações e para traçado de rotas. Através do uso de 24 satélites geoestacionários e cálculos de triangulação é possível determinar a localização de um receptor com altíssima precisão (PERES, 2016).

O GPS possui 2 funcionalidades:

- Determinação das Coordenadas do Receptor:
  Essa é a função mais conhecida do GPS e para muitos a única. Através de cálculos realizados determina-se a posição do receptor em qualquer ponto da terra ou em sua órbita instantaneamente, composta por latitude, longitude e altitude. Essa função é usada para navegação, para localização de pontos turísticos, para traçado de rotas, entre outras aplicações;
- Determinação do Tempo de Atraso:
  Essa função, bem menos conhecida, surgiu a partir da necessidade de obter posições (latitude, longitude e altitude) mais precisas. Os cálculos não levavam em conta o teorema da relatividade e, por isso, as posições calculadas eram bastante imprecisas.

Para alcançar a alta precisão hoje existente, uma nova variável precisava ser calculada para correção dos cálculos. A variável τ no sistema não linear de equações formado representava a diferença de tempo entre o receptor GPS (em geral na Terra) e os 4 ou 5 satélites usados para determinar a posição. O sistema que antes era formado por 3 variáveis (latitude, longitude e altitude) agora tinha uma 4ª variável a ser determinada, τ.

É justamente a função da determinação do tempo de atraso que é tão importante em subestações de energia. Os 24 satélites geoestacionários são dotados de relógios de precisão atômica (nanossegundos) que garantem a sincronização entre eles.

Conhecendo o tempo com precisão atômica através dos satélites geoestacionários e o tempo de atraso τ faz-se possível atualizar as medidas de tempo nos receptores GPS, obtendo assim também nos receptores precisão atômica.

Assim, receptores GPS são aplicados em subestações de energia para que através deles o *clock* de todos os equipamentos pertencentes à mesma arquitetura de rede seja sincronizado e tenha precisão atômica.

Essa ação é importantíssima para que os equipamentos atuem na ordem correta e não desencadeiem reações desastrosas. A sincronia determinada pelo receptor GPS atua como um maestro em uma orquestra, garantindo que cada componente acompanhe a melodia no tempo apropriado.

Os receptores GPS fazem parte da rede da subestação e podem ter um impacto significativo sobre o sistema de automação da subestação em caso de mal funcionamento. Por esse motivo, esse é um dos componentes que precisam ser muito bem protegidos contra ataques cibernéticos (MELLO, 2006).

A figura 6 mostra um modelo de receptor GPS desenvolvido pela GE, o RT434 GNSS *Precision-Time Clock* pertence à linha de equipamentos *Reason* da GE que pode ser utilizado em sistemas de automação de subestação e possui compatibilidade com protocolos da norma IEC 61850.

Figura 6 – GPS da GE: RT434 GNSS *Precision-Time Clock*

Fonte: (GE, 2019)

2.4.6 Outros elementos elétricos da SE

Foram citados nas subseções anteriores alguns dos elementos de grande importância para subestações de energia, porém existem outros elementos que também fazem parte

desse sistema e também executam funções importantes nesse processo. Alguns deles são:

- *Merging Unit*:
  Esse dispositivo é responsável por receber grandezas analógicas e digitais e convertê-las para um protocolo de comunicação comum (*Sample Values*) determinado pela norma IEC 61850 (VIEIRA, 2017). A partir daí, todas as grandezas medidas são transmitidas em *Sample Values* (SV) através da rede. Esse é um equipamento bastante especial visto que ele atua como intermediador da comunicação e pode se comunicar com todos os equipamentos que pertencem à arquitetura de rede da subestação. Um dos resultados da utilização da *merging unit* é a redução dos cabos entre os equipamentos, que resulta também na redução de custos (AYELLO, 2017);

- Chaves Seccionadoras:
  Esses dispositivos são utilizados em conjunto com os disjuntores para oferecer um sistema mais seguro e maior proteção em casos de faltas. Uma chave seccionadora consiste em um dispositivo de manobra com objetivo de isolar fisicamente os circuitos. Em geral, primeiro a alimentação do circuito deve ser interrompida através da atuação dos disjuntores, então com o circuito eletricamente desconectado executa-se o chaveamento para que os circuitos fiquem fisicamente isolados. Operar uma chave seccionadora em um circuito eletricamente alimentado resulta em arcos voltaicos que são muito perigosos e podem danificar os equipamentos da subestação e até mesmo ferir pessoas (BONFIM, 2016);

- Disjuntores:
  A principal função do disjuntor é proteger os equipamentos elétricos através do isolamento do circuito (FRONTIN, 2013). Em casos de falta (caracterizadas, por exemplo, pela presença de correntes de curto-circuito), o disjuntor atua interrompendo a circulação dessas correntes que atingem níveis altíssimos. Os disjuntores são equipamentos de extrema complexidade elétrica e que devem ser muito robustos para que operem com confiabilidade. São eles que garantem a integridade física dos demais elementos da subestação em casos de falta. Em geral, eles possuem dois estados: aberto ou fechado. O primeiro estado, pode ser utilizado como proteção em caso de falta ou como medida necessária para manutenção de partes do circuito. O segundo estado garante a transmissão da corrente normalmente pelo circuito.

Dentre esses 3 componentes, apenas a *merging unit* possui funções digitais que podem afetar diretamente o restante dos componentes da arquitetura. Assim, não são aplicadas medidas de segurança cibernética nem em TPs, nem em TCs, nem em disjuntores, nem em chaves seccionadoras.

Na sequência, são dados exemplos dos equipamentos acima através dos modelos de *Merging Unit* (figura 7a) e Chave Seccionadora (figura 7b) da ABB e do modelo de Disjuntor da Siemens (7c).

Figura 7 – Exemplo de Elementos de SEP

(a) *Merging Unit* ABB (b) Chave Seccionadora ABB (c) Disjuntor Siemens

Fonte: (ABB, 2019c)

Fonte: (ABB, 2017)

Fonte: (SIEMENS, 2012)

2.5 Computadores e Equipamentos de Rede

Além de equipamentos e dispositivos elétricos, as subestações de energia também são compostas por alguns elementos de tecnologia de informação, em sua maioria computadores, *switches* e roteadores.

2.5.1 *Workstation*

Os computadores são elementos conhecidos e as máquinas utilizadas em subestações não diferem muito dos *desktops* e *notebooks* utilizados em casa, no trabalho ou nas escolas pelas pessoas.

A grande diferença que caracteriza as máquinas utilizadas em subestações (*workstations*), são a alta capacidade de processamento e interfaceamento com a rede e a robusteza física para aplicação em ambientes hostis. Esses computadores industriais são equipados de proteções (contra poeira e impacto, por exemplo) e são utilizados nas subestações através da instalação de *softwares* de controle e manutenção do sistema de automação da subestação.

Algumas funções pelas quais os computadores são responsáveis são:

- Ser o mediador entre o processo operado pelos equipamentos elétricos e os operadores da subestação. Os operadores são responsáveis pelo monitoramento da subestação e pela atuação em caso de comportamento anormal não detectado pelo sistema de automação. Em um computador dedicado instala-se um *software* específico conhecido por Interface Homem-Máquina ou IHM. A IHM é uma aplicação que torna visuais todos os dados recebidos através da rede, tornando a comunicação entre homem e máquina mais clara (GOMES, 2018);
- Oferecer as ferramentas de manutenção para os engenheiros do sistema. Algumas dessas ferramentas requisitam alto poder de processamento e capacidade de operação em paralelo. Por isso, as máquinas nas quais serão instaladas essas ferramentas

precisam oferecer bom desempenho computacional;

- Oferecer o sistema de automação da subestação. O *software* responsável pela programação e controle lógico da automação da subestação desempenha ações críticas na operação do processo, por isso esse sistema costuma ser instalado em um computador dedicado, para que seja capaz de processar e analisar todos os dados gerados em campo e recebidos através da rede e para que através desses dados possa atuar com o controle.

A seguir pode-se observar um exemplo de computador industrial nas figuras 8a e 8b. A primeira delas é uma visão frontal do computador, essa é a parte que fica exposta, geralmente a *workstation* é instalada em um *rack* ou painel juntamente de outros equipamentos necessários para automação da subestação. A segunda imagem mostra a visão traseira da *workstation*, deve-se notar nessa imagem a quantidade de entradas existentes para comunicação, no caso existem 6 entradas que podem ser usadas para comunicação com outros equipamentos através da rede.

Figura 8 – Modelo de Computador Industrial

(a) Computador Industrial UNO-4673A - Vista frontal

(b) Computador Industrial UNO-4673A - Vista traseira

Fonte: (ADVANTECH, 2019)

2.5.2 *Switch*

Redes de computadores são utilizadas para comunicação através da transmissão e do recebimento de dados. Essas redes podem ser compostas por um grande número de elementos com funções diversificadas. Assim, para entendimento mais claro das funções do *switch* será usado um exemplo.

Considere o seguinte exemplo: Uma rede com 1 servidor (S1) e 10 clientes (computadores A1 até A10), nesse primeiro momento não são utilizados nem *switches* e nem roteadores.

Uma possível aplicação seria enviar uma mensagem através da rede do computador A1 para o servidor (essa mensagem pode ser uma requisição de acesso, por exemplo). Para que a comunicação seja possível, o computador A1 e o servidor S1 precisam estar interligados fisicamente, essa conexão pode ser do tipo *ethernet* com ambos conectados através de um cabo de rede. Dessa forma garante-se que o servidor irá receber a mensagem do computador A1.

Mas, se o computador A2 precisar enviar uma mensagem para o servidor S1 ele também precisará estar conectado fisicamente diretamente ao servidor. Logo conclui-se que essa abordagem não é prática. Seriam necessárias 10 conexões físicas cabeadas entre os computadores e o servidor. Muito provavelmente o servidor S1 nem possui tantas interfaces de rede para viabilizar essa comunicação.

Para resolver o problema das interfaces de rede, foi criado um dispositivo chamado *hub*. Esse dispositivo contém várias interfaces de rede e, geralmente, é instalado próximo à concentração dos computadores que formam a rede. Esse dispositivo cheio de interfaces, retransmite as informações recebidas em todas as suas interfaces. Assim, os 10 computadores seriam conectados ao *hub* através de 10 cabos conectores curtos e apenas 1 cabo longo seria necessário para conexão com o servidor. Representando uma grande melhora.

Os *hubs*, no entanto, são dispositivos sem nenhuma inteligência computacional e pertencem à Camada 1 do modelo ISO/OSI (camada física). Assim, eles também apresentam algumas falhas, por exemplo: não existe uma real necessidade de todos os computadores receberem a mensagem se ela é enviada do computador A1 ao servidor S1, até porque os demais computadores quando receberem a mensagem irão ler o seu cabeçalho e verificar que ela é endereçada ao servidor S1 e não a eles, descartando assim essa mensagem.

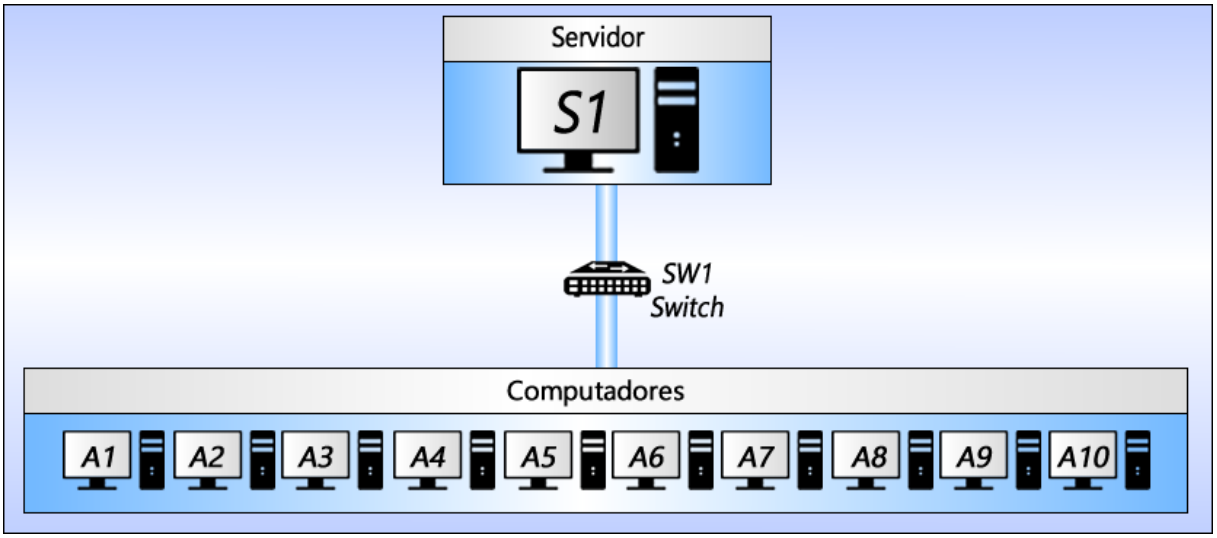
Outros problemas dos *hubs* relacionados com essa retransmissão envolvem conflitos causados quando dois computadores enviam pacotes simultaneamente e sobrecarregamento de computadores que ficam recebendo mensagens não endereçadas a eles continuamente.

Para oferecer uma comunicação entre as partes da rede de maneira mais inteligente foi desenvolvido o *switch*. Esse dispositivo pertence à Camada 2 (de enlace de dados) do modelo ISO/OSI, é composto por várias interfaces de rede (que podem ser elétricas ou ópticas) e pode receber a comunicação dos elementos de rede.

O grande diferencial do *switch* é que esse dispositivo consegue abrir os as mensagens e ler o cabeçalho delas, conhecendo assim o destino das mensagens. Então, através de uma tabela de dispositivos conectados a ele, ele encaminha a mensagem apenas para a porta que conecta com o destinatário da mensagem, tornando o processo bem mais inteligente e eficiente.

A figura 9 exemplifica a arquitetura de rede citada anteriormente, porém agora utiliza-se um *switch* como intermediador entre os computadores e o servidor, reduzindo a quantidade de portas necessárias no servidor, reduzindo a metragem de cabos a ser utilizada e oferecendo uma arquitetura de rede mais segura (TANENBAUM; WETHERALL, 2011).

Figura 9 – Exemplo de uso de *switch* para comunicação entre computadores e servidor



Fonte: Autoria própria

Na figura 10 observa-se um *switch* da RuggedCom (empresa do grupo Siemens), esse modelo é o RS900. Conforme pode ser observado, esse equipamento de rede possui várias interfaces de comunicação, algumas são elétricas e outras são ópticas.

Figura 10 – *Switch* da RuggedCom

Fonte: (SIEMENS, 2019a)

2.5.3 Roteador

O roteador é um dispositivo ainda mais inteligente do que o *switch* e pertence à Camada 3 (de rede) do modelo ISO/OSI.

Considerando novamente o exemplo anterior, agora serão utilizados 2 servidores, S1 e S2. Ou seja, será feita uma subdivisão da rede existente anterior em duas subredes.

Deseja-se que cada servidor fique responsável por 5 computadores (S1: A1,A2,A3,A4,A5

e S2: A6, A7, A8, A9, A10), assim utilizam-se 2 *switches*, o primeiro (SW1) interligará os primeiros 5 computadores com o servidor S1 e o segundo (SW2) interligará os demais 5 computadores com o servidor S2.

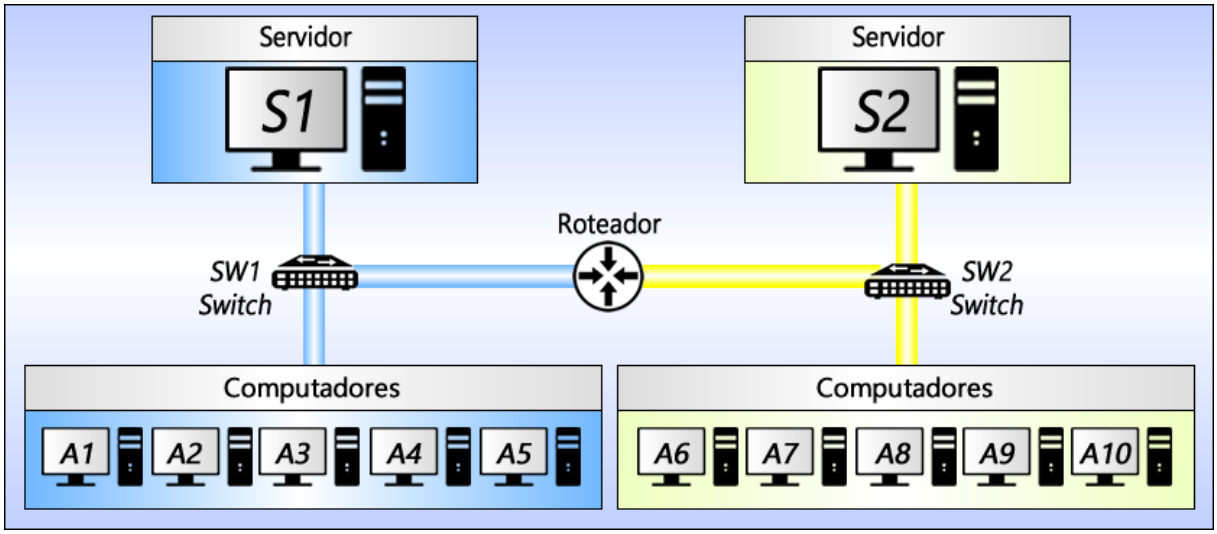
Se o computador A1 quiser se comunicar com os computadores A3 ou A5 será possível através do *switch* SW1, pois o *switch* conhece todos os demais dispositivos conectados em suas interfaces de rede.

Porém, se o computador A1 enviar uma mensagem destinada ao computador A7 essa transmissão irá falhar. O *switch* SW1 não sabe da existência do computador A7. Na verdade, apenas o *switch* SW2 tem essa informação.

Para interligar essas duas redes distintas, usa-se o roteador. Ele interligará os *switches* SW1 e SW2. Agora, caso o computador A1 deseje se comunicar com o computador A7, o *switch* SW1 sem conhecer o endereço do destinatário irá enviar a mensagem para o elemento superior na hierarquia de rede, nesse caso o roteador. Então, o roteador irá identificar que aquele endereço não foi encontrado no escopo do *switch* SW1 porque, na verdade, ele pertence ao escopo do *switch* SW2. A mensagem é então repassada ao *switch* SW2 que conhece o destinatário (computador A7) e encaminha a mensagem a ele.

A arquitetura sugerida, utilizando o roteador como solucionador do problema comentado, pode ser observada na figura 11.

Figura 11 – Exemplo uso de roteador para comunicação entre equipamentos de 2 redes distintas



Fonte: Autoria própria

Por esses motivos, roteadores são equipamentos essenciais em grandes arquiteturas de rede porque eles tornam a comunicação mais segura e eficiente, conseguem calcular as rotas mais rápidas para comunicação e garantem o uso otimizado da capacidade de comunicação do sistema (TANENBAUM; WETHERALL, 2011).

Na figura 12 observa-se um roteador da RuggedCom (empresa do grupo Siemens), esse modelo é o RX1500. Esse equipamento, assim como o *switch*, possui várias interfaces de rede.

Figura 12 – Roteador da RuggedCom

Fonte: (SIEMENS, 2019b)

2.6 Protocolos de Comunicação

Sem os equipamentos de rede seria impossível estabelecer uma comunicação eficiente entre as partes. Porém, mais do que permitir fisicamente que a comunicação aconteça, é de grande importância que as partes envolvidas falem a mesma língua, ou seja, entendam as mensagens recebidas através da rede.

Para que os dispositivos e aplicações possam se entender através da comunicação, foram criadas línguas comuns. De uma maneira mais técnica, padronizações de comunicação foram estabelecidas com regras que definiram os chamados protocolos de comunicação. Assim, um protocolo pode ser definido como "as regras que governam"a sintaxe, semântica e sincronização da comunicação e podem ser implementados por *hardware*, *software* ou por ambos.

Um artigo de sobre a norma IEC 61850 (CRISPINO, 2004) informou que existiam cerca de 152 protocolos diferentes sendo utilizados pelas concessionárias de energia elétrica para transmissão de dados, além disso eram utilizados cerca de 28 diferentes protocolos de comunicação em equipamentos específicos como sensores de temperatura, nível de óleo e pressão de gás.

Essa informação destaca que para obter um sistema de comunicação eficiente era necessário padronizar os tipos de protocolos utilizados, reduzindo a complexidade da arquitetura de comunicação entre os componentes do sistema elétrico e tornando o serviço mais seguro e confiável (COVRE, 2011).

Nas próximas subseções serão tratados alguns protocolos utilizados em subestações de energia tais como IEC 61850, IEC 60870-5-104, DNP 3.0 e Modbus.

2.6.1 A Norma IEC 61850

A 61850 é uma norma internacional definida pela Comissão Eletrotécnica Internacional (IEC). O 57º Comitê Técnico (IEC, 2019), responsável pelo desenvolvimento de padrões para troca de informação em sistemas elétricos de potência e sistemas relacionados, foi o responsável por essa padronização internacional que se encontra dividia em 10 tópicos.

A tabela 1 ajuda a entender como a norma está subdividida de acordo com seus tópicos (PAULINO, 2008). Essa norma que hoje rege as aplicações de protocolos em

Tabela 1 – As partes da norma IEC 61850

Parte	**Título**	**Função**
1	Introdução e Visão Geral	Informações básicas para entendimento e compreensão
2	Glossário	
3	Requisitos Gerais	
4	Administração do Projeto e Sistemas	Impacto da norma em ofertas e na condução do projeto
5	Requisitos de Comunicação	Requisitos básicos para aplicar a norma
6	Linguagem de Configuração de Subestação (SCL)	Impacto da norma na engenharia do projeto
7	Modelo de Comunicação	Parte principal da IEC 61850
8. 1	Mapeamento para MMS-TCP / IP-Ethernet	Como o modelo pode ser executado usando Ethernet
8. X	*para mapeamentos futuros*	
9. 1	Mapeamento para conexões ponto-a-ponto	
9. 2	Mapeamento para conexões do barramento	
10	Testes de Conformidade	Impacto da norma na verificação

Fonte: (PAULINO, 2008)

sistemas de energia começou a partir dos esforços do também internacional EPRI (*Electric Power Research Institute*) que publicou em 1999 um conjunto de padrões chamado UCA 2.0. O objetivo do UCA 2.0 era integrar padrões e fornecer uma solução para aplicar orientação a objetos (equipamentos digitais de subestação podiam ser modelados logicamente através de objetos).

Com a adesão da UCA 2.0 pelas concessionárias, a IEC decidiu se juntar à EPRI para juntos desenvolverem um padrão internacional a partir da generalização da UCA 2.0 para subestações de energia. Assim foi criada a IEC 61850, baseada em princípios tais como orientação a objetos, protocolos de rede TCP/IP e interface *ethernet*.

Nos próximos parágrafos serão expostos brevemente alguns protocolos de comunicação padronizados pela norma IEC 61850, esses protocolos são classificados de acordo com o tipo de mensagem que enviam, a tabela 2 descreve os tipos de mensagem para melhor

entendimento.

Tabela 2 – Os tipos de mensagem da norma IEC 61850

Tipo	**Classe**
1	Mensagens Rápidas
1A	*Trip*
2	Velocidade Média
3	Velocidade Baixa
4	Dados em Rajada
5	Transferência de Arquivos
6	Sincronização de Tempo

Fonte: (GURJAO; SOUZA; CARMO, 2007)

- **GOOSE**: As mensagens GOOSE (*Generic Object Oriented Substation Event*) são mensagens de comunicação horizontal referentes a eventos da subestação que podem ser modelados como objetos. Essas mensagens são do tipo *multicast* (ou seja, um remetente com vários destinatários) e carregam informações entre os relés digitais (IEDs) na subestação de energia. A informação carregada pelas mensagens GOOSE diz respeito à atuação da proteção dos relés digitais e pertence às classes 1. Mensagem Rápida e 1A. *Trip* (sinal enviado por um dispositivo de proteção para abertura do disjuntor se detectar uma falta). As mensagens GOOSE, em geral, são mensagens de alta velocidade transmitidas através do protocolo UDP (*User Datagram Protocol*) da Camada 4 (de transporte) do modelo ISO/OSI (SANTOS; PEREIRA, 2007b);

- **MMS**: As mensagens MMS (*Manufacturing Message Specification*) são mensagens de comunicação vertical utilizadas para indicar o estado dos equipamentos através de sinais digitais ou analógicos (entre IEDs e sistema de supervisão) ou para transferência de arquivos. Utiliza o protocolo TCP (*Transmission Control Protocol*) também da Camada 4 (de transporte) do modelo ISO/OSI e, por isso, são significantemente mais lentas do que as mensagens GOOSE. Assim, não é recomendado que se utilizem mensagens MMS para transmissão de informações referentes à atuação da proteção. Além disso, as mensagens MMS são do tipo *unicast*, transmitidas de um remetente para um único destinatário (VICENTE, 2011);

- **SV**: O protocolo SV (*Sample Values*) é utilizado para transmissão das medidas analógicas obtidas pelos TPs e TCs na subestação aos relés digitais que possuem conversores analógico-digital. As leituras realizadas precisam ser transmitidas aos relés em altas velocidades para garantir um rápido comando de atuação em caso de faltas, por isso pertencem à classe 1 da tabela 2;

- **SCL**: A linguagem SCL (*Substation Configuration Language*) foi desenvolvida para permitir a configuração da subestação e a especificação da relação de comunicação entre os componentes do sistema de automação da subestação. Essa linguagem

é baseada na estrutura XML (*eXtensible Markup Language*) e também define a padronização de nomenclatura dos equipamentos (LACERDA; CARNEIRO, 2010).

2.6.2 DNP 3.0 - A Solução Norte-Americana

O protocolo de rede distribuída DNP (*Distributed Network Protocol*) é outro padrão de comunicação utilizado mundialmente na automação de subestações de energia e sistemas de controle.

Enquanto o padrão europeu é definido pela norma internacional IEC 61850, em alguns países como Estados Unidos da América (EUA), o padrão DNP 3.0 é mais largamente utilizado como solução.

O objetivo do DNP é facilitar a comunicação entre os vários dispositivos responsáveis pela aquisição de dados e o sistema de controle. Alguns dos equipamentos e sistemas que podem ser configurados para se comunicar utilizando DNP são os relés digitais (IEDs), os terminais de aquisição de dados (UCA) e o sistema SCADA do centro de controle.

O DNP é um protocolo público aberto cuja interoperabilidade, longevidade e capacidade de atualização dependem de seu grupo de usuários. O comitê técnico responsável pelo DNP 3.0 avalia as mudanças ou adições sugeridas pelo grupo de usuários e então atualizam os parâmetros do protocolo (USERS-GROUP-DNP3, 2019).

O DNP 3.0 é um protocolo antigo (de 1993), mas suas constantes atualizações garantem que ele seja um protocolo robusto e confiável para comunicação, contando com algumas ferramentas de segurança que viabilizam seu uso em sistemas de automação de energia. Assim, ainda que a maior parte das aplicações sejam nos EUA, subestações no Brasil também fazem uso desse protocolo.

2.6.3 O antigo Modbus

Esse protocolo desenvolvido em 1979 para sistemas de controle de processos existe nas versões serial (Modbus RTU) e Ethernet (Modbus TCP).

O protocolo Modbus foi desenvolvido para ser utilizado nos CLPs (Controladores Lógicos Programáveis) através de uma lógica *Master-Slave*, onde o *Master* (mestre) é o equipamento que recebe informações do *Slave* (escravo), que é o equipamento que envia informações. Esse protocolo permite que até 247 equipamentos escravos se comuniquem com o equipamento mestre e, se necessário, o mestre também pode atuar transmitindo informações aos escravos.

Apesar de ter sido desenvolvido para indústria, o Modbus pode ser usado para comunicação entre componentes de uma subestação de energia, tais como IEDs. Seu uso

mais comum em subestações é para transmissão de dados entre as unidades de aquisição (Modbus RTU) e os sistemas supervisores (SCADA) (MODBUS-ORGANIZATION, 2012).

O protocolo Modbus também é um protocolo aberto e mantido por grupos de usuários. Porém, esse protocolo mais antigo possui menos ferramentas de segurança e, por isso, não é recomendável que se aplique em alguns casos em sistemas de subestações de energia.

3 Segurança Cibernética: Conceitos, Técnicas e Ferramentas

Este capítulo tem como objetivo apresentar alguns tópicos de sistemas de tecnologia da informação (TI) necessários para o entendimento claro do trabalho desenvolvido.

São abordados, mais especificamente, os conceitos, técnicas e ferramentas relacionados à segurança cibernética, muito comuns ao ambiente de TI, mas de igual relevância em ambientes de TO (tecnologia de operação).

O primeiro tópico desse capítulo discute a importância de se utilizar arquiteturas de rede seguras em projetos de tecnologia da informação, introduzindo algumas medidas que podem ser utilizadas para alcançar esse objetivo. Na sequência, são abordadas algumas estratégias de mitigação de riscos que envolvem a redução das vulnerabilidades e da superfície de ataques que poderia ser explorada por ameaças. Também são apresentados conceitos de prevenção e defesa contra *softwares* maliciosos e conceitos relacionados a um plano de resposta a incidentes que envolvem estar preparado para o pior (*backup*) e como atuar nessa situação (restauração).

3.1 Arquitetura de Redes

Uma arquitetura de rede envolve a estrutura completa da rede de computadores de uma organização. Seu diagrama oferece uma visão completa da rede estabelecida, com detalhes de todos os recursos de comunicação, incluindo:

- *Hardwares*;
- Conexões (físicas e sem fio) e tipos de dispositivos;
- *Layout* e topologias de rede;
- Área abrangida pela rede e localizações dos dispositivos;
- Regras de comunicação;
- Protocolos utilizados.

Em outras palavras a arquitetura de rede consiste no *design* físico e lógico que envolve *software*, *hardware*, protocolos e transmissão de dados.

A arquitetura é sempre projetada por um administrador de rede com coordenação de engenheiros de rede e outros engenheiros de projeto. Os projetos precisam atender requisitos de comunicação, segurança e operação do sistema, requisitando soluções robustas e inteligentes (SOUZA; CARLSON; SANTANA, 2012).

As seguintes subseções abordarão conceitos básicos e introdutórios de redes e, na sequência destes, técnicas que podem ser aplicadas como medidas de segurança em sistemas de TI através do correto projeto e planejamento de uma arquitetura de rede.

3.1.1 Conceitos Introdutórios

Para melhor entendimento das medidas propostas em arquiteturas de rede seguras, são abordados na sequência alguns conceitos básicos muito utilizados em redes de computadores.

3.1.1.1 Arquiteturas P2P e *Client/Server*

Existem diferentes tipos de arquitetura, cujo uso varia de acordo com a aplicação e os objetivos do projeto. Os dois tipos mais comuns são: P2P e *Client/Server* (SOUZA; CARLSON; SANTANA, 2012).

Em uma rede *peer-to-peer* (ou ponto-a-ponto), as tarefas são alocadas entre todos os dispositivos da rede, de forma que não há hierarquia real, todos os computadores são considerados iguais e todos têm as mesmas habilidades para uso dos recursos disponíveis. Não existe nenhum servidor central atuando como unidade compartilhada, cada computador conectado a essa rede atua como próprio servidor dos arquivos armazenados nele para os demais.

Por outro lado, em uma rede *Client/Server* (cliente/servidor) um computador centralizado e com alto poder de processamento (*server*) atua como um *hub* no qual outros computadores ou estações de trabalho (*client*) se conectam. Este servidor é o coração do sistema, que gerencia e fornece recursos para qualquer *client* que os solicite.

Em geral, aplicações de rede P2P são mais baratas e continuam em funcionamento ainda que algum dos computadores pare de funcionar, diferente das redes cliente/servidor que são mais caras dada a necessidade de um poderoso servidor central e oferecem uma comunicação muito mais segura entre os *endpoints*, mas que podem ter a operação completamente interrompida em caso de falhas do servidor (caso que pode ser contornado pelo uso de redundância de rede).

3.1.1.2 Modelo ISO/OSI

Um dos conceitos mais importantes que devem ser introduzidos para entender bem uma arquitetura de rede segura é o modelo de divisão da arquitetura através de camadas.

O modelo OSI (*Open Systems Interconnection*) foi estabelecido e proposto pela Organização Internacional para Padronização (ISO), por isso é chamado modelo de camadas ISO/OSI. São utilizadas 7 camadas para subdivisão o problema, de maneira que cada protocolo tenha suas funcionalidades correlatas a uma determinada camada.

As camadas do modelo ISO/OSI são:

1 Camada Física: Responsável pela conexão física entre os sistemas (seja ela ponto-a-ponto, multiponto, *half duplex*, *full duplex*, serial ou paralela). Aborda também as características técnicas dos meios de transmissão, sejam eles elétricos ou ópticos (fios, conectores, níveis de tensão, taxa de dados, entre outros). Seu objetivo é assegurar uma comunicação simples e confiável entre as partes;

2 Camada de Enlace: Também é conhecida como camada de *link* de dados, é capaz de detectar e tratar alguns erros ocorridos na camada física. Realiza o controle de fluxo e a delimitação de quadros (*frames*). É responsável pelo *link* (ligação) com o meio físico. Em redes do tipo Ethernet, por exemplo, cada placa de rede deve possuir um endereço de rede único para atender os requisitos de comunicação;

3 Camada de Rede: É responsável pelo endereçamento dos pacotes, capaz de ler os endereços de rede e convertê-los em endereços físicos (*MAC address*). Outra função dessa camada é determinar qual a rota que os pacotes devem seguir para chegar ao seu destino (com base em condições de tráfego e prioridade);

4 Camada de Transporte: Para enviar os dados entre transmissor e receptor, é necessário que os dados sejam subdivididos em porções menores. Dessa forma, um dado é formado pela união de uma série de pacotes recebidos. A camada de transporte é a camada responsável por organizar a divisão dos dados em pacotes no transmissor e por organizar a união dos pacotes no receptor. Ela é chamada camada de transporte não por executar o transporte, mas por ser responsável pela preparação dos pacotes imediatamente antes deles serem transportados e após eles serem recebidos. Ela faz a ligação entre as camadas de aplicação (camadas 5 a 7) e as camadas físicas (1 a 3);

5 Camada de Sessão: Essa camada fornece os mecanismos para abertura, fechamento e gerenciamento de sessões de comunicação entre dois processos, permitindo a comunicação entre dois computadores diferentes. Ela é responsável por definir como será feita a transmissão e quais dados serão transmitidos;

6 Camada de Apresentação: Atua na tradução dos dados gerados pela e para camada de aplicação (7). Se a camada de aplicação está recebendo dados através de uma sessão, esses dados são enviados em pacotes que seguem a estrutura do protocolo definido, mesmo após a união dos pacotes, o dado original permanece configurado na estrutura utilizada pelo protocolo de comunicação, então é responsabilidade da camada de apresentação traduzir esse dado para a estrutura utilizada pela aplicação de maneira que ele possa ser apresentado. De maneira similar, uma aplicação que irá enviar um dado, requisita à camada de apresentação que ela traduza o dado na estrutura do protocolo que será utilizado na sessão de comunicação;

7 Camada de Aplicação: Responsável pela leitura e entendimento dos dados traduzidos e pela utilização desses dados em suas funções. É nessa camada que os dados são manipulados para gerar alguma saída que faça sentido para o usuário.

Muitas referências ao modelo de camadas ISO/OSI são feitas durante discussões que envolvem protocolos e *firewalls*. A breve introdução aqui apresentada é base suficiente para entendimento dos tópicos seguintes.

3.1.2 Segmentação de Rede

A segmentação de rede é um mecanismo de proteção poderoso cuja ideia fundamental é agrupar elementos de rede com requisitos de segurança similares, realizando uma separação física da rede em subredes (ou se possível utilizar a virtualização, criando uma separação virtual entre elas).

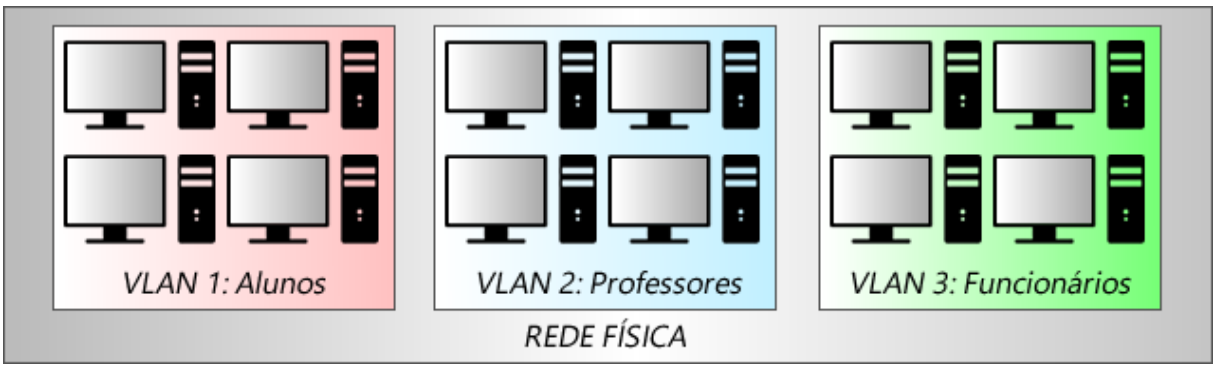
Essa segmentação é realizada por separar as redes utilizando-se de elementos de rede dedicados como *firewalls* ou roteadores que possuem essa função. Através desses elementos os controles de segurança apropriados são definidos de acordo com os níveis de segurança exigidos para cada segmento da rede.

A segmentação da rede pode ser categorizada de diferentes maneiras: de acordo com as funções dos usuários, de acordo com a hierarquia da empresa, de acordo com níveis de segurança, entre outras possibilidades.

Para exemplificar, considere que uma escola deseja criar através de sua rede interna um sistema de compartilhamento de arquivos entre os computadores de seus alunos, funcionários e professores.

A figura 13 sugere uma segmentação categorizada de acordo com a função dos usuários, nela observe que foram criadas 3 VLANs (*Virtual Local Area Network*) que dividem a rede de acordo com os papéis de cada usuário, resultando em uma rede para professores, uma rede para alunos e uma rede para funcionários.

Figura 13 – Exemplo de Segmentação de Rede usando VLANs



Fonte: Autoria própria

Considerando ainda estas 3 redes virtuais criadas, faz-se necessário utilizar métodos e ferramentas auxiliares para monitorar e controlar a comunicação entre elas, as próximas duas subseções (*Firewall* e *Intrusion Detection and Prevention Systems*) tratarão destes aspectos.

3.1.3 *Firewall*

O *Firewall* é um sistema de segurança da rede que pode ser baseado em *software* ou *hardware* e que controla o tráfego de rede com base em um conjunto de regras definido, esse conjunto reconhece o protocolo de comunicação e os *endpoints* que se comunicam entre si.

Alguns *softwares* que executam funções de *Firewall* são (TECHTUDO, 2014):

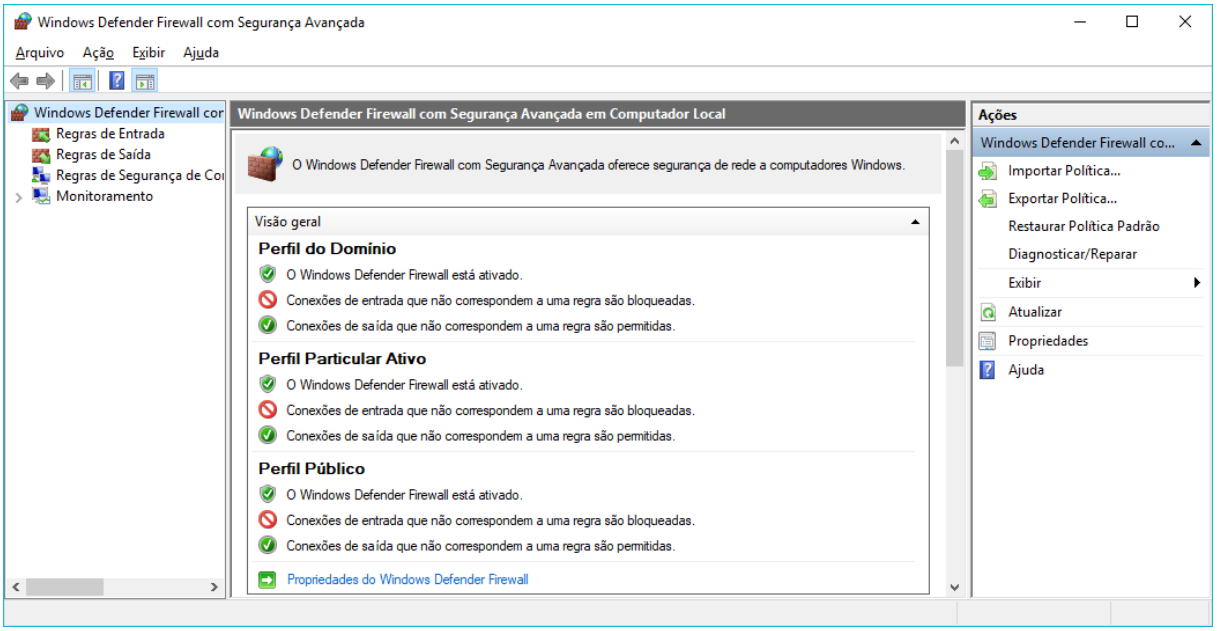
- *Firewall* do Windows (veja figura 14): Essa aplicação nativa do sistema operacional oferece todas as funcionalidades básicas necessárias para configuração de regras e controle do tráfego de rede. Também oferece algumas configurações mais avançadas que podem ser configuradas por engenheiros de rede experientes. Trata-se de uma poderosa ferramenta gratuita;

- AVG *internet security*: Um pacote de ferramentas muito reconhecido por suas funções *anti-malware*, mas que também oferece soluções para controle de tráfego de rede e regras de comunicação (*firewall*). Apesar de oferecer algumas funcionalidades gratuitas, essa ferramenta mostra-se muito mais versátil em sua versão paga;

- *ZoneAlarm Firewall*: Essa aplicação oferece gratuitamente as funções necessárias para configuração de um *firewall* robusto e eficiente. A diferença essencial para o *firewall* oferecido nativamente pelo Windows é que essa aplicação oferece algumas soluções extras tais como: conexão com a *DefenseNet* que fornece atualizações em tempo real e detecção de novas ameaças, proteção otimizada para computadores conectados a pontos públicos de internet sem fio e 5GB de armazenamento em nuvem.

Porém, existem vantagens em utilizar aplicações físicas de *firewall* tais como centralizar todo o processamento de regras em um dispositivo dedicado confiando a ele a tarefa de controlar e monitorar o tráfego de maneira otimizada e mais eficientemente do que em soluções de *software*, sem sobrecarregar os servidores com essas tarefas e com tráfego desnecessário. Outra vantagem das aplicações de *firewall* físico é que elas podem ser utilizadas em dispositivos que não possuem soluções de *software* aplicáveis (como casas inteligentes com geladeiras, televisões, sistemas de controle de temperatura, entre outros, que se comunicam através da rede e não oferecem muitas alternativas de segurança).

Figura 14 – *Firewall* nativo do Windows



Fonte: Autoria própria

Alguns exemplos de *hardware* usado como *firewall* são (LIQUIDWEB, 2018):

- *Bitdefender Box 2*: Esse *firewall* voltado para casas inteligentes e aplicações similares oferece monitoração da rede através de um aplicativo, além de varrer a rede em busca de vulnerabilidades e oferecer as ferramentas básicas que um *firewall* precisa;
- *SonicWall* TZ400 (conforme figura 15): Esse modelo é bem mais robusto e usado em soluções empresariais. Possuindo alta velocidade de processamento e altas taxas de transmissão, esse *hardware* tem interferência quase nula na latência da rede. Também oferece ferramentas mais poderosas como defesa automática de ataques de negação de serviços (DoS).

Figura 15 – *Firewall* físico *SonicWall* TZ400 voltado à aplicações empresariais.

Fonte: (SONICGUARD, 2019)

Além da divisão entre *firewall* físico e *software*, também podem ser divididos em duas outras categorias:

- *Network Firewall*: Atuam filtrando o tráfego entre duas ou mais redes;
- *Host-Based Firewall*: Atuam filtrando o tráfego que chega e sai das máquinas.

Independente da categoria pertencente, os *firewalls* podem executar as seguintes ações: *Packet Filtering*, *Stateful Inspection* e *Application Layer Firewall*, mais detalhes sobre cada uma dessas ações serão explorados nos próximos tópicos.

3.1.3.1 *Packet Filtering*

O filtro de pacotes é uma aplicação de *firewall* executada na camada 4 do modelo ISO/OSI. Essa ação consiste em inspecionar os pacotes transferidos entre os computadores.

O *firewall* recebe o pacote e compara ele com um conjunto de regras pré-definido, se o pacote atender os requisitos então o *firewall* permite que o pacote seja entregue ao computador, aplicação ou processo.

Se o pacote não atende os requisitos ele poderá então ser descartado (sem gerar mensagens) ou rejeitado (enviando uma notificação ICMP para o remetente do pacote).

Algumas das configurações que podem ser usadas para filtrar pacotes são:

- IP 1: Endereço de rede do Remetente;
- Port 1: Porta de envio do Remetente;
- IP 2: Endereço de rede do Destinatário;
- Port 2: Porta de destino do Destinatário.

Apesar de ser um método eficiente ele se mostra vulnerável contra alguns tipos de ataque como *IP Spoofing*.

3.1.3.2 *Stateful Inspection*

A ação *Stateful Inspection* é uma evolução da anterior e por isso também pode ser referenciada como *Dynamic Packet Filtering*. O filtro dinâmico de pacotes também é executado na camada 4 do modelo ISO/OSI e fornece níveis adicionais de segurança que corrigem problemas como a vulnerabilidade contra *IP Spoofing* citada anteriormente.

Essa tecnologia mantém uma tabela atualizada que monitora todas as conexões abertas, assim quando um pacote é recebido suas informações de cabeçalho são comparadas com as informações da tabela e isso determina se aquele pacote é parte de uma conexão já estabelecida.

Se o pacote recebido for parte de uma conexão já existente ele é aceito, senão um conjunto de regras pré-definido é verificado para validar ou não a criação de uma nova conexão e aceitar esse pacote.

Apesar de monitorar toda a comunicação (envio e recebimento de pacotes), o *firewall Stateful Inspection* apresenta 2 problemas:

- É vulnerável a ataques de negação de serviços (DoS);

- Não permite o monitoramento do conteúdo dos pacotes (visto que ele trabalha na camada 4 do modelo ISO/OSI e somente checa o cabeçalho da mensagem).

Esses problemas são herança dos *firewalls* que executam *Packet Filtering*, descritos na subseção anterior.

3.1.3.3 Application Layer Firewall

Essa é a aplicação de *firewall* mais inteligente, a diferença essencial que torna esse *firewall* interessante é que ele atua na camada de aplicação do modelo ISO/OSI (camada 7). Assim, ele oferece maior controle sobre os pacotes, possuindo acesso aos dados que são enviados a aplicações ou que são gerados por elas.

Esse tipo de *firewall* permite que se examine o conteúdo das mensagens, aumentando a segurança contra ataques que manipulam o conteúdo dos pacotes inserindo neles códigos maliciosos disfarçados. Esse tipo de *firewall* permite também que engenheiros de segurança tenham um controle mais granular sobre o tráfego na rede e configurem um conjunto de regras para permitir ou negar ações ou comandos específicos do sistema.

Alguns dos protocolos que podem ser controlados utilizando AppLaFW são muito utilizados em sistemas elétricos de potência e automação de subestações, tais como: RDP, SNMP, NTP, IEC104, entre outros.

3.1.4 *Intrusion Detection and Prevention Systems*

Os Sistemas de Detecção de Intrusão (IDS) e os Sistemas de Prevenção de Intrusão (IPS) são ferramentas inteligentes, com algumas propriedades similares e algumas leves diferenças. Esses sistemas atuam nas camadas 3 a 7 do modelo ISO/OSI.

Um Sistema de Detecção de Intrusão é um equipamento ou aplicação de software que monitora a rede ou os sistemas ativos contra atividades maliciosas e violação de políticas e produz reportes eletrônicos para um centro de gerenciamento.

Em geral, são gravadas as informações dos eventos observados e são enviadas as devidas notificações de segurança aos administradores do sistema. Qualquer atividade maliciosa ou violação deve ser reportada aos responsáveis e os dados coletados devem ser disponibilizados através de aplicações SIEM (*Security Information and Event Management*).

O IDS pode atuar em dois escopos (similarmente à categorização dos *firewalls* anteriormente), seja monitorando sistemas "*host-based*"(computadores) quando é chamado HIDS ou monitorando redes (*network IDS*) quando é chamado NIDS.

Um exemplo de ferramenta NIDS/NIPS conhecida e utilizada é o *software open source* SNORT. Essa aplicação gratuita tem a habilidade de realizar análise de tráfego

em tempo real e registro de pacotes em redes IP, além de fornecer funções de análises, pesquisa e correspondência entre protocolos. Alguns ataques que podem ser detectados pelo SNORT envolvem, por exemplo: ataques de URL semânticos, *buffer overflow* e *stealth port scans* (SNORT, 2019).

Existem também os Sistemas de Prevenção de Intrusão (IPS), a diferença essencial entre eles é o fator responsivo existente nessa segunda tecnologia. Ela não só monitora e detecta o ataque, mas também permite reagir contra ele através de uma retaliação automática. Algumas dessas ações são a reconfiguração do *firewall* ou a manipulação do conteúdo do pacote considerado malicioso.

3.2 *Hardening* do Sistema

Hardening são todas as medidas usadas para tornar um sistema mais seguro por reduzir a superfície de vulnerabilidades existentes que é tão grande quanto a quantidade de funções executadas pelo sistema. Ou seja, um sistema que realiza uma única função possui muito menos vulnerabilidades do que um sistema que executa centenas de funções. Reduzir os caminhos que podem ser aproveitados pelos atacantes inclui alterar as senhas padrão, remover *softwares* não necessários, remover usuários não utilizados e desativar serviços e funções inoperantes.

Hardening também pode-se referir a limitar a superfície de ataque através da aplicação de configurações específicas sobre o sistema, essas configurações podem ser aplicadas sobre o sistema operacional, sobre softwares proprietários e terceiros e também sobre equipamentos de rede.

Dessa forma, o *Hardening* do sistema garante que todas as partes da solução utilizem uma configuração segura.

Algumas ações que podem ser executadas para reduzir a superfície de ataques:

- Desativar ou remover contas de usuários;
- Modificar e configurar as contas existentes de acordo com os papéis dos usuários;
- Remover serviços e programas dos quais não se faz uso;
- Aplicar alterações nas permissões de arquivos e do sistema operacional;
- Aplicar alterações nas permissões de *hardware*;
- Desativar portas de *hardware* que não serão utilizadas.

A partir dos pontos acima comentados, conclui-se que *Hardening* não consiste em uma atividade única, singular. Pelo contrário, envolve todo o ciclo de vida do produto, desde seu desenvolvimento até o comissionamento do sistema. Por isso, as medidas de

hardening em geral estão relacionadas com uma série de outras medidas de arquitetura segura, proteção contra *malware*, *patching* de segurança, entre outras.

Alguns exemplos de *Hardening* são brevemente descritos a seguir, porém as próximas subseções detalharão algumas técnicas eficientes em reduzir a superfície de ataque de um sistema.

- *Hardening in Hardware*: Bloquear através do sistema operacional portas físicas que não são usadas ou removê-las fisicamente quando necessário, garantir que os equipamentos físicos (roteadores, *switches*, computadores) estejam protegidos fisicamente em salas de acesso controlado (de forma a evitar acesso não autorizado à infraestrutura física de TI) e remover componentes de *hardware* que não são utilizados para a solução proposta;
- *Hardening in BIOS*: Configurar a senha de acesso à BIOS de forma que o acesso às suas configurações só seja permitido ao administrador do sistema;
- *Hardening in Operating System*: Sugere-se seguir as recomendações do CIS (*Center for Internet Security*) sempre que essas recomendações não afetarem a disponibilidade de entrega do serviço (CIS, 2019);
- *Password Policies*: Recomenda-se mínimo de 8 caracteres, letras maiúsculas e minúsculas, com um ou mais dígitos numéricos e caracteres especiais. Pode ser recomendado alterar as senhas a cada 90 ou 180 dias.

Além dessas recomendações, sempre que uma função ou software novo for adicionado ao sistema, novas configurações de *hardening* precisam ser executadas de acordo com os requisitos de segurança apropriados.

3.2.1 Controle de Acesso e Gerenciamento de Contas

Uma das ações mais básicas quando se trata de *hardening* é controlar o acesso aos produtos, soluções ou infraestruturas que compõem o sistema para reduzir sua exposição frente a ameaças de ataques.

As medidas aplicáveis envolvem o controle de acesso físico e lógico (digital) dos envolvidos no processo. Tais medidas devem garantir que apenas os usuários autorizados tenham acesso a sistemas, instalações e informações, e que esse acesso seja limitado às funções que esses usuários executam. Mostrando-se uma medida eficiente de segurança e de redução da superfície de ataques por proteger dados, equipamentos e instalações contra perda, danos ou alterações não autorizadas.

O controle de acesso físico consiste em barreiras físicas que previnem a entrada em ambientes ou áreas de acesso controlado e pode, por exemplo, ser executado através

de cadeados, portas eletrônicas e sistemas de acesso digitais, exigindo chaves, cartões identificadores ou autenticação biométrica para liberação do acesso.

Por outro lado, o controle de acesso lógico, diz respeito a recursos na sua maioria digitais. Alguns exemplos de recursos que devem ser protegidos através do controle de acesso lógico:

- Aplicações: O acesso não autorizado ao código fonte de uma aplicação pode permitir que usuários mal-intencionados alterem algumas das funções que a aplicação desempenha com objetivos maliciosos;
- Arquivos de Dados: Bases de dados, arquivos e transações podem ser apagados, roubados ou alterados;
- Sistema Operacional: Por ser a base de execução de muitas aplicações e configurações pode ser utilizado como caminho para que os usuários mal-intencionados atinjam seus objetivos.

Em geral, usuários mal-intencionados quando conseguem acesso a aplicações, sistemas e/ou instalações, os exploram para obterem vantagens próprias ou para prejudicarem os usuários reais destes.

Postuladas tais informações, as premissas do controle de acesso lógico são:

- Apenas usuários autorizados podem acessar os recursos;
- Somente são disponibilizados os recursos referentes às tarefas do usuário;
- O acesso a recursos críticos é bem monitorado;
- O número de usuários com acesso aos recursos críticos é bastante limitado.

Sistemicamente, o controle de acesso lógico é realizado através da autenticação do usuário que possui um identificador único (ID do usuário) e uma senha que somente ele deve conhecer. Tanto a senha quanto o identificador são checados em uma base de dados criptografada para permitir ou negar o acesso (SEFTI, 2012).

Alguns sistemas mais críticos fazem uso da autenticação multifator, que exige que o usuário realize uma autenticação extra. Os fatores de autenticação possíveis são:

- *Something you know*: Consiste em senhas (maioria) ou em resposta a perguntas que se assume somente o usuário conhecer;
- *Something you have*: Pode ser realizado através de cartões, *tokens* ou outro item que o usuário deve carregar junto de si e que pode ser autenticado digitalmente;
- *Something you are*: Em geral realizado através de autenticação biométrica, checa alguma condição física do usuário que seja única do mesmo (leitura da íris ou impressão digital).

Além do controle de acesso, o gerenciamento das contas também é muito importante visto que é através dele que são configurados os papéis e as permissões de cada usuário de acordo com suas funções no sistema.

As aplicações e sistemas diferem entre si sobre qual a granularidade de configuração de privilégios dos usuários, assim faz parte de grandes projetos que se definam bem grupos de usuários. Como exemplo prático, em subestações de energia alguns grupos de usuário existentes são: administradores do sistema, engenheiros do sistema, operadores do sistema e convidados (*guests*).

3.2.2 Registros e Monitoramento de Segurança

Logging é a palavra utilizada para se referir a *log* de dados, que consiste no registro de eventos relevantes em um sistema.

Registrar informações relacionadas com a saúde e disponibilidade das funções e aplicações de um sistema é de importância chave na sua segurança. Porém, além de registrar, monitorar os dados registrados também é de suma importância em um ambiente protegido ciberneticamente.

O monitoramento pode ajudar a identificar comportamentos suspeitos no sistema e também pode auxiliar na reação em caso de ataques.

Possuir registros detalhados dos eventos de um sistema permite investigar incidentes e/ou ataques sofridos, assim as falhas e vulnerabilidades são identificadas e corrigidas para mitigar riscos de futura reincidência (PHINNEY, 2019).

3.2.3 *Patching* de segurança

Um *patch* consiste em uma série de mudanças aplicadas sobre o conjunto de dados de um computador, aplicação ou processo com objetivo de corrigir ou melhorar as funções por ele desenvolvidas. Um *patch* de segurança é, dessa forma, um pacote aplicado para correção de vulnerabilidades identificadas no computador, aplicação ou processo e consiste em uma ação preventiva para mitigar a capacidade de exploração das vulnerabilidades pelos atacantes.

Deve-se pontuar que as aplicações e processos estão sendo atualizados constantemente, recebendo novas funcionalidades e ferramentas. As novidades podem, no entanto, ser fontes de vulnerabilidades até então desconhecidas, requisitando assim que novas atualizações focadas na manutenção da segurança sejam aplicadas.

Assim, para atender constantemente os níveis e requisitos de segurança do sistema é importante que exista um processo de gerenciamento de atualizações de segurança de todos os componentes relevantes do sistema.

A norma IEC 62443 possui um capítulo específico para tratar das recomendações de gerenciamento de patches, essa norma deve ser seguida como requisito sempre que possível.

3.3 Proteção contra *Malware*

A proteção contra *malware* consiste no uso de tecnologias que forneçam ferramentas e técnicas que atuem na prevenção contra infecção de um sistema por *softwares* maliciosos, sendo essencial em todos os ambientes de TI e, em especial, aqueles que envolvem arquiteturas de redes complexas e sistemas de controle (tais como o Sistema Elétrico de Potência).

Existem duas abordagens para proteção contra malware, sendo elas a de *Blacklisting* e a de *Whitelisting*, que serão abordadas em mais detalhes nas subseções seguintes.

Cabe destacar, no entanto, que é possível utilizar as duas abordagens em um mesmo sistema para alcançar níveis mais elevados de segurança. Essa ação deve ser considerada cautelosamente para não influenciar a disponibilidade do sistema.

3.3.1 *Blacklisting*

A abordagem de (*blacklisting*) é a mais utilizada em aplicações de proteção contra *malware*, sendo a técnica base por trás dos *softwares* antivírus.

Para melhor entendimento, considere as autoridades responsáveis pelo controle de tráfego de pessoas em um aeroporto internacional. Cada pessoa que deseja entrar ou sair do país tem suas informações verificadas em um número incontável de banco de dados (polícia local, polícia internacional, hospitais, entre outros). O sistema de pesquisa automaticamente gera relatórios e alertas para as autoridades se encontrar qualquer problema relacionado aquela pessoa para que uma investigação mais detalhada seja executada. Ou seja, cada nome é verificado em várias listas.

Basicamente, a técnica de *blacklisting* utilizada pelos antivírus consiste em uma execução similar. Cada empresa desenvolvedora de antivírus possui em seu banco de dados uma listagem de assinaturas de todos os vírus que já foram encontrados anteriormente. Sempre que se executa um novo *software* no computador, a assinatura dele é cruzada com o banco de dados da desenvolvedora do antivírus. Se a assinatura dele for encontrada nesse banco de dados ele é então classificado como um *software* malicioso ou *malware* e suas ações são bloqueadas.

Para ser funcional, o método de *blacklisting* requer que o antivírus esteja constantemente atualizado com os mais recentes bancos de dados (que irão incluir as assinaturas de *malwares* recém descobertos). Por isso, em infraestruturas onde o acesso à internet é

limitado, deve-se considerar a criação de processos para atualização periódica das bases de dados (*blacklists*).

Uma aplicação de *blacklisting* pode atuar de diferentes maneiras, sendo as duas mais comuns: 1. Varredura de arquivos recém baixados e de *softwares* e processos recém executados; e 2. Varredura completa dos arquivos do sistema.

O método de *blacklisting* é muito eficiente como proteção de ataques não-direcionados, tipo de ataque caracterizado pela criação de um *malware* e distribuição dele através de toda a internet, sem necessariamente a determinação de um alvo (*target*).

Existem, no entanto, ataques direcionados, onde um novo *malware* é desenvolvido para atingir um alvo (*target*) específico, sendo o *malware* enviado diretamente ao alvo.

Nesses casos, não é possível que as desenvolvedoras de antivírus conheçam a assinatura do *malware* antes do incidente para adicioná-la na base de dados (*blacklist*) e proteger o sistema do ataque.

Para contornar essa situação, cada mais as desenvolvedoras de antivírus têm utilizado de técnicas de inteligência artificial e análise de dados para desenvolvimento de técnicas que permitam identificar ameaças desconhecidas (completamente novas) a partir do comportamento padrão de inúmeras ameaças conhecidas. Essas técnicas são eficientes e reduzem a exposição dos antivírus à ataques direcionados.

A conclusão é que apesar de sistemas de *blacklisting* serem muito eficientes contra a maior parte das ameaças existentes na internet e oferecem algumas ferramentas auxiliares para prevenção contra ameaças desconhecidas, eles ainda assim apresentam algumas vulnerabilidades frente a ataques direcionados.

3.3.2 *Whitelisting*

Whitelisting de aplicações é um mecanismo de proteção que consiste em permitir que apenas processos e aplicações confiáveis sejam executados no sistema.

O primeiro passo para solidificar o sistema (executar o *whitelisting*) é garantir que todos os programas que fazem parte do processo e que poderão ser necessários futuramente estejam corretamente instalados, configurados e atualizados. Após a solidificação, alterações poderão ser bloqueadas.

Também, antes de realizar a solidificação, deve-se garantir a inexistência de *malwares* no sistema (caso haja algum *malware* antes da solidificação, este será considerado um *software* confiável e poderá causar incidentes).

Finalmente, uma vez que o sistema estiver solidificado, ele impedirá qualquer alteração executada por um programa não confiável, assegurando a proteção de todo o sistema.

Consideradas ambas as técnicas, verifica-se que *whitelisting* é uma abordagem muito eficiente até mesmo contra ataques direcionados, ponto no qual sistemas de *blacklisting* oferecem algumas vulnerabilidades.

3.4 *Backup* e Restauração

As técnicas de segurança de *backup* e recuperação consistem no processo de copiar dados preventivamente para o propósito específico de restaurar tais dados após um evento que resulte em danos ao hardware responsável pelo armazenamento dos dados ou em danos aos dados em si. Esse processo pode ser usado para restauração dos dados em específico ou para restauração de volumes inteiros.

Alguns danos que podem acontecer em sistemas de arquivos envolvem: eliminação acidental de arquivos, corrupção de arquivos, sequestro de arquivos (através de criptografia), danos físicos ao hardware de armazenamento (*bad block*, *head crash*, *stiction*, falha de circuito, falha mecânica, entre outras), outros danos causados por ataques cibernéticos e até mesmo danos causados por desastres naturais.

Quando se trata de armazenamento, existem 2 medidas aplicáveis com objetivos ligeiramente distintos: *Backup* e Arquivamento.

Backup: O objetivo do *Backup* (cópia de segurança) é permitir uma recuperação confiável do sistema, por isso deve utilizar tecnologias de armazenamento primário, robustas e com altas taxas de transferência (que viabilizem uma rápida recuperação do sistema frente à incidentes), cujos preços costumam ser mais altos do que as tecnologias de armazenamento secundário (que oferecem maior volume de armazenamento). As soluções de backup oferecem proteção aos dados por fazerem uma cópia dos dados mais recentes, podendo ser incremental ou completa.

Arquivamento: A abordagem do arquivamento de informações tem como objetivo a preservação dos dados e é, na maior parte das ocasiões, utilizada para armazenar arquivos antigos e arquivos que não são acessados frequentemente, cujas funções não são críticas para operação do sistema. A lógica simples que condiciona essa técnica é: se um arquivo não sofre alterações ou é tão antigo que já não se faz mais uso dele, não faria sentido utilizar a técnica de *backups* constantes, nesse caso é de maior coerência o uso do arquivamento em sistemas de armazenamento secundários.

4 Configuração do *Test-Bed*

Uma bancada de testes pode ser composta por inúmeros equipamentos, computadores e *softwares*. Assim, nesse capítulo, serão abordados quais foram os componentes utilizados na bancada de testes e como esses foram configurados.

A *test-bed* ou bancada de testes da figura 16 foi o ambiente de trabalho configurado para vários testes de segurança que permitiram obter os resultados discutidos nos capítulos seguintes.

Figura 16 – Bancada de Testes na Siemens

Fonte: Autoria Própria.

A Siemens foi a grande patrocinadora desse trabalho, cedendo os equipamentos e *softwares* necessários bem como permitindo a utilização do laboratório de proteção e controle aplicado a subestações de energia.

Por isso, os métodos, materiais e configurações foram determinados com base na documentação interna desenvolvida pela Siemens para segurança cibernética em subestações de energia. Essa documentação é composta por 6 livros:

- IT Security Engineering Instructions;
- IT Security Design Guidelines;

- FAT/SAT Maintenance Testbook;
- Functional Design Specification;
- Offer Template;
- Tender Text.

As devidas precauções para não violar os direitos intelectuais e industriais foram consideradas, por isso partes técnicas e explicações detalhadas dos métodos e técnicas foram mantidas em sigilo.

4.1 Estações de Trabalho da Bancada

Os computadores são componentes essenciais para execução dos testes, assim fez-se uso de uma bancada com 3 estações de trabalho com funções diferentes, que serão detalhadas na sequência. Observe na figura 17 esses equipamentos.

Figura 17 – Estações de Trabalho na Bancada de Testes

Fonte: Autoria Própria.

4.1.1 *Service* PC - EWS

O computador de Serviço também pode ser chamado *engineering workstation* ou EWS.

As configurações do computador utilizado são dadas pela tabela 3.

Tabela 3 – Tabela de Especificações do Computador de Serviço

CPU	Intel Core 2 Duo E8400
Velocidade	3.0 GHz
RAM	4Gb
HDD	500Gb
OS	Windows 10 Enterprise
Version	LTSB 2016

Fonte: (SIEMENS, 2018)

Esse computador possui o mínimo de memória RAM recomendado para executar as ferramentas de engenharia nele instaladas, 4Gb. Além disso, não é necessário que esse computador tenha mais de 500Gb de armazenamento, desde que se utilize um sistema de *backup* auxiliar.

O sistema operacional Windows 10 Enterprise LTSB 2016 é apropriado visto que garante as atualizações de segurança do sistema até o ano 2026 (10 anos a partir de 2016). A versão LTSB do Windows é apropriada também porque conta com menos ferramentas e funcionalidades das quais não se faria uso, tornando ele mais leve e menos vulnerável.

O computador de serviço é o intermediador dos zonas seguras com a as redes não confiáveis, por isso esse computador é configurado para não ter nenhuma vulnerabilidade e para analisar e controlar todo o tráfego que entra ou sai de si.

Além disso, é nesse computador que são instaladas as ferramentas de engenharia, usadas para configurar os relés digitais (IEDs) e outros componentes chave do sistema de automação de subestações.

4.1.2 *Station Controller* - SC

A estação de controle (SC) é outra estação de trabalho imprescindível no sistema de automação de subestações (SAS).

As configurações do computador utilizado são dadas pela tabela 4.

Assim como na EWS, utilizou-se nesse computador o mínimo de memória RAM recomendado para executar o sistema de automação da subestação, 4Gb. Esse sistema também não requisita muito armazenamento, portanto o HDD de 500Gb é suficiente. Por motivos análogos aos da instalação na EWS, instalou-se nele o sistema operacional Windows 10 Enterprise LTSB 2016.

A estação de controle é responsável por um dos principais *softwares* utilizados no sistema. É nesse computador que fica instalado o sistema de automação da subestação e, por isso, ele deve ser configurado para estar na zona segura da rede.

Tabela 4 – Tabela de Especificações da Estação de COntrole

CPU	Intel Core 2 Duo E7500
Velocidade	2.93 GHz
RAM	4Gb
HDD	500Gb
OS	Windows 10 Enterprise
Version	LTSB 2016

Fonte: (SIEMENS, 2018)

4.1.3 Interface Homem-Máquina - IHM

Um computador dedicado para interface homem-máquina é utilizado, fazendo dessa estação mais um componente insubstituível do *setup* e que requer as configurações corretas.

As configurações do computador utilizado são dadas pela tabela 5.

Tabela 5 – Tabela de Especificações da Interface Homem-Máquina

CPU	Intel Core i7-4790K
Velocidade	4GHz
RAM	4Gb
HDD	500Gb
OS	Windows 10 Enterprise
Version	LTSB 2016

Fonte: (SIEMENS, 2018)

A grande diferença desse computador para os demais é que ele requer mais poder de processamento para lidar com as operações em tempo-real da interface homem-máquina.

Nos outros quesitos, montou-se uma configuração de *hardware* similar aos demais (SC e EWS), com 500Gb de armazenamento em disco rígido e 4Gb de memória RAM.

Por também ser um computador que não receberá atualizações e ferramentas constantemente, sendo instalado nesse computador basicamente o *software* responsável pela IHM, também foi escolhido o Windows 10 Enterprise LTSB 2016 para ser seu sistema operacional.

O objetivo desse computador é conter a interface homem-máquina, oferecendo um sistema visual que permita ao operador acompanhar e monitorar tudo que acontece na subestação. Por ser um sistema importante, ele também deve fazer parte da zona segura de rede.

4.2 *Softwares*

Além dos inúmeros equipamentos, um sistema de automação de subestação (SAS) também é composto pelos *softwares* responsáveis pela parte computacional (lógica) do

processo.

A Siemens é uma das desenvolvedoras de *software* para automação de subestação reconhecidas nacionalmente e oferece soluções para serem utilizadas em conjunto com os equipamentos para proteção e controle por ela desenvolvidos.

Na bancada de testes os *softwares* foram instalados nas estações de trabalho de acordo com suas funções. Conforme apontado na seção anterior, foram utilizadas 3 estações de trabalho e, por isso, os *softwares* estão descritos na sequência de acordo com a estação no qual eles estavam instalados.

4.2.1 *Service* PC

No Computador de Serviço ou EWS foram instaladas as ferramentas de engenharia, essas ferramentas são necessárias para configurar os demais equipamentos que são parte da arquitetura proposta (tais como os relés digitais).

As ferramentas de engenharia instaladas foram:

- DIGSI 4 (v4.90)
  Esse *software* desenvolvido pela própria Siemens é utilizado para parametrizar e configurar os relés de proteção da linha SIPROTEC 4. Além da instalação do *software* os devidos pacotes de *drivers* foram instalados e também as atualizações de segurança e correções de *software* (*hotfix*);

- DIGSI 5 (v7.50)
  Esse *software* é uma evolução do DIGSI 4, ele foi desenvolvido para atender a linha de produtos SIPROTEC 5 da Siemens. Mais moderno e com mais ferramentas do que seu antecessor, o DIGSI 5 também é utilizado para parametrizar e configurar relés de proteção (IEDs). Além do *software*, também foram instalados os *drivers* e *hotfixes*;

- TOOLBOX II (V6.00)
  Esse *software* consiste na verdade em um conjunto de ferramentas integrado e distribuído pela Siemens para configurar e executar diversas operações na subestação, sendo algumas delas: coleta de dados, modelagem de dados e parametrização. Essa ferramenta também é compatível com dados gerados por equipamentos de terceiros (que não sejam fabricados pela Siemens) e permite programação orientada a objeto. Também fez-se a instalação dos *hotfixes* desse *software*.

4.2.2 Estação de Controle

A estação de controle contém o *software* responsável pela automação da subestação.

O SICAM PAS/PQS é o sistema de automação de subestações desenvolvido pela Siemens e a sua versão 8.10 foi instalada na estação de controle.

Esse *software* foi desenvolvido com uma arquitetura que permite escalabilidade e interoperabilidade, sendo capaz de utilizar vários protocolos de comunicação como os mantidos pela norma IEC 61850 e outros como DNP3.0 e Modbus.

O SICAM PAS controla e registra dados do processo de todos os dispositivos na subestação através dos protocolos de comunicação.

Mas, além de receber dados de todos os dispositivos através de diferentes protocolos, o SICAM PAS também atua como *gateway*, direcionando a comunicação para os níveis superiores do sistema supervisório através de um protocolo único.

O SICAM PAS também oferece uma interface visual intuitiva para configuração dos parâmetros da subestação e para visualização dos dados coletados.

4.2.3 Interface Homem Máquina

A interface homem máquina é composta basicamente por dois *softwares*, o SICAM SCC e o SIMATIC WinCC.

O SIMATIC WinCC foi instalado na versão 7.02 junto de suas atualizações. O WinCC é a plataforma sobre a qual o SICAM SCC opera, assim sua instalação é um pré-requisito para a instalação do SICAM SCC.

O SICAM SCC é uma ferramenta para visualização de processos para sistemas de transmissão e distribuição de energia elétrica e foi instalado na estação de trabalho IHM em sua versão 8.04, juntamente de suas *hotfixes*.

É através da interface homem-máquina que os operadores da subestação acompanham todos os processos em tempo-real. Essa interface de visualização é desenvolvida para ser intuitiva e permitir um entendimento claro de todas os dados aquisitados na subestação e na rede de transmissão ou distribuição. Algumas informações que podem ser visualizadas em uma interface homem-máquina são as barras do sistema, os níveis de tensão e corrente, o fluxo de potência, entre outras informações importantes.

4.3 Outros Equipamentos da Bancada

Além dos computadores e *softwares*, alguns componentes foram utilizados para simular a arquitetura de rede que se utiliza em uma subestação de energia e, ainda outros componentes foram utilizados para simularem os equipamentos de campo de uma subestação de energia. Na figura 18, podem ser observados em destaque esses componentes.

O *switch* é um equipamento de rede, foi utilizado o modelo RSG2100 da RuggedCom

(empresa do grupo Siemens). Após um *reset* completo para restaurar as configurações originais de fábrica, atualizou-se o *firmware* desse equipamento para sua versão mais recente (no caso v3.9.1). Então o IP dele foi configurado de acordo com a segmentação de rede determinada.

Figura 18 – Outros Equipamentos na Bancada de Testes

Fonte: Autoria Própria.

O roteador também é um equipamento de rede, nesse caso utilizou-se o modelo RX1501 da RuggedCom. De maneira similar, foi realizada a restauração do equipamento e a atualização de seu *firmware* com a instalação da versão ROX II v2.9.1. As devidas configurações de rede também foram aplicadas a ele para satisfazer a segmentação de rede.

Outro equipamento de rede utilizado foi o servidor NTP, através do GPS Reason RT420. Esse equipamento foi responsável pela sincronia de todos demais componentes da arquitetura.

Apesar da grande importância dos equipamentos de rede na comunicação entre os componentes, para terminar a preparação de uma bancada de testes capaz de simular um ambiente de subestação de energia, faltavam os componentes de campo.

Dessa forma, foram utilizadas duas IEDs Siemens, sendo uma delas SIPROTEC 4 e a outra SIPROTEC 5. Essa configuração foi apropriada para verificar a compatibilidade das ações testadas com as soluções mais novas que estão sendo adotadas (SIPROTEC 5) e com as mais antigas (SIPROTEC 4) que ainda são utilizadas em muitas subestações de

energia. Outro equipamento de campo utilizado foi o SICAM AK 3.

5 Aplicação de medidas de Segurança Cibernética em Subestações de Energia

Até o momento já foram introduzidos os conceitos, técnicas e ferramentas tanto de sistemas elétricos de potência quanto de segurança cibernética.

A proposta desse capítulo é mostrar como essas duas áreas se unem e abordar algumas das recomendações apropriadas para obter um ambiente mais ciberneticamente seguro em sistemas de automação de subestações.

O conteúdo desse capítulo visa discutir os conceitos apresentados nos capítulos Subestações em SEP e Segurança Cibernética: Conceitos, Técnicas e Ferramentas considerando a bancada de testes descrita no capítulo Configuração do *Test-Bed*.

Inicia-se a abordagem com a definição de uma arquitetura de rede segura, depois são consideradas as medidas preventivas que podem ser aplicadas para reduzir a superfície de ataques do sistema e suas vulnerabilidades. Na sequência, as recomendações de aplicação são voltadas para técnicas e ferramentas de defesa contra *softwares* maliciosos e, finalmente, são abordadas algumas medidas que devem ser aplicadas para reduzir o impacto de um ataque.

5.1 Arquitetura de Redes

No capítulo 3 Segurança Cibernética: Conceitos, Técnicas e Ferramentas foram introduzidos os conceitos de arquitetura de redes sob a perspectiva da tecnologia da informação. Agora, nesse capítulo discute-se como esses conceitos são relevantes em ambientes de sistemas elétricos de potência, mais especificamente em subestações de energia elétrica.

No que se refere aos tipos de arquitetura de redes mais utilizados em sistemas de TI (P2P (*peer-to-peer*) e *Client/Server*), ambos são de grande importância em projetos de arquitetura de rede para subestações de energia elétrica.

Uma abordagem que utiliza ambos pode ser exemplificada com base na norma IEC 61850 e no protocolo de comunicação GOOSE (utilizado em subestações de energia elétrica). Segundo o artigo *Substation Communication Architecture to Realize the Future Smart Grid* (ALI; THOMAS; GUPTA, 2011), a norma IEC 61850 estabelece que os sistemas de controle e proteção da subestação de energia elétrica façam uso de comunicação *Client/Server*. Esse tipo de rede é usado para comunicação com as aplicações e processos em nível de operação, tais como o gerenciamento e controle de chaves seccionadoras (responsáveis pelo

isolamento físico do circuito).

Por outro lado, segundo o mesmo artigo, a confiabilidade e o desempenho geral das funções de automação da subestação podem ser aprimorados pelo uso de comunicação *peer-to-peer* de alta velocidade (protocolo GOOSE). Uma única mensagem GOOSE contém todas as informações necessárias sobre o estado de um evento e é repetida até que os *endpoints* a recebam ou o até que o tempo de espera termine (ALI; THOMAS; GUPTA, 2011).

Essa abordagem é utilizada em subestações de energia para satisfazer os requisitos de disponibilidade e de segurança cibernética em sistemas elétricos de potência.

Nas próximas seções desse capítulo são discutidas como outras medidas de segurança podem ser aplicadas em subestações de energia elétrica, considerando a segmentação da rede em zonas confiáveis e não confiáveis e a aplicação de técnicas e ferramentas para controle e monitoramento do tráfego.

5.1.1 Segmentação de Rede

A segmentação de rede é uma das técnicas mais importantes que pode e deve ser aplicada em um sistema de automação de subestação para obter uma arquitetura de rede segura.

Conforme pode ser observado na figura 19 e conforme também pode ser observado na legenda (figura 20), uma simples segmentação entre 3 redes é suficiente para tornar a arquitetura segura, no caso foram utilizadas uma rede segura, uma rede segura intermediária e uma rede insegura para exemplificar a arquitetura.

Os testes dessa arquitetura, utilizando a bancada de testes, foram realizados usando as configurações de IP segundo a tabela 6.

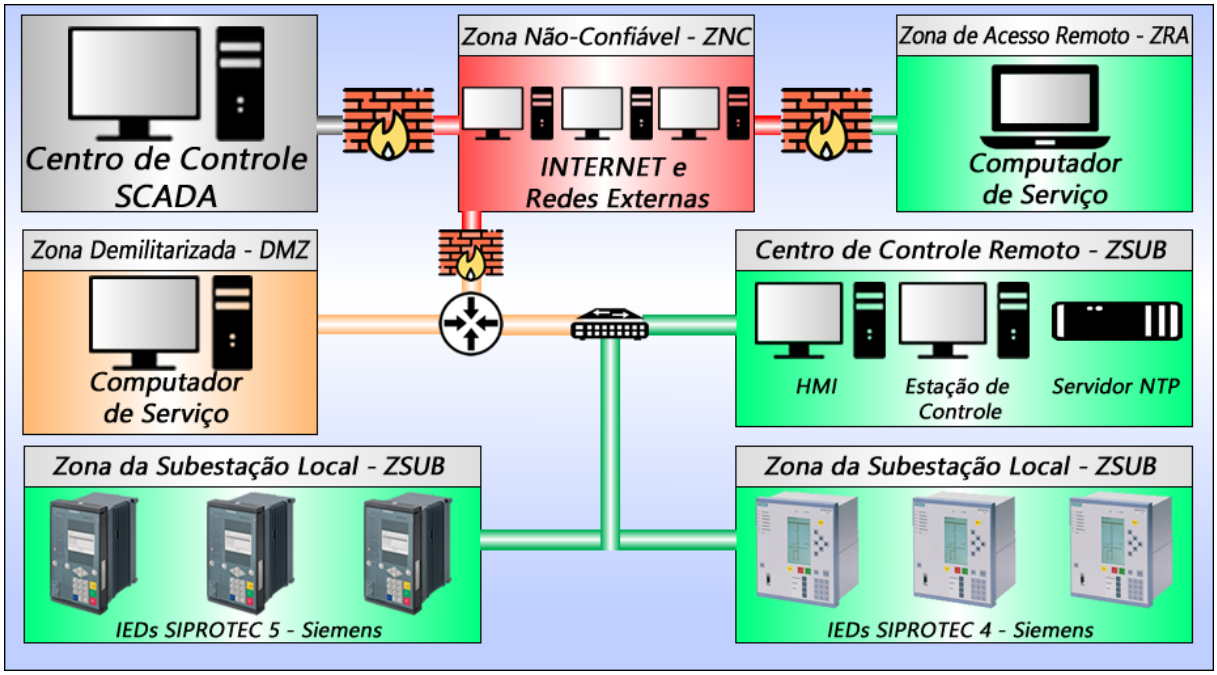
Conforme pode ser observado nessa tabela, o roteador ficará entre as 3 redes, portando ele deve ser configurado com um endereço pertencente a cada uma destas, os IPs escolhidos foram:

- 172.16.21.1: Responsável pela comunicação com os equipamentos da rede segura (IEDs, IHM, SC, AK 3, *switch* e servidor NTP);
- 172.16.11.1: Responsável pela comunicação com os componentes da rede segura intermediária, no caso formada apenas pelo computador de serviço (EWS);
- 10.10.10.1: Responsável pela comunicação com os níveis acima, que podem ser com redes inseguras.

Os componentes IEDs, IHM, SC, AK 3, *switch* e servidor NTP estão todos configurados sob o prefixo de IP: 172.16.21.XX, sendo os dois últimos valores seus identificadores exclusivos na rede.

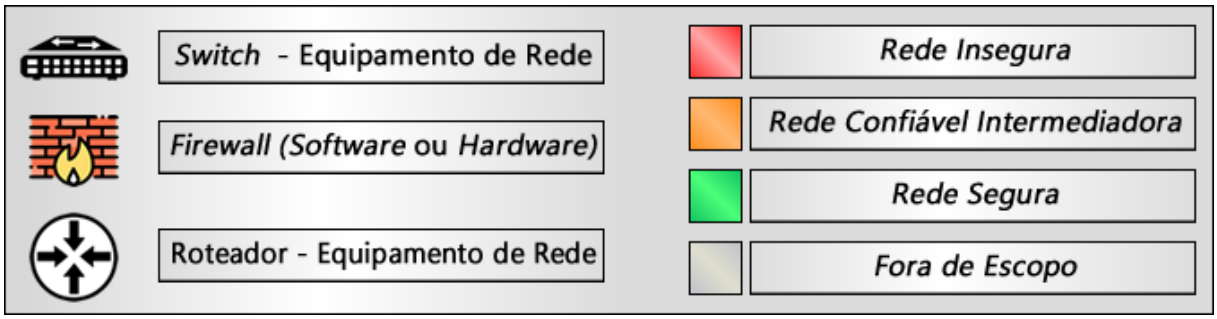
O computador de serviço está configurado sobre o prefixo de IP 172.16.11.XX, estando assim separado da rede dos demais e realizando a comunicação com eles através do roteador.

Figura 19 – Exemplo de Segmentação de Rede aplicado em Subestações de Energia Elétrica.



Fonte: Autoria própria.

Figura 20 – Legenda para auxílio na compreensão da figura 19.



Fonte: Autoria própria.

Em arquiteturas de rede seguras para utilização em subestações de energia, providenciar uma correta segmentação de rede é mais do que uma alternativa para melhoria, sendo considerado um requisito de segurança que precisa ser atendido.

Para atender a esse requisito, uma sugestão é segmentar a rede através de zonas confiáveis, semi-confiáveis e não confiáveis, descritas em mais detalhes como:

ZC **Zona Confiável**: É composta pela Zona de Subestação e pela Zona de Acesso Remoto. Essa zona é protegida por um firewall e abrange os processos confiáveis em

um perímetro no qual as trocas de informações são conhecidas;

- ZSUB **Zona da Subestação**: Considere a subestação do exemplo introduzido anteriormente, a zona da subestação compreende seus principais componentes e redes. Essa zona pode ainda ser subdividida em 2 partes. A primeira chamada de Centro de Controle Remoto (CCR) contém equipamentos tais como a interface homem-máquina, o servidor NTP, o computador usado como estação de controle, entre outros. A segunda parte é composta por equipamentos de campo tais como IEDs;

- ZRA **Zona de Acesso Remoto**: Um computador que não faz parte da infraestrutura da subestação pode acessar remotamente as funções de controle e operação da subestação através de um serviço de acesso remoto confiável usado para verificação, autenticação e autorização do usuário;

DMZ **Zona Desmilitarizada**: A zona desmilitarizada é responsável por intermediar a comunicação entre a zona segura e a zonas não confiáveis. Medidas extremas de segurança são aplicadas nessa zona da rede para impedir que ataques alcancem os equipamentos críticos localizados na zona confiável através da comunicação estabelecida entre a DMZ e a ZSUB;

ZSC **Zona Semi-Confiável**: São as redes que seguem padrões de segurança, mas que são compostas por processos que não dizem respeito ao objetivo da rede local interna e confiável (como, por exemplo, uma rede de escritório).
Elas são consideradas semi-confiáveis visto que os requisitos de segurança que elas atendem dizem respeito ao contexto no qual elas são utilizadas, porém isso não garante que o nível de segurança entregue por elas satisfaz os mesmos requisitos de segurança que a Zona Confiável deve entregar;

ZNC **Zona Não Confiável**: Todas as demais redes, sejam externas ou internas, que não tenham pertençam aos escopos citados acima e não estejam documentadas como confiáveis segundo os padrões e requisitos de segurança cibernética devem ser consideradas não confiáveis e a comunicação através dessas deve ser evitada sempre que possível.

De forma mais geral, a Zona Desmilitarizada é localizada entre a Zona Confiável (interna) e a Zona Não Confiável (externa), essa é uma estratégia utilizada para prevenir o acesso direto da rede externa e não confiável aos processos controlados pela rede interna e confiável.

O principal objetivo de criar a DMZ é fazer com que ela receba os acessos provenientes da rede externa e atue com a validação das identidades e verificação das autorizações, providenciando uma camada a mais de segurança (de acordo com a estratégia de defesa em profundidade) e protegendo a rede interna.

Tabela 6 – Endereços de IP de cada dispositivo da bancada de testes

Dispositivo	Endereço IP	Rede
SC	172.16.21.11	Segura
IHM	172.16.21.12	
IED SIP4	172.16.21.71	
IED SIP5	172.16.21.72	
AK 3 (IEC 104)	172.16.21.13	
AK 3 (IEC 61850)	172.16.21.14	
Switch	172.16.21.31	
Servidor NTP	172.16.21.10	
Roteador #1	172.16.21.1	
EWS	172.16.11.6	Segura Intermediária
Roteador #2	172.16.11.1	
Roteador #3	10.10.10.1	Externa

Fonte: Autoria Própria

5.1.2 Firewall

Em geral, no ambiente de subestações de energia são configurados *firewalls* do tipo *Stateful Inspection* através dos roteadores e *firewalls* do tipo *Application Layer Firewall* através de equipamentos para *firewall* dedicado (*Next Generation Firewall*).

Alguns dos motivos pelos quais se recomenda a utilização do *Application Layer Firewall* são citados na sequência:

- Reconhecimento de ataques na camada 7 do modelo ISO/OSI;
- Previne a rede de pacotes corrompidos destinados a aplicações selecionadas;
- Possui funcionalidade *all-in-one*, onde o *Next-Generation-Firewall* combina funcionalidades de detecção de intrusão, antivírus e filtro de protocolos;
- É possível configurar requisitos para DPI (*Deep Package Inspection* ou inspeção profunda de pacotes);
- É possível controlar aplicações SCADA utilizando a definição do protocolo (Modbus, DNP ou IEC104) e não configurando diretamente a porta;
- É possível criar assinaturas que identifiquem as aplicações do AppLaFW.

5.1.3 *Intrusion Detection and Prevention Systems*

Em ambientes de subestação de energia é altamente recomendado que se use NIDS focado em ataques que possam acontecer dentro da rede interna. Para funcionar corretamente o NIDS precisa ser utilizado em pontos estratégicos da arquitetura de redes de maneira que seja possível monitorar todo o tráfego fluindo entre os dispositivos. Dessa forma é possível realizar análises do tráfego e comparar com as políticas definidas e com

as bibliotecas de ataque conhecidas. Assim, sempre que se identificar um ataque serão enviados um alerta e uma notificação.

Alguns dos motivos pelos quais recomenda-se o uso de IDS são listados a seguir:

- É uma ferramenta de monitoração da rede;
- Não intervém nos processos em execução;
- Pode reconhecer ataques cibernéticos que foram criados ou iniciados fora da rede em questão;
- Consegue identificar ataques cibernéticos do tipo *long-term* (*slow attack*);
- Provê uma série de assinaturas pré-definidas e permite a criação de assinaturas;
- Provê informações para forense digital, quando um ataque for confirmado para identificar o caminho percorrido pelo atacante e as possíveis vulnerabilidades;
- IDS podem ser encontradas em Next-Generation-Firewalls.

Não é recomendado utilizar-se de IPS em sistemas elétricos de potência visto que essa tecnologia gera um alto número de falsos positivos (quando pacotes são considerados maliciosos ainda que não sejam, resultando em alterações da rede e do ambiente que podem prejudicar a operação da subestação, em maior instância podendo afetar a comunicação entre os equipamentos e impactando diretamente a disponibilidade dos serviços).

5.1.4 Diferenças básicas entre FW e IDS

A tabela 7 destaca algumas das diferenças entre *firewall* e NIDS (*network* IDS). Conforme observado, apesar de ambos serem soluções utilizadas para obter uma rede mais segura, a diferença essencial entre essas ferramentas é o escopo no qual elas atuam.

O *firewall* é focado em observar a movimentação de pacotes entrando e saindo da rede à procura de ameaças com o objetivo de bloqueá-las, atuando como limitador da comunicação entre as redes e prevenindo contra intrusões. O NIDS, por sua vez, possui um escopo de atuação maior, observando todo o tráfego gerado e capaz de monitorar os dados internamente aos pacotes, é capaz de gerar relatórios e notificações com base nas análises executadas, porém não é capaz de barrar a comunicação.

Dessa forma, ambas as ferramentas se mostram de extrema eficiência no aumento da segurança do sistema, sendo a recomendação final aplicá-las em conjunto sempre que apropriado.

5.2 *Hardening* do Sistema

Sistemas de Infraestrutura Crítica são responsáveis pela operação dos serviços mais essenciais de uma nação, tais como: energia, água, gás e combustível (entre outros). Por

Tabela 7 – Algumas diferenças entre NIDS e *Firewall*.

NIDS	Firewall
Localizado dentro de uma rede.	Localizado nas bordas da rede.
Analisa todo o tráfego de informações.	Analisa apenas as entradas ou saídas de informações.
Não é capaz de bloquear conexões.	Possui ferramentas para bloqueio de conexões.
Possui ferramentas para reportar tráfego suspeito através de alertas e notificações.	Possui ferramentas que permitem apenas reportar pacotes que foram bloqueados.

Fonte: (SIEMENS, 2018)

esse motivo, esses sistemas são muitas vezes alvos de ataques direcionados, bem planejados e executados.

Dado o nível crítico das operações executadas por esses sistemas, é imprescindível garantir, por exemplo, um controle de acesso físico e lógico robusto de acordo com os usuários e as funções pelas quais estes são responsáveis (TAYLOR; KRINGS; ALVES-FOSS, 2002).

Mas, quando se trata de Sistemas Elétricos de Potência, muitas outras medidas preventivas podem ser aplicadas, principalmente em subestações de energia digitais, para garantir um ambiente mais seguro.

As subseções seguintes exploram como podem ser reduzidas as vulnerabilidades e a superfície de ataques considerando a arquitetura de rede de uma subestação digital simples (proposta na figura 19).

5.2.1 Controle de Acesso e Gerenciamento de Contas

Os Sistemas Elétricos de Potência são bastante complexos e possuem uma série de controles e proteções digitais que atuam em tarefas críticas, garantindo o fornecimento ininterrupto de energia e protegendo a infraestrutura elétrica da rede. Dessa forma, é de máxima importância garantir que o acesso e as permissões sejam fornecidos de acordo com o papel de cada usuário no sistema.

Considerando a arquitetura descrita anteriormente, algumas configurações que podem ser aplicadas são:

- **Computador de Serviço**
  Visto que esse computador fornece as ferramentas de engenharia necessárias para algumas operações, faz sentido oferecer 3 grupos de permissão:

  1. Administradores do Sistema

     - Direitos de Administrador do Windows;

- Senhas não expiram.

2. Engenheiros do Sistema

- Direitos Padrões do Windows;

- Senhas expiram a cada 180 dias, notificações são usadas para lembrar de trocar a senha;

Permissões adicionais para uso das ferramentas de engenharia são concedidas.

3. Serviços Remotos

- Direitos Padrões do Windows;

- Senhas expiram a cada 180 dias, notificações são usadas para lembrar de trocar a senha;

- Sem permissão para uso das ferramentas de engenharia.

- ***Station Controller***
  Esse sistema é utilizado por administradores do sistema e engenheiros que precisam ter acesso às interfaces de configuração e operação. Esse sistema, requisita que o autologon seja configurado no Windows, dessa forma o controle de acesso precisa ser configurado em outros níveis. Algumas configurações que devem ser seguidas:

  - A conta configurada para o *autologon* do Windows não pode ter direitos de administrador do sistema;

  - Acessos ao painel de controle e ao terminal de comandos *shell* devem ser desabilitados;

  - Sempre que o computador suspender deve exigir senha para acesso;

  - Após o *autologon* ao iniciar o sistema, deve-se bloquear todas as tarefas até que o sistema suspenda automaticamente pela primeira vez, assim para acessar será obrigatório entrar com a senha (essa é a única forma de satisfazer os requisitos do software base da *Station Controller* e os requisitos de proteção do sistema);

  - Internamente ao *software* base da *Station Controller* existe a possibilidade configurar contas de usuário, a recomendação é que cada engenheiro tenha sua própria conta (assim através dos registros pode-se identificar qual usuário responsável por cada ação no sistema).

- **Interface Homem Máquina**
  O *software* base da IHM também requer o *autologon* do Windows, assim de maneira similar deve ser configurado junto de uma conta que não tenha direitos de administrador e que não possua acesso ao painel de controle e ao terminal de comandos *shell*. Apesar disso, esse software oferece sua própria solução para controle de acesso e gerenciamento de contas que deve ser configurada de acordo com os 4 papéis que são desempenhados por 4 tipos de usuário:

- Administradores do Sistema;

- Engenheiros do Sistema;

- Operadores do Sistema;

- Usuário especial sem senha.

Apesar das configurações específicas de gerenciamento de contas citadas acima, algumas configurações comuns devem ser obedecidas em todas as contas:

- Todas as contas devem usar senhas que atendam aos requisitos NERC CIP de políticas de senha (senhas vazias desativadas);
- Sempre que o computador suspender deve exigir senha para acessar novamente.

Não menos importante, devem ser executadas as configurações necessárias para registrar tentativas bem e malsucedidas de acesso através do sistema de registro e monitoramento.

A tabela 8 fornece um resumo de algumas configurações de conta recomendadas para redução da superfície de ataques em sistemas elétricos de potência considerando alguns componentes essenciais da arquitetura proposta (19).

Além do gerenciamento das contas de usuário de acordo com as funções por eles desempenhadas no sistema, é de suma importância que sejam utilizadas técnicas para controle de acesso que garantam a identidade dos usuários, verificando através das ferramentas se o usuário é realmente quem ele diz ser.

Na tabela 9 encontra-se um resumo de técnicas e ferramentas para controle de acesso em função de cada componente da arquitetura de subestação considerada.

5.2.2 Registro e Monitoramento de Segurança

Para configurar o registro e monitoramento de segurança em um ambiente de subestação de energia, recomenda-se uma abordagem interessante e coerente com a arquitetura proposta, onde utiliza-se o computador de serviço localizado na zona desmilitarizada como coletor central.

Coletores locais (demais computadores em suas respectivas zonas) são então usados para agrupar as informações e enviar ao Coletor Central (computador de Serviço), nesse momento o computador de serviço agrupa as informações e as envia ao Servidor localizado no Centro de Controle que possui um SIEM (*Security Information and Event Management*) que permite monitoramento, análise e controle através dos dados recebidos.

O SIEM será o responsável por identificar incidentes ou ataque através das informações disponíveis, essa identificação é possível através da visão centralizada e compreensiva do cenário de toda a infraestrutura da subestação, gerando alertas e notificações sempre que os requisitos e/ou políticas de segurança não forem satisfeitos.

Tabela 8 – Resumo de recomendações para gerenciamento de contas e privilégios segundo aplicação em subestações de energia elétrica.

Componente	**Grupos de Usuário**		
	Administrador	**Engenheiro**	**Operador**
Computador de Serviço	Administrador do Windows Administrador do TOOLBOX	Usuário com direitos padrão do Windows e permissão de uso das ferramentas de engenharia (DIGSI, TOOLBOX).	Usuário padrão do Windows, sem permissões de uso das ferramentas de engenharia (DIGSI, TOOLBOX).
SICAM SCC	Administrador do Windows	Conta de autologon do Windows; Privilégios de leitura para SICAM SCC Runtime; Privilégios de administrador para SICAM WinCC Explorer.	Conta de autologon do Windows; Privilégios de operador no SICAM SCC Runtime.
SICAM PAS	Administrador do Windows Administrador do SICAM PAS	Conta de autologon do Windows; Privilégios de engenheiro do sistema no SICAM PAS.	N/A
SICAM RTU	Acesso indireto ao AK através do TOOLBOX; Acesso indireto ao A8000 através do navegador usando RADIUS.	Acesso indireto ao AK através do TOOLBOX; Acesso indireto ao A8000 através do navegador usando RADIUS.	N/A
SIPROTEC 5	Acesso indireto através do DIGSI usando RADIUS.	Acesso indireto através do DIGSI usando RADIUS.	Acesso indireto através do DIGSI usando RADIUS.
NTP Server	Conta de admin com todos os privilégios	Conta de device com privilégios restritos	Conta de device com privilégios restritos
Switch	Conta de admin com todos os privilégios	Contas de guest e operator com privilégios restritos	Contas de guest e operator com privilégios restritos
Roteador	Conta de admin com todos os privilégios	Conta de guest e oper com privilégios restritos	Conta de guest e oper com privilégios restritos

Fonte: (SIEMENS, 2018)

As atividades mais comuns que podem ser monitoradas são:

- Atividades relacionadas a contas;
  - Login/Logout;
  - Tentativas falhas de acesso;
  - Alteração de senha de acesso.
- Alterações nas políticas e/ou configurações do sistema;
- Atualização de *software* ou *firmware*;
- Instalação de *software*;
- Mensagens do sistema operacional;
- Detecção de *malwares*;
- Tráfico através do *firewall*;

Tabela 9 – Resumo de autenticações, credenciais e protocolos utilizados de acordo com os componentes de uma arquitetura de subestação de energia elétrica.

Caso de Uso	Tipo de Autenticação	Protocolo	Credenciais	AD
Computador de serviço	Conta do Windows (local ou remota)	RDP via IPsec VPN (se remota)	Usuário e Senha	Sim
SICAM SCC e SICAM PAS	Conta do Windows (local ou remota a partir do computador de serviço)	RDP local ou remota		
SICAM AK3 através do computador de serviço	Computador de Serviço: 1. Conta do Windows 2. Conta de Engenheiro do TOOLBOX AK3: 3. Autenticação da conexão	TOOLBOX (TLS)	Computador de Serviço: 1. Usuário e Senha; Computador de Serviço e AK3/SIPROTEC/ Roteador/Switch: 2. Credenciais TLS; 3. Senha para conexão.	PC: Sim AK3: Não
SIPROTEC através do computador de serviço	Computador de Serviço: 1. Conta do Windows. SIPROTEC 5: 2. Autenticação do usuário.	DIGSI5 (TLS)		PC: Sim SIP: Sim
Roteador através do computador de serviço	Computador de Serviço: 1. Conta do Windows. Roteador: 2. Autenticação do usuário.	https (TLS)		Sim
Switch através do computador de serviço				

Fonte: (SIEMENS, 2018)

- Alteração de data e hora do sistema.

Em ambientes de subestação de energia ocorre a grande necessidade de centralizar os eventos registrados para o monitoramento, esse agrupamento de eventos em sistemas como o SIEM pode ser realizado através de protocolos conhecidos da área de TO como o Syslog, as subseções seguintes se propõem a explicar melhor como esse protocolo atua com grande importância na infraestrutura de segurança de sistemas elétricos de potência.

5.2.2.1 O Protocolo Syslog no Monitoramento

Syslog é um padrão para registro de mensagens e eventos definidos pelo RFC 5424 (GERHARDS, 2009). O protocolo Syslog é tipicamente usado em sistemas para aumentar a segurança por esses oferecida. Além disso, por oferecer suporte a um largo conjunto de sistemas e dispositivos é muitas vezes utilizado para integrar diferentes sistemas de *logging* em um único repositório central (como o SIEM citado anteriormente).

Esse protocolo permite que um dispositivo ou *software* envie mensagens de notificação ou eventos através da rede para os chamados coletores (ou *syslog servers*), essas mensagens são transmitidas através de protocolos TCP ou UDP usando como porta padrão a 514. Para tornar a transmissão segura, é possível criptografar a mensagem transmitida

usando o protocolo de segurança TLS (*Transport Layer Security*).

Em geral, equipamentos de rede (*switches* e roteadores) estão preparados para se comunicar usando protocolo Syslog e oferecem vários níveis de registro.

Por outro lado, o sistema operacional Windows não oferece comunicação através do protocolo Syslog nativamente, dessa forma faz-se necessário a instalação de *softwares* terceiros que ficarão encarregados de encaminhar os eventos registrados no Windows Event Logs (ferramenta nativa do sistema operacional Windows) para o coletor através do protocolo Syslog.

5.2.2.2 Protocolo Syslog e seu padrão de pacotes

A mensagem enviada pelo protocolo Syslog é em geral composta por informações que respondem três perguntas básicas: para onde enviar, quando foi enviado e por quê a mensagem foi enviada (conceito *where*?, *when*? and *why*?).

De forma mais completa, o pacote de uma mensagem Syslog carrega as seguintes informações: *Facility* , *Severity*, *Hostname*, *Timestamp*, *Message*. Uma breve explicação sobre cada um desses é dada na sequência:

- *Facility*: Esse conceito é utilizado para identificar e categorizar a fonte que gerou a mensagem (essa fonte pode ser um sistema operacional, um processo ou uma aplicação). Veja com mais detalhes na tabela 10;
- *Severity*: Esse conceito é utilizado para descrever o nível de importância do evento ocorrido, que pode assumir os seguintes valores de estado:

  0 - Emergência: O sistema não pode ser usado;

  1 - Alerta: Ações precisam ser executadas imediatamente;

  2 - Crítico: O sistema atingiu condições de limite que não podem ser ultrapassadas;

  3 - Erro: O sistema apresenta operação falha;

  4 - Alarme: Há ocorrência de comportamentos que podem levar a falhas do sistema;

  5 - Aviso: O sistema não está em condições perfeitas, deve-se fazer uma análise mais cuidadosa para prevenção;

  6 - Informação: Mensagens informativas apenas;

  7 - Debug: Mensagens de ações que não são cruciais para operação do sistema.
- *Hostname*: Essa informação determina para onde a mensagem deve ser enviada, apesar de poder utilizar o nome do *host* como identificação, também é possível que se atribua aqui o endereço IP do *host* que deve receber a mensagem;

- *Timestamp*: Determina a hora local no formato MM DD HH:MM:SS de quando a mensagem foi gerada. Essa informação só possui real valor quando todos os equipamentos interligados através da rede estão sincronizados através do protocolo NTP (*Network Time Protocol*);
- *Message*: Contém a mensagem em si e preenche todo o restante do pacote, essa informação contém os campos ***tag*** que descreve qual processo, aplicação ou dispositivo enviou a mensagem e **conteúdo** que contém detalhes do ocorrido.

A tabela 10 também ajuda a entender quais são algumas fontes responsáveis pelos registros gerados, se observa que o nível de detalhamento oferecido é suficiente para que em futuras análises seja possível encontrar as fontes do problema.

Tabela 10 – Informação sobre os valores que a fonte do registro pode assumir.

Código	***Facility***
0	Mensagens do kernel
1	Mensagens a nível de usuário
2	Mail-system
3	System-daemon
4	Mensagens de segurança e de autorização
5	Mensagens geradas internamente pelo syslog-daemon
6	Subsistema de impressão de linhas
7	Subsistema de novas redes
8	Subsistema UUCP
9	Daemon-clock
10	Mensagens de segurança e de autorização
11	FTP-daemon
12	Subsistema FTP
13	Log audit
14	Log alert
15	Daemon-clock
16 a 23	Uso local

Fonte: (SIEMENS, 2018)

5.2.2.3 Aplicação do Protocolo Syslog em Subestações de Energia

Todos os dispositivos que puderem utilizar o protocolo Syslog devem ser configurados corretamente para encaminhar as mensagens de segurança relevantes ao coletor central (computador de Serviço). Analogamente, o coletor central deve ser corretamente configurado para encaminhar todas as mensagens recebidas ao Centro de Controle onde está instalado o SIEM (FRANCESCHETT; BARROS; PERES, 2007).

Visto que todos os computadores da subestação fazem uso do sistema operacional Windows e este sistema não oferece nativamente a capacidade de se comunicar através do protocolo Syslog, faz-se necessário utilizar-se de um software terceiro que adicione essa

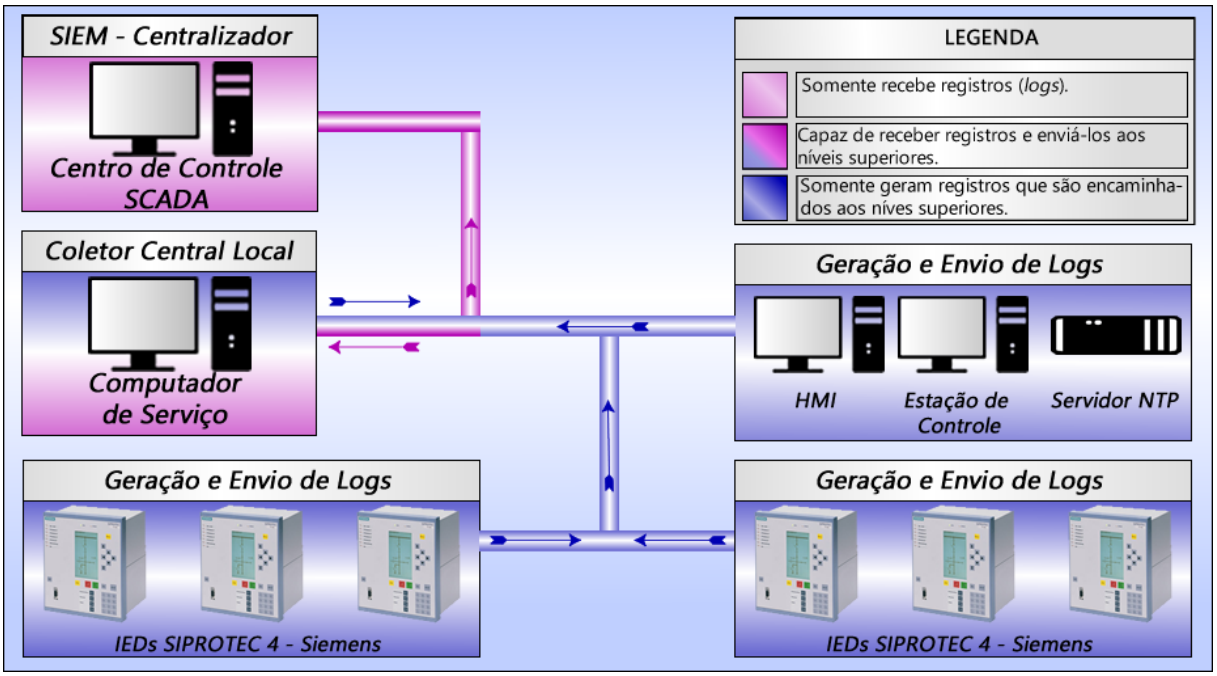
capacidade ao sistema, uma recomendação é a utilização do NXLog (oferecido em versões *Community* e *Enterprise*).

Além dos computadores, a arquitetura da subestação sugerida é composta por uma série de dispositivos Siemens com diferentes funções. Em geral, esses dispositivos possuem nativamente o protocolo Syslog como uma de suas ferramentas, permitindo assim uma integração eficiente entre os componentes da rede. Em diferentes arquiteturas que utilizem dispositivos de outros fabricantes deve-se verificar a capacidade de se comunicar utilizando protocolo Syslog.

Outros dispositivos e equipamentos que façam parte da arquitetura do sistema também devem ser corretamente configurados para registrar e enviar as informações ao coletor através da rede.

Para melhor visualização do fluxo de registros através da rede foi desenvolvida a figura 21.

Figura 21 – Exemplo de Funcionamento do Sistema de *logging* de acordo com arquitetura proposta de subestação digital.



Fonte: Autoria própria.

Observe nessa figura que um mesmo computador pode atuar como coletor (servidor) e transmissor (cliente), essa ação é executada pelo computador de serviço que atua como um centralizador local das mensagens. Para fins de análise mais detalhada, o Centro de Controle responsável pela operação, dotado de um SIEM corretamente configurado, monitora e analisa constantemente os dados por ele recebidos e provenientes do coletor local. Os demais componentes da rede atuam gerando registros e transmitindo os mesmos ao coletor local.

5.2.3 *Patching* de Segurança

Uma série de responsabilidades estão envolvidas na aplicação dos pacotes de segurança, assim é comum associar tais responsabilidades com o trabalho do integrador do sistema.

Essas responsabilidades envolvem:

- Garantir que o sistema projetado seja entregue com todos as atualizações de segurança;
- Garantir que o processo seja executado segundo sua versão mais recente de projeto;
- Garantir que as listas de componentes e de aplicações estejam atualizadas inclusive com suas versões atuais;
- Garantir que através das listas de componentes e aplicações, seja realizado um acompanhamento constante de novas versões e atualizações de segurança;
- Desenvolver documentos e planos para mitigação de riscos juntamente dos clientes envolvidos.

Assim, para obter um sistema seguro faz-se de suma importância que o integrador do sistema execute as ações necessárias de acordo com as responsabilidades acima comentadas.

Em sistemas mais simples, basta estabelecer ciclos de atualização em intervalos curtos de tempo. Porém, essa abordagem pode se mostrar de difícil execução ao se tratar de sistemas mais complexos.

A complexidade se dá no Sistema Elétrico de Potência visto que a "disponibilidade"do conceito (CIA) é o pilar mais importante. Se todas as atualizações simplesmente forem aplicadas sem os devidos testes e precauções podem surgir incompatibilidades imprevistas no sistema, afetando diretamente sua disponibilidade através de comportamentos inesperados.

Além disso, algumas atualizações exigem grande poder de processamento, tempo e até mesmo que os serviços ou componentes sejam reiniciados, operações que também podem influenciar na operação e disponibilidade do sistema como um todo um todo.

Considerando tais situações, é de praxe elaborar um plano bem definido e estruturado que classifique as atualizações de acordo com sua prioridade e seu impacto no sistema. Também, as atualizações só podem ser instaladas após os devidos testes de compatibilidade e impacto no sistema.

5.3 Proteção contra *Malware*

No que se refere à proteção e detecção de *malwares* em Sistemas Elétricos de Potência existem 3 vertentes básicas de proteção:

1 Proteção básica através do *hardening* do sistema, já comentado;

2 Uso de *softwares* apropriados para *scan* do sistema à procura de vírus/*malwares*;

3 Restrição da troca de dados entre os componentes da rede.

Essa seção trata mais especificamente da segunda vertente: *softwares* e/ou ferramentas para *blacklisting* e *whitelisting*.

Em geral, a maior parte das ferramentas de TI utilizadas para prevenção contra *malware* também são válidas para o ambiente de TO, porém algumas configurações podem diferir devido à diferente natureza desses ambientes.

Atenção deve ser dada em especial à três pontos nos sistemas de TO:

- Atualizações da ferramenta de proteção contra *malware* podem influenciar na disponibilidade do sistema;
- Em equipamentos pertencentes à zona segura, não se deve permitir que a ferramenta tenha acesso direto à internet para download das atualizações de segurança;
- A detecção e remoção automática de componentes, aplicações e/ou processos deve ser muito bem estudada para garantir que nenhuma parte crítica para operação do sistema seja desativada incorretamente através de um falso-positivo (resultando na indisponibilidade do sistema).

Além disso, destaca-se a necessidade do uso dessas ferramentas no ambiente do sistema elétrico de potência visto que até mesmo a arquitetura segura proposta anteriormente apresenta algumas vulnerabilidades que podem ser exploradas como vetores de infecção do sistema, tais como:

- Comunicação com *endpoints* fora da zona segura através da rede;
- Dispositivo portáteis de armazenamento (tais como pen drives) conectados diretamente na zona segura;
- Computadores/Notebooks quando conectados diretamente à zona segura da rede interna.

Determinada a necessidade do uso de ferramentas contra *malware*, as subseções seguintes são dedicadas a explorar em mais detalhes às aplicações de *blacklisting* e *whitelisting*.

5.3.1 *Blacklisting*

Primeiro, considere a categoria de SO Não-Padronizados, formada por sistemas operacionais dos componentes do ambiente de Automação de Energia (ou com funções correlatas). Compõem essa categoria: IEDs, controladores embarcados (como SICAM RTU), CLPs (Controladores Lógicos Programáveis), equipamentos de rede (*switches* e roteadores), dispositivos de comunicação, entre outros.

A recomendação para sistemas elétricos é que não se aplique o uso de aplicações de *blacklisting* (antivírus) em sistemas que pertençam à categoria de SO Não-Padronizados.

Na verdade, o uso de antivírus convencionais não se aplica à esses dispositivos visto que eles não são programados para oferecer proteção nesses sistemas e também os *malwares* encontrados nesses sistemas não costumam ser conhecidos (para que o antivírus seja eficiente ele precisa conhecer o vírus, se o antivírus não possuir uma base atualizada ele dificilmente será útil na detecção de ameaças).

Por isso, para certificar-se de que os componentes da categoria de SO Não-Padronizados estejam seguros, devem ser seguidas as vertentes de segurança 1 (*hardening*) e 3 (restrição de dados) referidas anteriormente.

Para os equipamentos da arquitetura de rede que utilizam sistema operacional Windows tais como os sistemas de interface homem-máquina (SICAM SCC), o computador de Serviço (que contém as ferramentas de engenharia), a estação de controle (SICAM PAS), os servidores, entre outros, deve-se fazer uso de antivírus reconhecidos e atualizados.

A compatibilidade do antivírus com o restante do sistema deve ser garantida para que não interfira na disponibilidade da operação.

Além disso, antes da entrega do sistema operante, deve-se verificar todos os computadores para checar a possível existência de algum *malware*, dessa forma faz-se possível a correção antes que o sistema entre em operação.

5.3.2 *Whitelisting*

Aplicações de *whitelisting* se mostram uma alternativa viável em subestações de energia visto que alguns de seus componentes não são atualizados frequentemente.

Após a instalação de todas as aplicações, ferramentas e *softwares* que compõem o projeto de uma subestação digital, e após a configuração de todas as medidas de *hardening* sugeridas (controle de acesso, gerenciamento de contas, antivírus, *firewall*, entre outros), o sistema se encontra preparado para ser solidificado.

A solidificação consiste na execução da aplicação *whitelisting* que executa então uma varredura no sistema mapeando todas as assinaturas existentes e as classificando como confiáveis (por isso é importante garantir que nenhum *malware* tenha infectado o sistema).

A recomendação é que a solidificação seja executada antes da execução do FAT (*Factory Acceptance Test*), de maneira que nas etapas de comissionamento e SAT (*Site Acceptance Test*) o sistema já esteja devidamente seguro (não costumam ser feitas atualizações durante essas etapas).

Cabe destacar que a aplicação do *whitelisting* é uma técnica complementar de

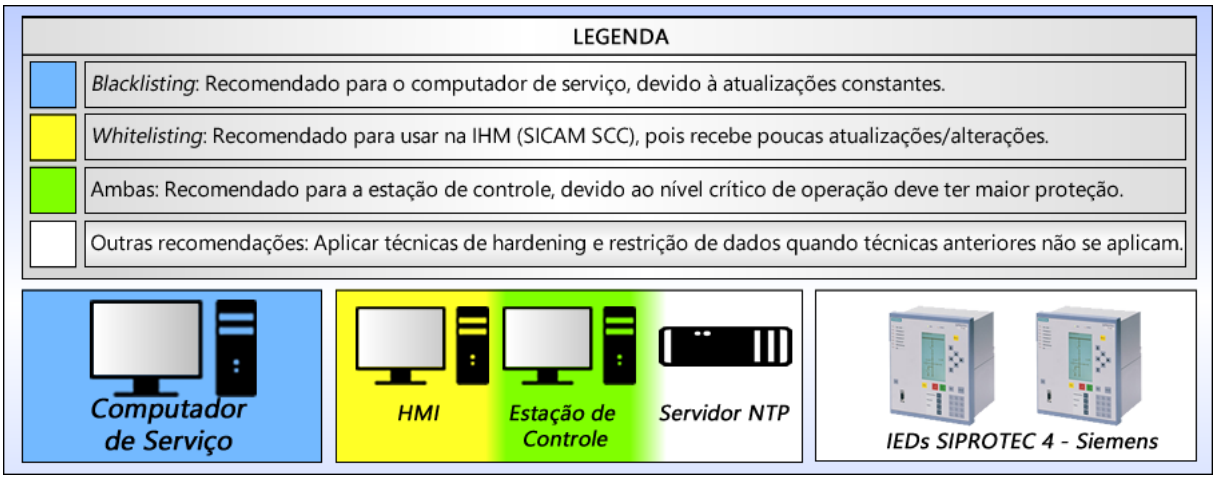
proteção que segue os princípios da defesa em profundidade, porém ela não substitui as demais técnicas para redução da superfície de ataques e otimização da segurança.

Segundo a arquitetura de subestação digital proposta na figura 19, recomenda-se aplicar a solidificação na estação de controle e na interface homem-máquina.

5.3.3 Exemplo de Aplicação de *Blacklisting* e *Whitelisting*

A figura 22 foi desenvolvida para auxiliar no entendimento das recomendações citadas anteriormente sobre quais componentes devem receber as aplicações de *blacklisting* e *whitelisting*, respectivamente.

Figura 22 – Ilustração das recomendações de aplicação de *blacklisting* e *whitelisting*.



Fonte: Autoria própria

5.4 *Backup* e Restauração

O uso de *backups* em ambientes de subestação de energia é extremamente necessário para permitir a recuperação frente à incidentes sem perdas significativas de operação. As subseções seguintes exploram com mais detalhes os procedimentos para *backup* e para restauração.

5.4.1 *Backup* em Subestações

Para executar um procedimento de *backup*, faz-se necessário conhecer suas configurações corretas de execução. Tais configurações envolvem as respostas a três perguntas simples:

1 *What*?: *Data Types* ou Tipo de Dados (conferir tabela 11)

- Dados de aplicações, do sistema operacional, de arquivos de instalação, entre outros;

- Dados de configuração dos equipamentos tais como desenhos na interface homem máquina, lógicas para controle da subestação, configurações de proteção, configurações dos equipamentos de rede;

- Dados de processos em tempo real tais como lista de eventos, medidas, entre outros.

2 *When*?: *Backup Schedule* ou Agendamento de *Backup* (conferir tabela 12)

- As aplicações usadas para *backup* oferecem como parte de suas funções a possibilidade de agendamento do início da execução, dessa forma pode-se criar uma rotina de *backup* que seja constante, automática e independente da ação humana.

3 *Where*?: *Backup Media* ou Mídia de Armazenamento

- A pergunta "onde o *backup* será salvo?"pode ter basicamente duas respostas: local (armazenado em uma mídia física parte da arquitetura local) ou externo (armazenado em nuvem através de soluções online).

A tabela 11 é baseada na arquitetura de subestação da figura 19, nesse caso considera-se o uso de equipamentos, ferramentas de engenharia e aplicações da Siemens (SICAM PAS, SICAM SCC, SIPROTEC IEDs, DIGSI, TOOLBOX, entre outros). Conforme observado a única aplicação que armazena dados em tempo real é o SICAM SCC, assim deve-se garantir a disponibilidade de armazenamento contínuo para que frente a um incidente seja possível recuperar o estado de operação com a menor perda possível.

Tabela 11 – Tipos de Dados para *Backup* e método sugerido em Subestações de Energia.

Tipo de Dados	**Método de *Backup***	**HMI**	***Station Controller***	**IEDs**	***Switches* e Roteadores**
Aplicações	PCs: Imagem do Sistema *Hardware* dedicado: Imagem do *firmware* Ferramentas de Engenharia: Imagem dos arquivos de configuração.	Imagem do Sistema	Imagem do sistema para SICAM PAS Imagem do firmware para SICAM RTU	Imagem do *firmware* usando DIGSI	Imagem do *firmware*
Config.	Armazenamento dos arquivos de configuração	Arquivos do SICAM SCC	Arquivos do SICAM PAS UI	Arquivos do DIGSI	Arquivos de configuração
tempo real	Garantir disponibilidade das mídias para armazenamento	Função de Arquivamento do SICAM SCC	N/A	N/A	N/A

Fonte: (SIEMENS, 2018)

Por outro lado, a tabela 12 traz uma recomendação de ciclos de *backup* que podem ser seguidos em uma subestação de energia, também considerando a arquitetura da figura 19 e que os equipamentos e aplicações base sejam Siemens. Os ciclos de *backup* variam

de acordo com a quantidade de dados gerados pela aplicação para que perdas sejam minimizadas. Por exemplo, dados do SICAM SCC que são gerados em tempo real precisam ser armazenados a cada 2 horas, isso garante que frente a um incidente, o máximo de informações perdidas será dado pelo tempo entre o incidente e o último *backup* (e, portanto, será menor do que 2 horas).

Os *backups* orientados a *Milestones* ou marcos históricos são necessários visto que algumas operações executadas em ambientes de subestação podem resultar em alteração de processos e configurações para que se atenda os requisitos da etapa do projeto em questão. Assim, para manter as bases de *backup* atualizadas de acordo com as alterações mais recentes, recomenda-se executar o procedimento de armazenamento de acordo com o equipamento e aplicação em questão.

Tabela 12 – Cronograma de *Backup* e sugerido para ambientes de Subestação de Energia.

Produto	**Tipo de Dados**	**Cronograma**
SICAM PAS **SICAM SCC** **Computador de Serviço**	Dados de Aplicações: Backup completo e imagem do sistema.	Orientado a Milestones: - Antes e depois do FAT - Antes e depois do SAT - Após atualizações de software - Após o comissionamento Orientado a ciclos: - Mensalmente
Switches **Roteadores** **Servidor NTP** **SIPROTEC IEDs** **Equipamentos de Terceiros**	Dados de Aplicações: Imagem do firmware	
SICAM PAS **SICAM SCC** **DIGSI** **TOOLBOX**	Dados de Aplicações: Arquivamento de ferramentas	Orientado a Milestones: - Após o comissionamento
SICAM PAS **SICAM SCC** **DIGSI** **TOOLBOX** **Roteadores** **Servidor NTP**	Dados de Configuração: Armazenar as base de dados desses sistemas	Orientado à Milestones: - Antes e depois do FAT - Antes e depois do SAT Orientado a ciclos: - Diariamente
SICAM SCC	Dados em Tempo Real	Orientado a ciclos: - A cada 2 horas

Fonte: (SIEMENS, 2018)

Finalmente, explorando em mais detalhes a terceira configuração (*Where*), recomenda-se para subestações de energia a utilização de discos rígidos externos (*External Hard Disks*) ou o uso de servidores NAS (*Network Attached Storage*). No caso do uso de servidores NAS é necessário garantir que a comunicação através da rede com o servidor seja segura e de alta disponibilidade, para permitir que os *backups* sejam realizados constantemente e sem interferência.

A solução mais segura no ambiente de subestação é o uso dos servidores NAS, visto que eles oferecem apenas as funções de armazenamento de arquivos do sistema operacional e se comunicam através de protocolos seguros tais como NFS (*Network File System*), SMB/CIFS (*Server Message Block / Common Internet File System*) ou AFP (*Apple File Protocol*). Por outro lado, usar discos rígidos externos pode causar infecção por *malwares* se estes dispositivos não forem corretamente protegidos.

Alguns benefícios de utilizar um servidor NAS incluem:

- Compartilhamento dos arquivos com vários computadores;
- Acesso mais rápido aos arquivos (rede de fibra ótica);
- Alta disponibilidade (*full-time*);
- Administração e configuração mais simples;
- Tolerância às vibrações;
- Possível recuperação frente à incidente de bloqueio de dados;
- Uso de paralelismo e redundância.

Uma vez que os *backups* tenham sido corretamente realizados, o processo de recuperação e restauração poderá ser bem-sucedido.

5.4.2 Recuperação e Restauração

Considerando a ocorrência de um incidente com danos causados ao sistema faz-se necessário a aplicação de um DRP (Plano de Recuperação de Desastres) que é parte de um BCP (Planejamento de Continuidade de Negócio), esses planos são definidos para garantir a operação das funções críticas mesmo após a ocorrência de um incidente, permitindo uma rápida recuperação das funções auxiliares e adjacentes.

O objetivo primário do DRP é minimizar o tempo inoperante do sistema e reduzir a perda de dados após um incidente. O DRP consiste em 3 ações:

1 Resposta;

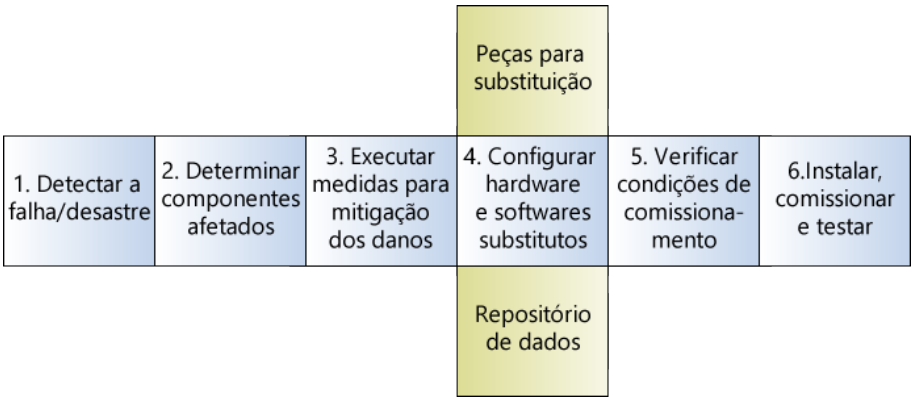
2 Funções Críticas;

3 Recuperação e Restauração.

Nesta sessão a terceira ação será abordada com mais detalhes.

O processo de recuperação (descrito na figura 23) é parte do escopo dessa seção por estar diretamente ligado ao uso de *backups* para segurança dos dados.

Figura 23 – Resumo de um Plano para Resposta a Incidente focado na recuperação do sistema.



Fonte: Autoria própria

Esse processo inicia pela identificação do desastre (1. Detectar a falha/desastre), que pode resultar na falha de um ou mais elementos, inclusive elementos armazenadores de dados. É seguido por "2. Determinar componentes afetados", que consiste em analisar todos os componentes e equipamentos da arquitetura para identificar os afetados e inclui investigar a razão do desastre/falha. Essa informação é então usada para "3. Executar medidas para mitigação dos danos"e para reduzir a probabilidade de reincidências.

Antes da execução do passo "4. Configurar e softwares substitutos", faz-se necessário alguma preparação que envolve obter as peças e equipamentos adequados que irão substituir os danificados e obter os dados a partir dos repositórios utilizados pelos *backups*.

Assim, para que a restauração aconteça de forma apropriada é necessário garantir que o sistema que irá receber a restauração seja uma cópia idêntica ao sistema danificado (em questão de *hardware* e *software*) antes do incidente. Completada essa etapa, a sequência exige "5. Verificar as condições comissionamento", que envolve checar e garantir que condições especiais de comissionamento e operação sejam atendidas através da aplicação das devidas configurações aplicadas.

Enfim, a etapa "6. Instalar, comissionar e testar", pode encerrar o processo de recuperação se este for bem-sucedido ou pode requisitar a reexecução de alguma das etapas para obter os requisitos de operação necessários.

A restauração é bem-sucedida quando através dos arquivos de *backups* disponíveis, executa-se a recuperação do sistema.

A tabela 13 fornece algumas recomendações de resposta e estratégia de recuperação frente a desastres em alguns dos componentes utilizados na arquitetura de uma subestação de energia.

Tabela 13 – Estratégia recomendada para recuperação e restauração frente à desastre.

Sistema Crítico	Estratégia de Resposta	Passos para Resposta	Passos para Recuperação
IHM com redundância de hardware (SICAM SCC)	Desastre: Defeito de hardware Resposta: Chavear para atuar com IHM secundária (redundante)	1. Verificar se a IHM primária está isolada ou desconectada; 2. Verificar se os backups foram realizados e estão seguros; 3. Testar a IHM secundária; 4. Alternar para IHM secundária.	1. Verificar a causa do desastre na IHM primária; 2. Obter as peças para reparo ou substituição; 3. Executar o conserto ou substituição da IHM 4. Testar a nova IHM primária; 5. Alternar a operação para IHM primária
Computador de Serviço	Desastre: Malware Resposta: Isolar o sistema infectado	1. Verificar se o computador está isolado do sistema	1. Garantir que as últimas atualizações de antivírus estejam instaladas; 2. Garantir que os antivírus estejam configurados para varrer todos os arquivos; 3. Executar uma varredura completa do sistema; 4. Recuperar dados perdidos ou corrompidos através de dados de backup; 5. Remoção de arquivos infectados. 6. Confirme que o sistema está livre do malware. 7. Reconecte o computador aos sistemas e a rede. Se o malware não for encontrado, deve-se restaurar o sistema para seu último estado e configurações seguro.
IED	Desastre: Defeito de hardware Resposta: Isolar a IED do equipamento de campo	1. Verificar se a IED está desligada; 2. Garantir que a IED está isolada e não terá influência nos equipamentos de campo; 3A. Para IEDs de controle verificar se é possível operar diretamente os equipamentos de campo; 3B. Para IEDs de proteção garantir que proteções alternativas continuam em funcionamento.	1. Obter uma IED para substituição; 2. Instalar o firmware mais atualizado; 3. Restaurar as configurações a partir dos backups para obter a configuração idêntica à da IED danificada; 4. Agendar uma intervenção no sistema para troca da IED danificada pela nova IED corretamente configurada; 5. Executar a substituição.
Equipamento de Rede	Desastre: Defeito de hardware Reposta: Isolar da rede o equipamento	1. Verificar se o equipamento está isolado do sistema.	1. Obter um equipamento equivalente para substituição; 2. Instalar o firmware e as atualizações necessárias; 3. Restaurar através dos backups a configuração idêntica ao antigo equipamento danificado; 4. Agendar uma intervenção no sistema para troca do equipamento de rede danificado pelo novo equipamento de rede corretamente configurado; 5. Executar a substituição.

Fonte: (SIEMENS, 2018)

6 Conclusão

Os testes realizados em laboratório permitiram concluir que realmente existem muitas brechas e vulnerabilidades que podem ser exploradas por criminosos cibernéticos e, dado o histórico de incidentes cibernéticos em sistemas elétricos de potência (como os ocorridos na Ucrânia), é realmente importante que tais vulnerabilidades sejam tratadas através de medidas preventivas e ferramentas.

Esse trabalho permitiu grande aprendizado, tanto em sistemas elétricos de potência quanto em segurança cibernética. Além disso, o estudo dos métodos, técnicas e ferramentas, trouxe *insights* sobre a aplicação de medidas de segurança cibernética em SEP. Visto que em sistemas de TO a disponibilidade dos serviços deve ser atendida continuamente, as técnicas de segurança cibernética precisam ser adaptadas para garantir que não interrompam a entrega dos serviços.

Esse trabalho foi um caso de estudo de segurança defensiva cuja validação dos resultados se deu pela criação de um ambiente de testes controlado para verificação da eficiência das medidas recomendadas e por considerar como as medidas poderiam ser escaladas para sistemas de maior complexidade. Os resultados obtidos a partir desses testes consistem em recomendações de medidas preventivas para segurança cibernética em SE e permitiram que o primeiro objetivo geral fosse alcançado.

Não foram detalhadamente descritos os passos para aplicação das recomendações para proteção da propriedade intelectual e industrial pertencentes à Siemens, que oferece soluções de subestação digital ciberneticamente seguras, nas quais esse trabalho foi baseado. Assim, para recomendações detalhadas sugere-se que se entre em contato com seus especialistas.

Finalmente, existe ainda margem para melhora no que se refere à aplicação de técnicas de segurança cibernética em sistemas elétricos de potência. As empresas estão começando a investir nessa área e talvez seja interessante ver iniciativas acadêmicas do lado de sistemas elétricos de potência liderando abordagens nesse escopo. Em geral, as pesquisas em segurança cibernética são lideradas por grupos de pesquisa em ciências da computação e engenharia de *software*, porém essas vertentes assumem hipóteses e considerações diferentes daquelas que seriam apropriadas para um sistema de tecnologia operacional (TO), tal como uma subestação de energia.

Muitos trabalhos ainda podem ser desenvolvidos voltados para tornar os setores de infraestrutura crítica menos frágeis e mais robustos, bem como para automatizar a aplicação de medidas de segurança propostas, essa deve ser uma das heranças desse trabalho.

Referências

ABB. **Indoor Switches - Air insulated switch-disconnectors**. 2017. Disponível em: <https://search-ext.abb.com/library/Download.aspx?DocumentID=9AKK106930A5834&LanguageCode=en&DocumentPartId=&Action=Launch>. Acesso em: 15 mai. 2019. 43

_____. **Capacitor Voltage Transformer CPB (72-800 kV)**. 2019. Disponível em: <https://new.abb.com/high-voltage/instrument-transformers/voltage/cpb>. Acesso em: 15 mai. 2019. 40

_____. **Current transformer LVB / IMT (40.5 - 550 kV)**. 2019. Disponível em: <https://new.abb.com/high-voltage/instrument-transformers/current/lvb-imt-(40-5---550-kv)>. Acesso em: 15 mai. 2019. 39

_____. **Substation merging unit SMU615**. 2019. Disponível em: <https://new.abb.com/medium-voltage/distribution-automation/campaigns/substation-merging-unit-smu615>. Acesso em: 15 mai. 2019. 43

ADVANTECH. **UNO-4673A**. 2019. Disponível em: <https://www.advantech.com.br/products/iec_61850-3%7B%7B--_ieee_1613/uno-4673a/mod_267fccba-d804-48b6-a383-f9b50d8992c7>. Acesso em: 15 mai. 2019. 44

ALI, I.; THOMAS, M.; GUPTA, S. Substation communication architecture to realize the future smart grid. Journal of Energy Technologies and Policy, 2011. 77, 78

ARCHANA, T. **Classification of Substations**. Circuit Globe, 2017. Disponível em: <https://circuitglobe.com/classification-of-substations.html>. Acesso em: 15 mai. 2019. 33

AYELLO, F. **Dez Desafios na Aplicação de Merging Unit em Subestações de Energia**. 2017. Disponível em: <https://www.linkedin.com/pulse/dez-desafios-na-aplica%C3%A7%C3%A3o-de-merging-unit-em-energia-fernando-ayello/>. Acesso em: 15 mai. 2019. 42

BONFIM, M. **Chaves Seccionadoras - O que são? Quais os Tipos?** 2016. Disponível em: <https://www.linkedin.com/pulse/chaves-seccionadoras-o-que-s%C3%A3o-quais-os-tipos-marcelo-bonfim/>. Acesso em: 15 mai. 2019. 42

CHEREPANOV, A.; LIPOVSKY, R. **GreyEnergy: Updated arsenal of one of the most dangerous threat actors**. 2018. Disponível em: <https://www.welivesecurity.com/2018/10/17/greyenergy-updated-arsenal-dangerous-threat-actors/>. Acesso em: 16 mai. 2019. 25

CIS. **CIS Microsoft Windows 10 Enterprise (Release 1803)**. 2019. 62

COVRE, H. **Integração de Dados dos Sistemas de Proteção de Subestações**. [S.l.]: Escola Politécnica da Universidade de São Paulo, 2011. 48

CRISPINO, F. Uma experiência aplicando um padrão orientado a objeto: Iec 61850 na implementação de sistemas scada para subestações. Escola Politécnica da Universidade de São Paulo, 2004. 48

CSANYI, E. **The basic things about substations you MUST know in the middle of the night!** Electrical Engineering Portal, 2019. Disponível em: <https://electrical-engineering-portal.com/substation-basics#transmission-substations>. Acesso em: 15 mai. 2019. 33

DHS. **Critical Infrastructure Sectors**. 2019. Disponível em: <https://www.dhs.gov/cisa/critical-infrastructure-sectors>. Acesso em: 16 mai. 2019. 23

DONEV, J. **Electrical Substation**. University of Calgary, 2018. Disponível em: <https://energyeducation.ca/encyclopedia/Electrical_substation>. Acesso em: 15 mai. 2019. 31

ESON, H.-E. O.; LEJDEBY, S.-A. **Evolução das Subestações**. O Setor Elétrico, 2009. Disponível em: <https://www.osetoreletrico.com.br/evolucao-das-subestacoes/>. Acesso em: 15 mai. 2019. 32

FRANCESCHETT, A.; BARROS, F. L. P.; PERES, N. T. Monitoramento da segurança cibernética de subestações utilizando syslog. 2007. 89

FRONTIN, S. O. **Equipamentos de Alta Tensão - Prospecção e Hierarquização de Inovações Tecnológicas**. [S.l.]: ANEEL, 2013. 29, 38, 39, 40, 42

GE. **RT434 GNSS Precision-Time Clock**. 2019. Disponível em: <https://store.gegridsolutions.com/ViewProduct.aspx?Model=RT434>. Acesso em: 15 mai. 2019. 41

GERHARDS, R. **The Syslog Protocol**. 2009. Disponível em: <https://tools.ietf.org/html/rfc5424>. Acesso em: 15 mai. 2019. 87

GOMES, H. **O que é IHM? Descubra aqui**. 2018. Disponível em: <https://engprocess.com.br/o-que-e-ihm/>. Acesso em: 15 mai. 2019. 43

GURJAO, E. C.; SOUZA, B. A.; CARMO, U. A. Aspectos de comunicação da norma iec-61850. 2007. 50

IEC. **TC 57 IEC TECHNICAL COMMITTEE**. 2019. Disponível em: <http://tc57.iec.ch/index-tc57.html>. Acesso em: 15 mai. 2019. 49

JARDINI, J. A. **Sistemas Elétricos de Potência - Automação**. 1997. 29, 34, 35

KASPERSKY. **Ataques de APT BlackEnergy na Ucrânia**. 2017. Disponível em: <https://www.kaspersky.com.br/resource-center/threats/blackenergy>. Acesso em: 16 mai. 2019. 24

LACERDA, S. L.; CARNEIRO, G. H. R. Dispositivos eletrônicos inteligentes (ied's) e a norma iec 61850: União que está dando certo. Instituto Federal de Educação, Ciência e Tecnologia da Paraíba, 2010. 37, 51

LAYTON, L. **Substation Design Volume I - Design Parameters**. PDH Online, 2015. Disponível em: <https://pdhonline.com/courses/e468/e468content.pdf>. Acesso em: 15 mai. 2019. 33

LIQUIDWEB. **Hardware Firewalls: An Overview of Benefits and How They Keep You Secure**. 2018. Disponível em: <https://www.liquidweb.com/blog/hardware-firewalls-an-overview-of-benefits-and-how-they-keep-you-secure/>. Acesso em: 15 mai. 2019. 58

MASLOW, A.; GREEN, C. D. A theory of human motivation. **Psychological Review**, p. 370–396, 1943. 23

MELLO, N. F. B. de. **Automação Digital de Subestações de Energia Elétrica**. 2006. Disponível em: <http://monografias.poli.ufrj.br/monografias/monopoli10000333.pdf>. Acesso em: 15 mai. 2019. 41

MODBUS-ORGANIZATION. **Modbus Application Protocol Specification**. 2012. Disponível em: <http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf>. Acesso em: 15 mai. 2019. 52

OSBORNE, C. **Industroyer: An in-depth look at the culprit behind Ukraine's power grid blackout**. 2017. Disponível em: <https://www.zdnet.com/article/industroyer-an-in-depth-look-at-the-culprit-behind-ukraines-power-grid-blackout/>. Acesso em: 16 mai. 2019. 25

PAULINO, M. E. C. Aspectos da implementação e validação de sistemas baseados na iec 61850. Anais do SBSE 2008 - Simpósio Brasileiro de Sistemas Elétricos, 2008. 37, 49

PERES, N. T. **Relatório Final de Iniciação Científica: GPS, posicionamento e relógios precisos**. 2016. 40

PHINNEY, T. **IEC 62443: Industrial Network and System Security**. 2019. Disponível em: <https://www.isa.org/pdfs/autowest/phinneydone/>. Acesso em: 15 mai. 2019. 64

POLITYUK, P.; VUKMANOVIC, O.; JEWKES, S. **Ukraine's power outage was a cyber attack: Ukrenergo**. 2017. Disponível em: <https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA>. Acesso em: 16 mai. 2019. 24

SANTOS, L.; PEREIRA, M. Uma abordagem prática do iec 61850 para automação, proteção e controle de subestações. Anais do VII SIMPASE - Sétimo Simpósio de Automação de Sistemas Elétricos, 2007. 36

SANTOS, L. F. d.; PEREIRA, M. Uma abordagem prática do iec 61850 para automação, proteção e controle de subestações. Anais do VII SIMPASE - Sétimo Simpósio de Automação de Sistemas Elétricos, 2007. 50

SEFTI. **Boas Práticas em Segurança da Informação**. [S.l.]: Tribunal de Contas da União, 2012. 63

SENGER, E. C. **Sistema de Automação de SE**. 2015. Disponível em: <https://edisciplinas.usp.br/pluginfile.php/3801723/course/section/900291/AULA%20SAS_Final%202015.pdf>. Acesso em: 15 mai. 2019. 35

SIEMENS. **High-Voltage Circuit Breakers**. 2012. Disponível em: <https://assets.new.siemens.com/siemens/assets/public.1493886289.57363d51dd291bd91128dd7665ae64e808f2fdf2.high-voltage-circuit-breakers-portfolio-en.pdf>. Acesso em: 15 mai. 2019. 43

_____. **Security Design Guidelines**. 2018. 71, 72, 83, 86, 87, 89, 95, 96, 99

_____. **RUGGEDCOM RS900G**. 2019. Disponível em: <https://w3.siemens.com/mcms/industrial-communication/en/rugged-communication/ruggedcom-portfolio/switches-routers-layer-2/compact-switches/pages/rs900g.aspx>. Acesso em: 15 mai. 2019. 46

_____. **RUGGEDCOM RX1500 / RX1501 Multi-Service Platform**. 2019. Disponível em: <https://w3.siemens.com/mcms/industrial-communication/en/rugged-communication/ruggedcom-portfolio/switches-routers-layer-3/pages/rx1500.aspx>. Acesso em: 15 mai. 2019. 48

SILVA, M. G. M. **Avaliação de Desempenho de Relés de Proteção Digitais**. 2012. Disponível em: <http://monografias.poli.ufrj.br/monografias/monopoli10005149.pdf>. Acesso em: 15 mai. 2019. 37

SNORT. **SNORT Users Manual**. 2019. Disponível em: <https://snort-org-site.s3.amazonaws.com/production/document_files/files/000/000/177/original/snort_manual.pdf>. Acesso em: 15 mai. 2019. 61

SONICGUARD. **SonicWALL TZ400 Series**. 2019. Disponível em: <https://www.sonicguard.com/datasheets/TZ/TZ_Series_Data_Sheet.pdf>. Acesso em: 15 mai. 2019. 58

SOUZA, A. L. d.; CARLSON, A. C.; SANTANA, F. R. **Arquitetura de Redes**. [S.l.]: SENAI, 2012. 53, 54

TANENBAUM, A. S.; WETHERALL, D. **Redes de Computadores 5ª Edição**. [S.l.]: Editora Campus, 2011. 29, 45, 47

TAYLOR, C.; KRINGS, A.; ALVES-FOSS, J. Risk analysis and probabilistic survivability assessment (rapsa): An assessmentapproach for power substation hardening. University of Idaho, 2002. 83

TECHTUDO. **Quais são os melhores firewalls gratuitos? Veja lista de sugestões**. 2014. Disponível em: <https://www.techtudo.com.br/dicas-e-tutoriais/noticia/2014/04/quais-sao-os-melhores-firewalls-gratuitos-veja-lista-de-sugestoes.html>. Acesso em: 15 mai. 2019. 57

USERS-GROUP-DNP3. **Overview Of DNP3 Protocol**. 2019. Disponível em: <https://www.dnp.org/About/Overview-of-DNP3-Protocol>. Acesso em: 15 mai. 2019. 51

VICENTE, D. T. d. **Aplicação dos padrões da norma IEC 61850 a subestações compartilhadas de transmissão/distribuição de energia elétrica**. [S.l.]: Escola Politécnica da Universidade de São Paulo, 2011. 50

VIEIRA, J. G. **Subestações Digitais: Tecnologias para Implementação de Uma Subestação Digital**. 2017. 42