Melhorando a Integridade de Sistemas de Automação e Comunicação em Smart Grids - Uma Arquitetura de Combate a Ciberataques

Alexandro de O. Paula[1], Rodolfo I. Meneguette[2], Vinícius P. Gonçalves[1], Alexsandra O. Andrade[3], Maycon L. M. Peixoto[4], Geraldo P. Rocha Filho[3]

[1]Universidade de Brasília – UnB – Brasília – DF – Brasil

[2]Universidade de São Paulo – USP – São Carlos – SP – Brasil

[3]Universidade Estadual Do Sudoeste Da Bahia – UESB – Vitória da Conquista – BA – Brasil

[4]Universidade Federal da Bahia – UFBA – Salvador – BA – Brasil

alexandroblind@gmail.com, meneguette@icmc.usp.br, vpgvinicius@unb.br,

alexsandra@uesb.edu.br, maycon.leone@ufba.br, geraldo.rocha@uesb.edu.br

Abstract. *This work proposes an automation architecture adapted from Smart Grid against cyberattacks, entitled STRAYER (**S**mar**T** a**R**chitecture **A**gainst c**Y**b**ER**attacks). The objective of STRAYER is to reduce the vulnerability of automation equipment in Smart Grids. STRAYER addresses parameters from i) cyber security for monitoring and access shielding, ii) interoperability to maintain communication between equipment/devices, and iii) risk management to maintain reliability and prevent cyberattacks in real-time. A prototype was built to validate the architecture. The results show increased security efficiency compared to traditional architecture, reducing equipment infection and excessive downtime in a Smart Grid. In addition, STRAYER helps prevent the network from collapsing, having only reversible losses, unlike traditional architecture.*

Resumo. *Este artigo propõe uma arquitetura de automação adaptada de Smart Grid contra ciberataques, intitulada STRAYER (**S**mar**T** a**R**chitecture **A**gainst c**Y**b**ER**attacks). O objetivo do STRAYER é reduzir a vulnerabilidade dos equipamentos de automação nas Smart Grids. O STRAYER endereça parâmetros de i) segurança cibernética para monitoramento e blindagem de acesso, ii) interoperabilidade para manter a comunicação entre equipamentos/dispositivos; e iii) gerenciamento de risco para manter a confiabilidade e prevenir ataques cibernéticos em tempo real. Um protótipo foi contruído para validar a arquitetura. Os resultados mostram aumento de eficiência de segurança em comparação com a arquitetura tradicional, diminuindo a infecção de equipamentos e o tempo de acesso indevido em uma Smart Grid. Além disso, o STRAYER contribui para evitar o colapso da rede, tendo apenas perdas reversíveis, diferente da arquitetura tradicional.*

1. Introdução

As *Smart Grids* permitem maior eficiência na operação e manutenção dos ativos das subestações de energia elétrica para melhor gerenciar suas cargas, reduzindo custos e melhorando as respostas a possíveis problemas que podem surgir [Geraldo Filho et al. 2019,

Gunduz and Das 2020]. O modelo mais atual elaborado pelo *National Institute of Standards and Technology* (NIST) consiste em um sistema de comunicação para interligar todas as áreas inerentes aos processos de energia elétrica (*i.e.* geração, transmissão, distribuição), além da inclusão das subáreas de atuação e mercado. A intenção é manter um domínio de gestão inteligente no setor elétrico [Greer 2014, Paula et al. 2020]. Além disso, todas as áreas têm seus recursos tecnológicos aprimorados para manter a automação no estado da arte, incluindo os preceitos de segurança cibernética [Cintuglu et al. 2016, Rocha Filho et al. 2020, Rocha Filho et al. 2022].

O avanço tecnológico nas *Smart Grids*, o qual visa digitalizar as subestações elétricas existentes, também proporcionou problemas de ataques cibernéticos aos meios de comunicação e protocolos do Sistema de Automação de Subestações (SAS), conceituado pela norma IEC 61850. Esses ataques ocorrem por meio das redes de computação das empresas de energia, tais como as redes de Tecnologia da Informação (TI), Tecnologia Operacional (OT), e em sua maioria, por acesso remoto [Mubarak et al. 2021]. Esses problemas foram relatados desde a concepção da *Smart Grids*, dentre os de maior impacto podem ser citados os ataques de 2017 e 2020 na Ucrânia [BBC 2016, Zhegulev 2020], em 2010 e 2015 no Irã, e 2020 no Brasil [Costa 2020].

Diversas abordagens foram propostas para resolver o problema de ataques cibernéticos nas *Smart Grids* [H.Vardhan et al. 2018, Yang et al. 2019, Lázaro et al. 2021, Faquir et al. 2021]. Recentemente, foram demonstradas formas de mitigar o ataque, como melhorias no sistema de telecomunicações [Lázaro et al. 2021], uso de soluções padrões de segurança de TI [Faquir et al. 2021] e até padronização de monitoramento e automação nas *Smart Grids* [Yang et al. 2019], sem mencionar em adaptações na arquitetura do SAS. Salienta-se, entretanto, que tais abordagens foram propostas para domínios específicos de ataques. Outra frente de pesquisa [H.Vardhan et al. 2018] propôs um projeto físico de uma subestação elétrica totalmente digital para monitorar a comunicação e automação. Contudo, os dados apresentados não visam a segurança efetiva da estrutura. Sobre os trabalhos supracitados, percebe-se a falta do fator dinâmico das referidas soluções, devido justamente à diversidade de tipos de ataques que é uma fator explorado nesta pesquisa.

Diante dessas limitações, este trabalho propõe o STRAYER (***S**mar**T** a**R**chitecture **A**gainst c**Y**b**ER**attacks*), uma nova arquitetura para mitigar problemas de ciberataques em *Smart Grids* no que diz respeito ao SAS e proteção de seus equipamentos. O STRAYER integra três parâmetros: (i) Segurança Cibernética para monitoramento e blindagem de acesso; (ii) Interoperabilidade para manter a comunicação entre equipamentos/dispositivos; e (iii) Gerenciamento de Risco para manter a confiabilidade e prevenir ataques cibernéticos em tempo real nas *Smart Grids*. Para a modelagem do STRAYER, foram utilizadas adaptações em redes de comunicação e arquitetura de automação propostas pelas normas IEC 61850, inserção de redundâncias e separação de redes de operação. Portanto, nossa arquitetura mantém a integridade do sistema de automação e comunicação para as *Smart Grids* e, consequentemente, a continuidade dessas estruturas e o pleno funcionamento dos serviços essenciais à população fornecidos por empresas de energia do setor público e privado.

Como prova de conceito, um protótipo comumente usado em redes inteligentes foi construído para validar o STRAYER projetado para operar em um SAS adaptado. Quando comparado à arquitetura tradicional, o STRAYER avança em quatro aspectos:

- Redução de $87,5$ % dos IED's afetados de ataques por acesso remoto;
- Diminuição de ataques a disjuntores em $88,9$ % a partir de acesso remoto;
- Diminuição no atraso no tempo de invasão ao sistema supervisório em $16min27seg$ em relação à arquitetura tradicional, e;
- Aumento de $01h11min23seg$ no tempo máximo de intrusão a um IED por meio do acesso remoto.

O restante deste artigo está estruturado da seguinte maneira. A Seção 2 apresenta os trabalhos relacionados e suas limitações que serão exploradas nesta pesquisa. A Seção 3 apresenta como o STRAYER foi modelado e sua principal contribuição. Seção 4 apresenta a validação do STRAYER em comparação com uma arquitetura tradicional do SAS. Por fim, a Seção 5 apresenta as conclusões e os trabalhos futuros.

2. Trabalhos Relacionados

Esta seção apresenta os trabalhos que exploram os problemas de ataques cibernéticos nas *Smart Grids*. Tais trabalhos utilizaram diferentes técnicas para propor uma solução robusta contra intrusões em seus sistemas de automação e comunicação. Em [Lázaro et al. 2021], é apresentada uma série de soluções para garantir a comunicação nas *Smart Grids*, atendendo aos requisitos estabelecidos na IEC 62351-6 com ênfase na troca de mensagens entre todos os equipamentos. Apesar da eficiência na robustez, o trabalho não apresenta soluções voltadas à segurança do SAS.

O trabalho proposto por [Faquir et al. 2021], utilizou diversas soluções existentes para proteção nas redes de TI, tais como firewalls, IDS/IPS, e acesso remoto via VPN. Com a mesma frente de pesquisa, [Yang et al. 2019] apresentou os principais problemas do sistema de monitoramento de subestações elétricas, com ênfase em comunicação e segurança cibernética. O trabalho consistiu em padronizar, de forma estática, soluções de monitoramento. Em ambos os trabalhos, não foi possível observar uma melhoria no sistema de proteção do IED. Além disso, os trabalhos baseiam-se na manutenção de atualizações de dados em *Smart Grids*, apenas com o recurso de segurança (sem gerenciamento de riscos ou interoperabilidade), mantendo uma arquitetura básica de automação. Como os ataques cibernéticos estão em constante evolução e estão mais dinâmicos, manter um método estático abriria brechas para problemas futuros.

Em [H.Vardhan et al. 2018], é modelado uma *Smart Grid* com base no conceitual de última geração. O modelo consistiu na criação de uma subestação elétrica digital piloto, com comunicação entre dispositivos no barramento de processo por meio de mensagens de SV [IEC61850-9-2 2011], com o objetivo de comparar os resultados com subestações elétricas tradicionais. Apesar de promissor, o conceito criado contou com a implementação de equipamentos e sensores digitais de alto custo nos poucos equipamentos de comutação analógicos. Ainda, o trabalho utiliza uma arquitetura básica, sem adaptações na topologia de automação e comunicação, não sendo possível perceber implementações eficientes de segurança cibernética.

Ainda com base em prototipação, [Fontes 2015] apresentou um protótipo, denominada LabProtec, para projetar uma infraestrutura para testes em subestações elétricas digitais com a aplicação da norma IEC 61850. Os testes visam facilitar o processo de comissionamento de subestações digitais por meio de testes de bancada de configurações e ajustes de proteção e automação. Foram utilizadas diversas modificações de arquiteturas

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

Voltado para o monitoramento de ameaças externas nas *Smart Grids*, [Heinisch et al. 2012] propôs um aplicativo para registro de parâmetros de segurança em tempo real. No entanto, não foi apresentado no trabalho, uso prático desses registros em possíveis ataques reais, nem dados de gerenciamento de risco. A aplicação do trabalho ainda não atingiu o estágio de ambiente controlado em uma *Smart Grid* real ou apresentação de uma arquitetura digital, diferente desta pesquisa.

Lellys et al. [Lellys et al. 2016] apresentou uma solução de interoperabilidade entre equipamentos de diferentes fabricantes. Para tanto, a partir do barramento de processos e por meio do uso de dispositivos SAMU (Stand Alone Merging Units) foi possível digitalizar uma subestação elétrica comum. Embora a apresentação dos resultados seja promissora, não foram relatadas soluções práticas em testes de lógica do SAS (sobre interesse de interoperabilidade) ou identificação de formas de abordar o risco de vulnerabilidades a ataques cibernéticos inerentes a dispositivos SAMU de alto tráfego de dados.

Outros estudos mostraram resultados em projetos piloto, como apresentado por [Kimura et al. 2010] no Brasil. Ge Li-Qing et al. [Li-Qing et al. 2019], sugeriu a integração dos sistemas de monitoramento, erro e decisão das *Smart Grids* em sua plataforma. Vicente [Vicente 2011] propôs uma visão abrangente da interoperabilidade em seu trabalho, com foco na troca de informações sobre relés de proteção de diferentes subestações elétricas e universalização da comunicação horizontal através de mensagens GOOSE. Apesar das soluções serem promissoras, não apresentam correlação ou similaridade com a proposta da STRAYER em termos de gerenciamento de risco em suas plataformas ou, apresentação de dados de validação em comum com o proposto nesta pesquisa.

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

3. STRAYER

Esta seção apresenta o STRAYER, uma nova arquitetura para mitigar os problemas de ataques cibernéticos nas *Smart Grids* no que diz respeito ao SAS e proteção de seus equipamentos. O principal objetivo do STRAYER é manter a integridade do sistema de automação e comunicação dessas estruturas e, portanto, a continuidade das mesmas e o pleno funcionamento dos serviços essenciais que são fornecidos por entidades públicas de governo e pelo setor privado.

O STRAYER foi desenvolvido em uma adaptação avançada e segura do modelo básico de arquitetura SAS da norma IEC 61850, realizando os devidos ajustes para

aplicação nas *Smart Grids*. Mantendo as recomendações que a norma exige, tais como i) a interligação entre os barramentos de Processo do *Smart Grid*; ii) o uso de mensagens GOOSE, e; iii) uso de um modelo SAS de três níveis (Estação, *Bay* e Processo). O STRAYER integra elementos de segurança, com o objetivo de identificar formas de mitigar vulnerabilidades e riscos relacionados ao alto tráfego de dados em situações de emergência na troca de informações entre os diversos dispositivos de rede como os IED's, barramentos elétricos de alta e baixa tensão e configurações de proteção, e, os sistemas envolvidos, como outras *Smart Grids*, o Centro de Operações Integrado (COI) e as redes de empresas de TI/TO.

O fluxo lógico operacional do STRAYER é apresentado na figura 1. O ponto integrador revela onde os dois dos três parâmetros são unidos. Há um grande esforço computacional neste ponto, que exige equipamentos com alto fator tecnológico e de processamento. Ao mesmo tempo, o integrador tenta fazer a comunicação entre todos os dispositivos do STRAYER e analisa os elementos que estão tentando fazer essa comunicação. Essa é a dinâmica de integração entre Interoperabilidade e Segurança Cibernética. O parâmetro de Gestão de Riscos está basicamente em todo o processo STRAYER, porém, com ênfase na entrada e na análise de dados. A análise de dados é realizada sobre os dados fornecidos. Com isso, os dados passam por um novo processo de análise de risco e são retroalimentados no integrador, possibilitando a fusão dos parâmetros em questão.

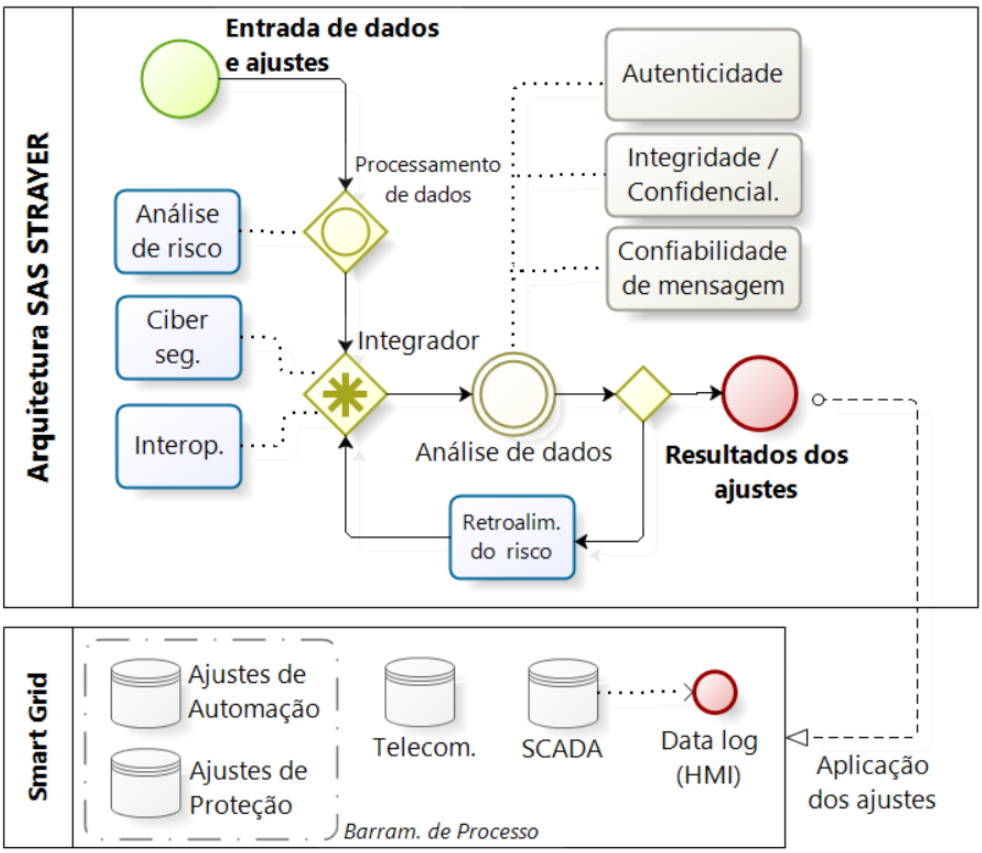


Figura 1. Fluxo lógico do STRAYER

O STRAYER foi configurado com mais de uma redundância de *switches*, ou seja, com mais de um concentrador (Principal e Secundário, conforme apresentado na Rótulo

A e ilustrado na figura 2), para manter uma arquitetura melhor estruturada em termos de segurança. O número de *switches* de cada concentrador será determinado pelo número de portas de entrada/saída (I/O) dos IED's. Existem modelos de IED no mercado com um número variado de portas dependendo de cada fabricante. Porém há unanimidade nos modelos de IED com duas portas na maioria deles. Portanto, para manter a situação de redundância nos IED's e a razoável relação custo-benefício para o STRAYER, a arquitetura é estruturado em duas portas. Como resultado, cada IED será alimentado por dois concentradores, cada um em portas diferentes (*Label* **A**, Figura 2).

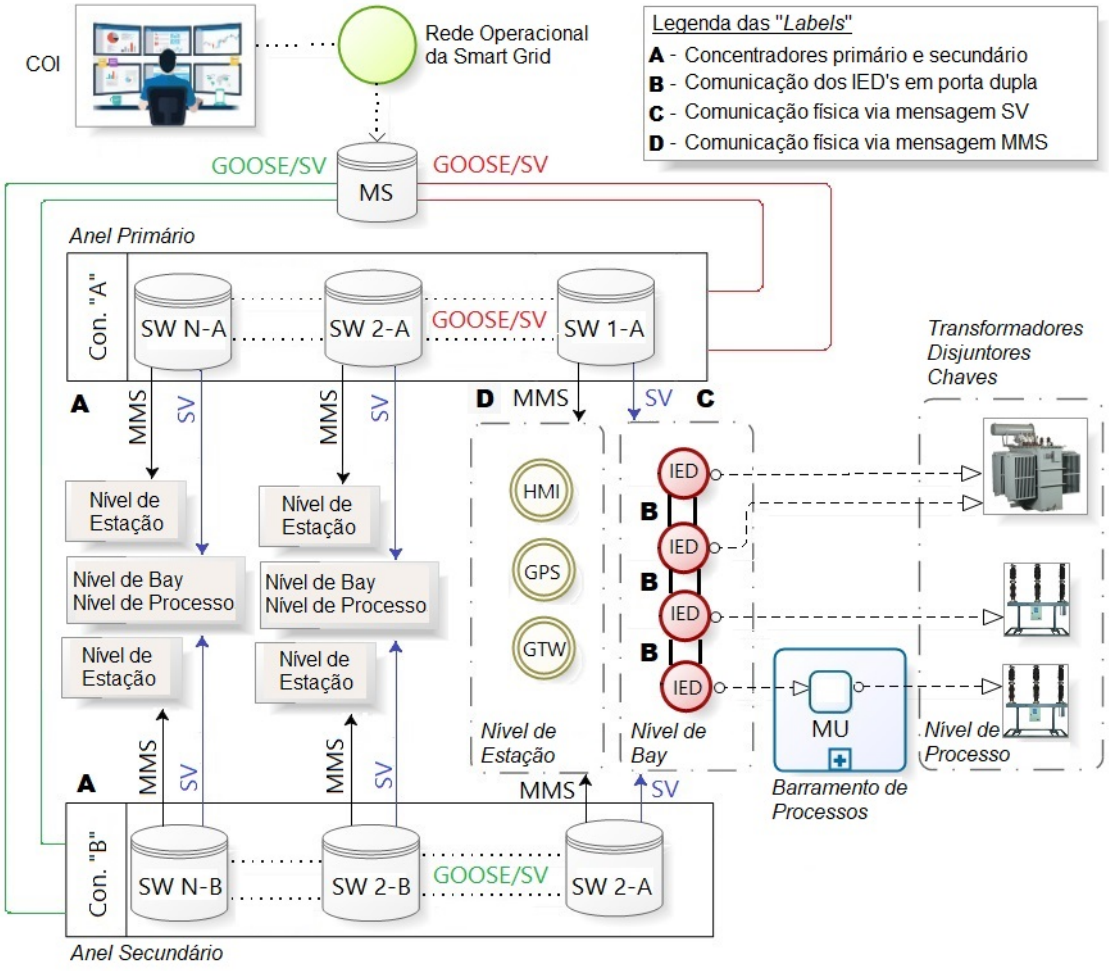


Figura 2. SAS adaptado para o STRAYER.

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

Para o requisito de comunicação no STRAYER, há o uso de mensagens SV (*Sam-*

pled Values) [IEC61850-90-1 2020, IEC61850-90-2 2020] em comunicação vertical, conforme apresentado no Rótudlo C da figura 2, e mensagens GOOSE em comunicação estritamente horizontal, com VLAN's restritas. Assim, as mensagens SV no STRAYER são um diferencial por não saturar a comunicação via GOOSE no Barramento de Processo.

Outra importante implementação realizada no STRAYER foi a utilização de protocolos de comunicação MMS (*Manufacturing Message Specification*) como comunicação vertical entre IED's de interface de usuário, conforme apresentado no Rótulo D da Figura 2, diferente da arquitetura tradicional. No STRAYER, os protocolos MMS [IEC9506 2003] atendem aos critérios de interoperabilidade, pois funcionam facilmente no processamento de dados em tempo real entre dispositivos de outros fabricantes. O MMS cria um dispositivo virtual, comum em todos os equipamentos de interface (HMI - *Human Machine Interface*) ou troca de mensagens entre usuários, como o SCADA (*Supervisory Control and Data Acquisition*), mas mantendo o nível de segurança para acesso remoto, conforme solicitado em Norma IEC 61850-7-410 [IEC61850-7-410 2015]. Quanto aos protocolos de sincronização de tempo, diferentemente da arquitetura tradicional, o STRAYER aproveita o próprio barramento de processos para implementar os protocolos, o que é permitido em algumas diretrizes.

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

4. Validação do Desempenho

Esta seção apresenta a validação do STRAYER em comparação com a arquitetura tradicional utilizada nas atuais *Smart Grids* em decorrência de um ataque remoto ao SAS. Com isso, foi possível identificar os principais avanços que o STRAYER tem em relação à um arquitetura tradicional. Em seguida, será apresentado o cenário modelado, as métricas utilizadas e o protótipo construído para gerar os resultados.

4.1. Configurações dos Experimentos e Protótipo Construído

Para o cenário, foi construído um protótipo comumente usado em uma *Smart Grids*, adaptando-o ao STRAYER, conforme apresentado na Figura 3. A configuração da arquitetura adaptada utilizou dispositivos de diferentes fabricantes para manter os critérios de interoperabilidade. A infraestrutura de campo da *Smart Grid* foi composta por duas linhas de entrada, dois transformadores de potência, dois alimentadores e nove disjuntores, conforme apresentado na figura 4. A descrição dos equipamentos utilizados no cenário para gerar os experimentos é apresentada na tabela 1.

Além disso, para validar o STRAYER, foi utilizado o software OMICRON™ IEDScout© [OMICRON 2021] para virtualizar os IED's.

Figura 3. Protótipo desenvolvido como prova de conceito para validar o STRAYER.

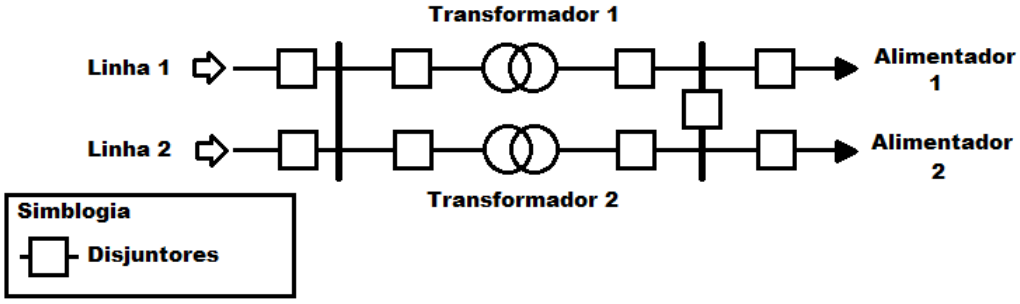


Figura 4. Diagrama unifilar da Smart Grid modelada no protótipo.

Uma vez configurado o cenário, o objetivo é atacar os comandos elétricos e as lógicas de automação dos IED's, remotamente, acessando os privilégios das mensagens GOOSE ou SV e desabilitando o acesso remoto de autenticidade do COI. Para isso, foram selecionadas três técnicas comumente utilizadas na literatura de Teste de Penetração (*PENTEST*): i) SNIFFING; ii) FORÇA BRUTA, e; iii) ROOTKIT. A forma utilizada nestes ataques foi baseada no trabalho de [Melo 2017].

O acesso remoto é o tipo mais difícil de intrusão, comparando-se com ataques diretos através das rede de Tecnologia da Informação e Operação (TI e TO), porém, não impede que seja o caminho mais acessado, historicamente, por invasores. Trata-se de um acesso não físico a qualquer estrutura, seja a *Smart Grid* ou o recinto de sua concessionária. Driblar o *firewall* é essencial.

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

Tabela 1. Dispositivos SAS e equipamentos de Smart Grid utilizados no cenário.

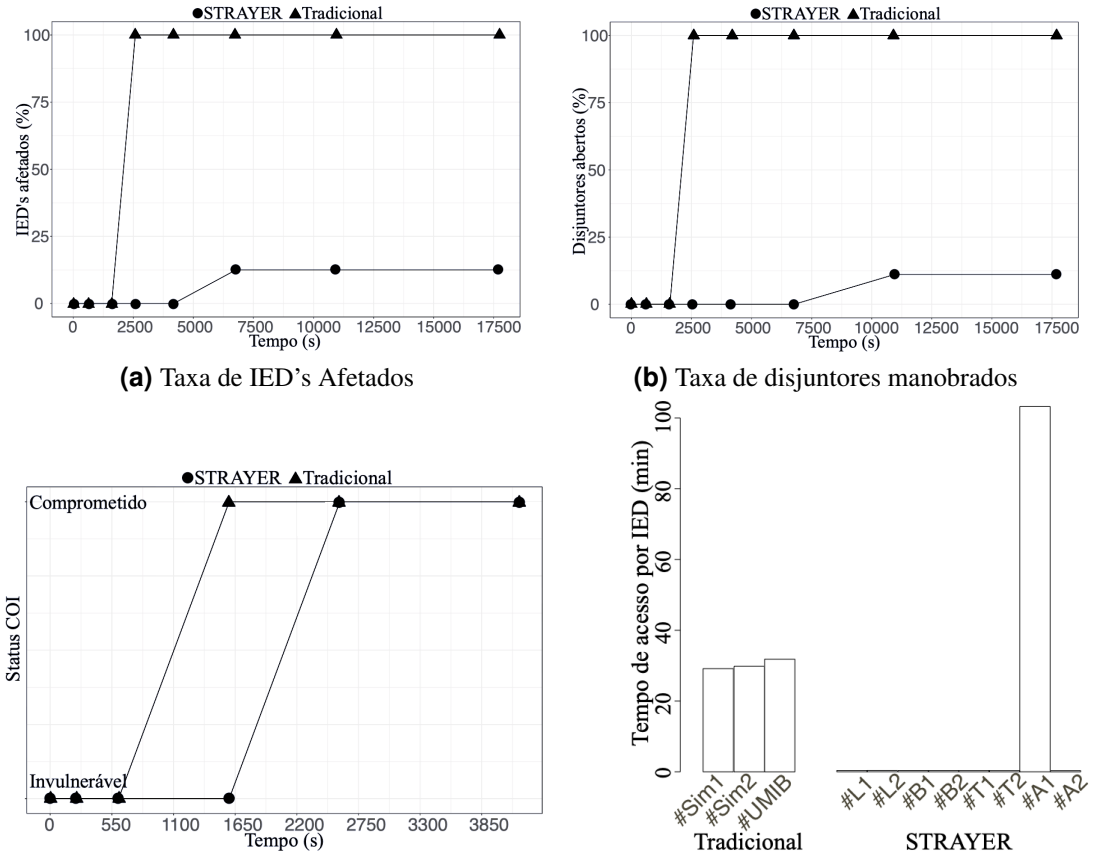
Dispositivo SAS	STRAYER	Equipamentos da SG	STRAYER
IED	8	Transformador de força	2
Switches Principais	2	Disjuntores	9
Concentrador	3	Linhas de entrada	2
Merging Unit	7	Alimentadores	2
HMI	1	Transformador de corrente	8
GPS	2	Transformador de potencial	4
Gateway	2	Chaves seccionalizadoras	10

- **Taxa de IED's Afetados** - porcentagem de IED's acessados com sucesso.
- **Taxa de disjuntores manobrados** – porcentagem de disjuntores abertos com sucesso.
- **Tempo decorrido de acesso ao COI** – tempo gasto para acessar o sistema supervisório SCADA do Centro de Operações da Smart Grid;
- **Tempo real para acessar um IED** – tempo gasto efetivo de acesso a cada IED.

Os resultados alcançados com suas discussões são apresentados a seguir.

4.2. Impacto dos Resultados Obtidos

O desempenho do cenário quando analisados de acordo com a métrica da Taxa de IED's Afetados é mostrado na Figura 5a. Uma arquitetura tradicional comumente tem perda de 100 % dos IED's em um tempo médio decorrido de 2584 segundos, enquanto que o STRAYER manteve a integridade de 87,5 % de seus oito IED's, superando aquela. O processo de retroalimentação do fluxo lógico do STRAYER detectou o acesso indevido ao switch principal do SAS, impedindo a tentativa de acessos adicionais.



(a) Taxa de IED's Afetados

(b) Taxa de disjuntores manobrados

(c) Tempo decorrido de acesso ao COI

(d) Tempo real de acesso a cada IED

Figura 5. Impacto no desempenho do STRAYER quando comparado com uma arquitetura tradicional do SAS, depois de uma invasão por acesso remoto.

O número de disjuntores afetados via acesso remoto em um determinado tempo é apresentado na figura 5b. Enquanto que historicamente, todos os disjuntores são comprometidos em uma arquitetura tradicional, apenas 11,1 % deles foram abertos no cenário do

STRAYER. Percebe-se que, mesmo com a invasão de dois IED's, referente à métrica anterior, o STRAYER impediu a abertura de um segundo disjuntor, mantendo a Smart Grid em pleno funcionamento, o que em uma arquitetura tradicional, provocaria um *blackout*.

O tempo de acesso ao COI e seu sistema SCADA remotamente é ilustrado na figura 5c. O tempo médio de invasão ao COI em uma arquitetura tradicional é de 2584 segundos. Pode-se observar que o cenário STRAYER atrasou o tempo de invasão ao COI em 987 segundos em comparação com uma arquitetura tradicional do SAS.

A relação de todos os IED's do cenário, com seus respectivos tempos de invasão, por acesso remoto foi observada na figura 5d. Uma arquitetura tradicional não consegue mitigar o ataque a seus IED's, e, tende a perder o acesso a todos os dispositivos em um tempo máximo de $31min52seg$, em média histórica, por acesso remoto. A primeira métrica mostrou que STRAYER perdeu apenas um unico IED, e mesmo assim, isso só aconteceu no momento de $1h43min15seg$, conforme a figura 5d da metrica atual. A atuacão do STRAYER quanto ao atraso de invasao foi evidenciada nesta métrica, pois, neste caso, atrasou o acesso em mais de uma hora. Esse tempo já é suficiente para que uma equipe de segurança da informação tenha tomado medidas preventivas em tempo real para eliminar a ameaça.

5. Conclusão

Apesar dos recentes avanços das *Smart Grids* e suas recomendações de segurança cibernética, ainda há ataques aos sistemas de automação e proteção dessas estruturas. Em despeito disso, este artigo expôs o problema sistêmico e real das vulnerabilidades de segurança dos padrões tradicionais de arquitetura de automação em *Smart Grids*, implantados principalmente em sistemas de governo, e propôs a arquitetura STRAYER para reduzir essa ameaça, com resultados promissores. O STRAYER integra segurança cibernética para monitoramento e blindagem de acesso, interoperabilidade para manter a comunicação entre equipamentos/dispositivos, e, gerenciamento de risco para manter a confiabilidade e prevenção contra ataques cibernéticos em tempo real em Smart Grids. Com isso, STRAYER analisou possíveis ataques cibernéticos utilizando lógica de fatores de integração dentro dos dispositivos de uma Smart Grid.

Como prova de conceito, um protótipo comumente usado nas *Smart Grids* foi construído para validar o STRAYER projetado para operar em um SAS adaptado. Os resultados mostraram que STRAYER tem um excelente desempenho no controle de acesso devido à lógica de automação e proteção de um sistema de fornecimento de energia elétrica. Além das reduções na quantidade de IED's afetados por invasões, também foi possível perceber que o STRAYER evitou o colapso de uma Smart Grid, tendo apenas perdas mínimas e reversíveis, diferentemente de uma arquitetura tradicional de SAS. Como trabalho futuro, pretendemos (i) empregar e avaliar uma arquitetura federada baseada no STRAYER para mitigar problemas de ataques em *Smart Grids*, e (ii) desenvolver um mecanismo de previsão para prevenir invasões ao STRAYER.

Agradecimentos: Geraldo P. Rocha Filho agradece à FAPESP (processo 2021/06210-3) por financiar seu projeto de pesquisa.

Referências

BBC (2016). Report: Hackers behind ukraine power cuts, says us report. *BBC News*, BBC Technology:URL: https://www.bbc.com/news/technology–35667989.

Cintuglu, M., Mohammed, O., Akkaya, K., and Uluagac, A. (2016). A survey on smart grid cyber-physical system testbeds. *IEEE Communications Surveys & Tutorials*, 19 n1:446–464.

Costa, L. (2020). Report: Energisa electric seeks to restore systems after being the target of cyberattack. *Reuters Brazil*, Yahoo Finanças:URL: https://br.financas.yahoo.com/noticias.

Faquir, D., Chouliaras, N., Sofia, V., Olga, K., and Maglaras, L. (2021). Cybersecurity in smart grids, challenges and solutions. *AIMS Electronics and Electrical Engineering*, 5:24–37.

Fontes, M. (2015). Compliant didactic platform design for commissioning a iec 61850 digital power substation control and protection system. *Masters dissertation from Rio Grande do Norte Federal University*, 129f:1–150.

Geraldo Filho, P., Villas, L. A., Gonçalves, V. P., Pessin, G., Loureiro, A. A., and Ueyama, J. (2019). Energy-efficient smart home systems: Infrastructure and decision-making process. *Internet of Things*, 5:153–167.

Greer, C. (2014). Nist sp 1108r3 - nist framework and roadmap for smart grid interoperability standards, release 3.0. *National Institute of Standards and Technology*, 1108r3:1–246.

Gunduz, M. and Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer networks*, 169:107094.

Heinisch, A., Leite, L., Spyer, B., and Rabello, M. (2012). Segurança cibernética para processos operativos em sistemas de energia elétrica. *Published in the Technology and Innovation Management Center - CGTI*, Library of Articles/Reports:–.

H.Vardhan, Ramlachan, R., Szela, W., and Gdowik, E. (2018). Deploying digital substations: Experience with a digital substation pilot in north america. *In: 71st Annual Conference for Protective Relay Engineers (CPRE). IEEE*, -:1–9.

IEC61850-7-410 (2015). Basic communication structure - hydroelectric power plants - communication for monitoring and control. *International Electrotechnical Commission*, pages 1–284.

IEC61850-9-2 (2011). Communication networks and systems for power utility automation - part 9-2: Specific communication service mapping (scsm) - sampled values over iso/iec 8802-3. *International Electrotechnical Commission*, pages 1–65.

IEC61850-90-1 (2020). Communication networks and systems for power utility automation - part 90-1: Use of iec 61850 for the communication between substations. *International Electrotechnical Commission*, pages 1–79.

IEC61850-90-2 (2020). Communication networks and systems for power utility automation - part 90-2: Using iec 61850 for communication between substations and control centres. *International Electrotechnical Commission*, pages 1–188.

IEC9506 (2003). Industrial automation systems — manufacturing message specification. *International Electrotechnical Commission*, pages 1–316.

Kimura, S., Rotta, A., Abboud, R., Moraes, R., Zanirato, E., and Bahia, J. (2010). Applying iec 61850 to real life: Modernization project for 30 electrical substations. *In: 1st Annual Protection, Automation and Control World Conference*, -:1–18.

Lellys, D., Paulino, M., d. C. Alves, and Schimitt, M. (2016). Process bus (merging unit): Concept, architecture and impact on substation automation. *Technology and Innovation Management Center - CGTI*, Library of Articles/Reports:1–7.

Li-Qing, G., Jian-Feng, W., Jing-Yu, T., and Ming, Y. (2019). Research and application of one-key sequence control technology for substations. *In: International Conference on Building Energy Conservation, Thermal Safety and Environmental Pollution Control - ICBTE 2019*, 136:01022.

Lázaro, J., Astarloa, A., Rodríguez, M., Bidarte, U., and Jiménez, J. (2021). A survey on vulnerabilities and countermeasures in the communications of the smart grid. *MDPI Electronics*, 10:1881.

Melo, S. (2017). Vulnerability exploitation in tcp/ip networks. *Alta Books*, 3:1–640.

Mubarak, S., Habaebi, H., Islam, R., Balla, A., Tahir, M., Elsheikh, A., and Suliman, M. (2021). Industrial datasets with ics testbed and attack detection using machine learning techniques. *Intelligent Automation & Soft Computing*, -:1–16.

OMICRON (2021). Test solutions for protection and measurement systems. *Product catalog*, -:35.

Paula, A. d. O., Dias, R. V., Silva, M. P., Ribeiro, M. G., Nakata, B. H., Knorst, N. A., Souza, J. R., Meneguette, R. I., Gonçalves, V. P., and Rocha Filho, G. P. (2020). Plataforma integrada de automação para simulação completa de subestações digitais com foco em interoperabilidade e segurança cibernética. *Anais*.

Rocha Filho, G. P., Brandão, A. H., Nobre, R. A., Meneguette, R. I., Freitas, H., and Gonçalves, V. P. (2022). Host: Towards a low-cost fog solution via smart objects to deal with the heterogeneity of data in a residential environment. *Sensors*, 22(16):6257.

Rocha Filho, G. P., Meneguette, R. I., Maia, G., Pessin, G., Gonçalves, V. P., Weigang, L., Ueyama, J., and Villas, L. A. (2020). A fog-enabled smart home solution for decision-making using smart objects. *Future Generation Computer Systems*, 103:18–27.

Vicente, D. (2011). Application of iec 61850 standards in electrical power transmission/distribution shared substations. *Thesis from Sao Paulo University*, -:1–117.

Yang, W., Heng-Xuan, L., Shi-Ping, E., and Kan-Jun, Z. (2019). Research on classification of substation background information for monitoring. *In: International Conference on Building Energy Conservation, Thermal Safety and Environmental Pollution Control - ICBTE 2019*, 136:01023.

Zhegulev, I. (2020). Report: Ukraine asks fbi to help probe suspected russian hack of burisma. *Reuters*, U.S. Legal News:URL: https://www.reuters.com/article/idUSKBN1ZF1KL.