Plataforma Integrada de Automação para Simulação Completa de Subestações Digitais com Foco em Interoperabilidade e Segurança Cibernética

Alexandro O. Paula[1,2], Ricardo V. Dias[2], Márcio P. Silva[2], Mauri G. Ribeiro[2], Bruno H. Nakata[3], Natasha A. Knorst[3], Jefferson R. Souza[4], Rodolfo I. Meneguette[5], Vinícius P. Gonçalves[1], Geraldo P. Rocha Filho[1]

[1]Universidade de Brasília (UnB)
unb.br – 70.910-900 – Brasília – DF – Brazil

[2]Gerência de Engenharia de Manutenção e Automação do Sistema – CEB Distribuição
ceb.com.br – 71.215-902 – Brasília – DF – Brazil

[3]Sinapsis Inovação em Energia
sinapsisenergia.com – 01.420-000 – São Paulo – SP – Brazil

[4]Faculdade de Computação – Universidade Federal de Uberlândia (UFU)
facom.ufu.br – 38400-902 – Uberlândia – MG – Brazil

[5]Instituto de Ciências Matemáticas e de Computação - Universidade de São Paulo (USP)
icmc.usp.br – 13566-590 – São Carlos – SP – Brazil

{alexandro.paula, ricardo.dias, marciopereira, mauri}@ceb.com.br,
{bruno.nakata, natasha.knorst}@sinapsisenergia.com, jrsouza@ufu.br,
meneguette@icmc.usp.br, {vpgvinicius, geraldof}@unb.br

Abstract. *In face of the current situation of vulnerability of supervisory energy systems, witnessed in Brazil and around the world (Ukraine and Iran), this work develops a study to the creation of a platform that simulates the implementation of a new automation/protection architecture, according to IEC 61850, in virtual substations created in laboratory, before applying it in digitalized physical substations, in order to obtain Cybersecurity, Integration between equipment of different manufactures and Risk Management. The assembly of this platform is still on evaluation with companies that will supply the necessary equipment for its conception. The differential of this work is based on previous analysis, in an isolated environment, of the application parameters at the commissioning of a digital substation.*

Resumo. *Tendo em vista à atual situação de vulnerabilidade digital dos sistemas supervisórios de energia, presenciada no Brasil e ao redor do mundo, este trabalho desenvolve uma plataforma que simula a implantação de nova arquitetura de automação/proteção, segundo a IEC 61850, em subestações virtuais em laboratório, antes de aplicá-la nas subestações físicas digitalizadas. O objetivo é obter Segurança Cibernética, Integração entre equipamentos de diferentes fabricantes e Gerenciamento de Riscos. A montagem da plataforma, em forma de laboratório, ainda está em fase de*

avaliação junto às empresas que irão fornecer os equipamentos necessários para a sua concepção. O diferencial deste trabalho está baseado na análise prévia, em ambiente isolado, dos parâmetros da aplicação no comissionamento de uma subestação digital.

1. Introdução

A constante evolução dos equipamentos presentes em sistemas elétricos de geração, transmissão e distribuição, fez com que as subestações ficassem comunicativas, pelo fato do rápido progresso de tecnologia, com a implantação do Sistema de Automação em Subestações (SAS) e concentradores via fibra ótica entre as subestações e centros de operação. Entretanto, tal avanço, apesar de contribuir com pontos positivos, traz malefícios no que diz respeito à vulnerabilidade a ataques cibernéticos gerais (*Denial of Service* - DoS) ou específicos, com a intenção crítica de derrubar determinadas ou várias subestações em um país, como houve na Ucrânia, em usinas de enriquecimento de urânio no Irã, e recentemente, em onze estados brasileiros [Costa 2020].

Os trabalhos realizados em destaque, especificamente, sobre a alteração de arquitetura de automação para a aplicação de segurança, segundo a norma IEC 61850 nas subestações [Heinisch et al. 2012] e sobre a concepção de uma plataforma de simulações [Lellys et al. 2010] estão sendo desenvolvidos em face das demandas de segurança em lógicas de automação dados aos acontecimentos no mundo. Essas tratativas dispostas pelo Brasil, é uma necessidade de ampliação da segurança da automação em subestações, abordada pelo Centro de Gestão e Estudos Estratégicos (CGEE) que propuseram rotas tecnológicas de Desenvolvimento de Funções de Barramento de Estação e de Processo, e para Desenvolvimento de Ferramentas para Sistemas de Testes em Tempo Real, que hoje possuem baixa maturidade tecnológica, e são essenciais para a modernização dos SAS [CGEE 2018].

A inovação deste trabalho em relação ao estado da arte [Heinisch et al. 2012, Lellys et al. 2010, Fontes 2015, Yang et al. 2015, Tebekaemi et al. 2016] consiste em desenvolver uma plataforma integrada de automação para as simulações de subestações digitais, a qual permite realizar não só testes de interoperabilidade de equipamentos e testes de lógicas que compõem o sistema de automação da subestação, mas estudar e identificar maneiras de mitigar vulnerabilidades relativas ao tráfego elevado de dados em situações de emergência e à segurança cibernética na troca de informações entre os vários componentes e sistemas envolvidos, em uma nova arquitetura, sendo complementado com a gestão dos riscos.

Ademais, o trabalho foi proposto seguindo a métrica administrativa de Gestão de Projetos [PMI 2018]. Por esse motivo, o mesmo foi fracionado em doze fases distintas para melhor organizar o andamento. A pesquisa se encontra em fase de montagem de parcerias com fabricantes para a conceituação da plataforma, seguindo o modelo de arquitetura proposta nesta pesquisa.

O restante deste artigo está organizado da seguinte forma. A Seção 2 apresenta os trabalhos correlatos com esta pesquisa, fazendo uma comparação entre todos eles; assim levando em consideração à originalidade. A Seção 3 descreve o desenvolvimento da pesquisa e a Seção 4, os resultados parciais são discutidos. A Seção 5 apresenta a conclusão e os trabalhos futuros.

2. Trabalhos Relacionados

Em outros trabalhos relacionados, os projetos registrados na ANEEL [ANEEL 2020] foram identificados com alguns tópicos específicos presentes nesta pesquisa. Vale frisar que até o momento não foram encontrados trabalhos com a abrangência da originalidade deste trabalho.

Ao tema de segurança cibernética, a pesquisa encontrada em [Heinisch et al. 2012], relacionado ao projeto PD-4950-0523/2012 da Aneel [ANEEL 2020], propuseram um plano estruturado de segurança cibernética com controle automático em uma distribuidora de energia elétrica brasileira, através de aplicativo de gestão da interoperabilidade. Entretanto, a ferramenta ainda não foi desenvolvida, e será aplicada inicialmente na distribuidora em questão, não prevendo abrangência universal diferente desta pesquisa.

Em relação ao tema de simulação do barramento de processos (Subestação digital), o trabalho de [Lellys et al. 2010] relacionado ao projeto PD-2934-0007/2011 da Aneel [ANEEL 2020] aborda a possibilidade de extração máxima dos relés digitais (IED's) como forma de utilizarmos como *Stand Alone Merging Units* (ou simplesmente, *Merging Units*), que é uma abordagem do barramento de processos disposto na IEC 61850. Todavia, o resultado do trabalho demonstrou apenas a implantação da função de Merging Unit em IED's presentes em subestações ao redor do mundo. Não foi apresentado o funcionamento do barramento dos processos realizando uma interoperabilidade, a não ser de um determinado fabricante presente no artigo.

Não foram encontrados trabalhos [Fontes 2015, Yang et al. 2015, Tebekaemi et al. 2016], que abordem uma plataforma para simulação de uma subestação digital, com características desta pesquisa, os quais são: a) Plataforma de automação que permite realizar testes completos de uma subestação digital; b) Desenvolvimento de metodologia e realização testes referentes à segurança cibernética; e c) Desenvolvimento de metodologia e simulação de barramento de processos e mensagens SV.

3. Desenvolvimento da pesquisa

A atividade envolve a elaboração de um *workstatement*, com análise, infraestrutura existente nas subestações da distribuidora, com o levantamento dos equipamentos, sistemas e lógicas de proteção e controle existentes em cada subestação, utilizando as técnicas de gerenciamento de riscos, seguindo a norma ISO 31000 [ISO 31000 2018].

Sendo assim, entre outros objetivos, a pesquisa visa a melhoria do barramento de processos, com adaptação da comunicação entre os IED's (*Sample Values - SV* ou GOOSE), testes dos requisitos de Segurança Cibernética e integração dos equipamentos com sistemas de supervisão externos às subestações e lógicas de proteção e controle.

3.1. Arquitetura Desenvolvida

O trabalho consiste em aplicar, entre outras normas da IEC 61850, a atual IEC 61850-9, através da plataforma de simulação controlada em laboratório, aplicando as mesmas condições de digitalização em subestações em nova arquitetura de automação.

Simulações são úteis, uma vez que são atividades experimentais antes da implantação do produto ou filosofia dentro de um sistema existente em qualquer distribuidora.

Para melhor apresentação do trabalho, é necessário definir a norma IEC 61850. A Figura 1 apresenta o modelo final proposto pela norma, com destaque no barramento de processos, que não existe em uma subestação convencional. Segundo [IEC 61850 2020], a definição do SAS é baseada em três níveis de barramentos, sendo elas:

1. Nível de estação: composto pela IHM (interface homem-máquina), sistema supervisório (SCADA), switch Ethernet e sincronismo de tempo via protocolo PTP.
2. Nível de *bay*: composto pelas lógicas de controle e proteção, implementados nos dispositivos eletrônicos inteligentes que realizam a operação dos disjuntores e chaves motorizadas.
3. Nível de processo: sensores, *Stand Alone Merging Units* (SAMU) e atuadores conectados em uma rede Ethernet.

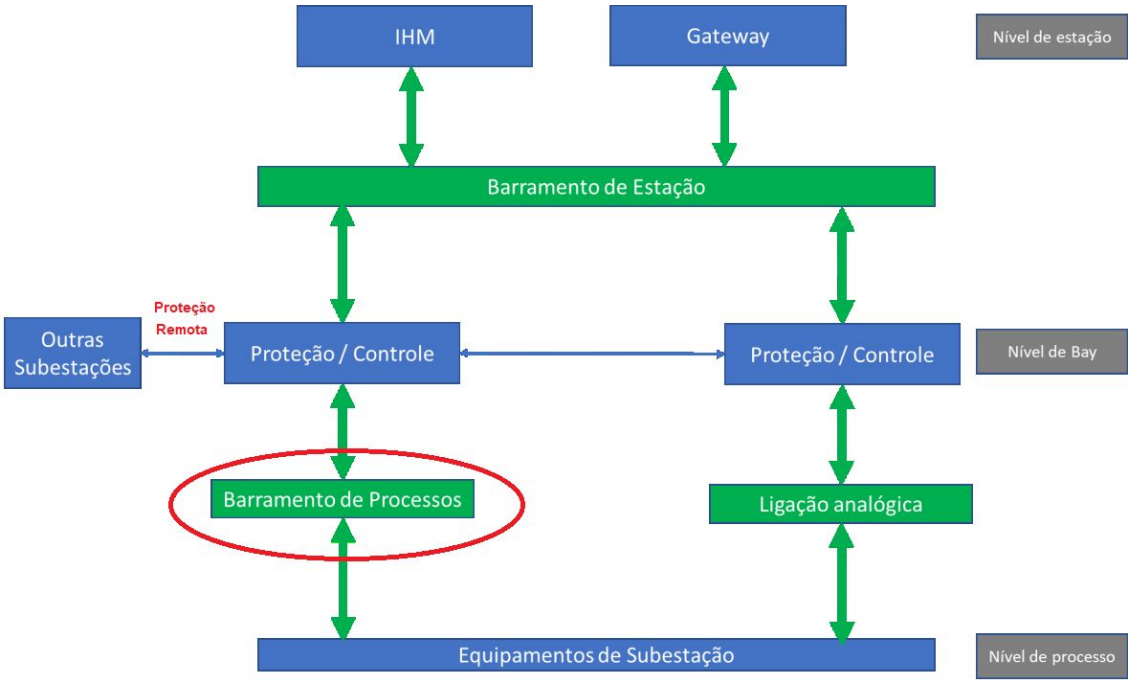

Figura 1. Sistema de Automação de Subestação (SAS), base da norma IEC 61850

A configuração aplica o uso de mais de um concentrador, *switches* em anel de forma a permitir autoconfiguração, comunicação via cabo ótico em nível de Gigabit Ethernet e utilização de dispositivos com portas duplas de comunicação.

Na parte lógica e de troca de mensagens, o destaque da arquitetura se dá pelo uso de mensagens GOOSE horizontalmente (entre os IED's, com VLAN's restritas), MMS para comunicação vertical (IHM, Centro de Operações, SCADA) e uso de PTP e PRP.

A Figura 2 apresenta a arquitetura desenvolvida. Percebe-se a separação dos dados das redes corporativas e da operação da subestação. Com isso, é possível

aumentar a dificuldade de acesso de fora para dentro de possíveis ataques cibernéticos. Cada barramento da subestação possui seu próprio concentrador, sendo este ainda com a redundância no outro lado dos IED's.

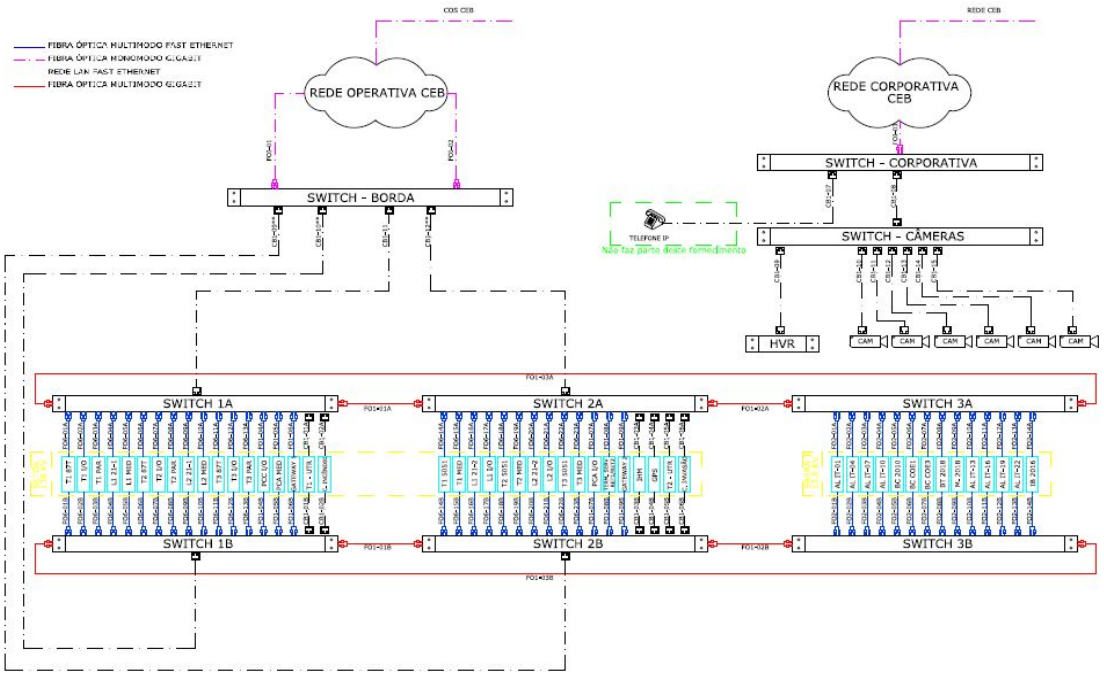

Figura 2. Arquitetura de automação. Aplicação integral da norma IEC 61850

3.2. Plataforma Proposta

Serão realizadas todas as atividades de montagem da Plataforma, com a instalação dos equipamentos em *racks* e conexão por meio de cabos de fibra ótica. A Figura 3 apresenta a plataforma integrada. A atividade de comissionamento da plataforma consiste em testes básicos de funcionamento dos sistemas e conexões para verificar funcionamento dos componentes e a execução deles.

A estrutura da Plataforma Integrada de Automação será destinada para testes de novos componentes de diferentes fabricantes, tendo nossa arquitetura como estudo de caso.

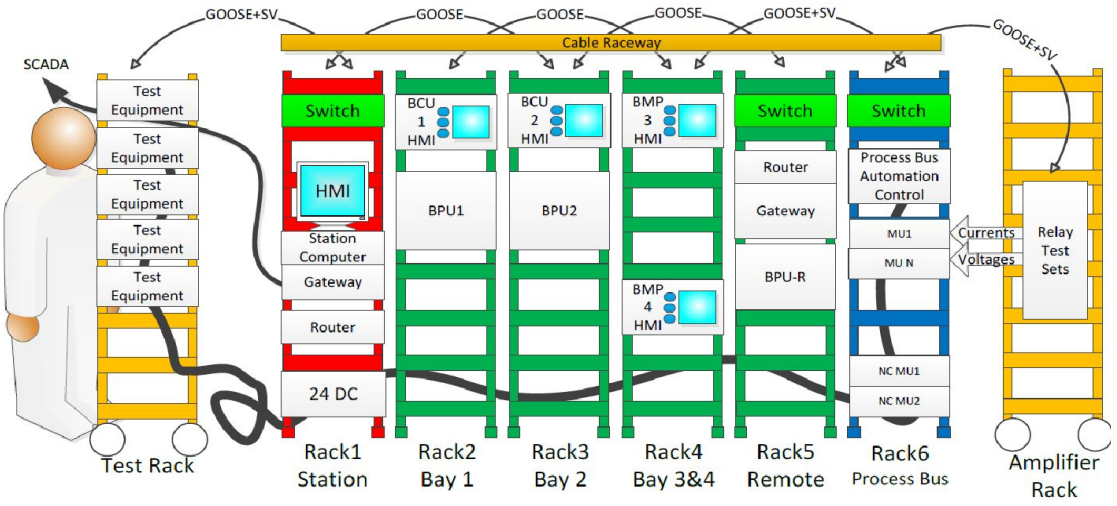

Figura 3. Plataforma Integrada montada e instalada

3.3. Teste de interoperabilidade entre equipamentos e de segurança cibernética

O objetivo é elaborar a metodologia para realização de testes de interoperabilidade entre equipamentos de diferentes fabricantes, verificando se os mesmos se comunicam de forma previsível e confiável. Para os casos de mensagens GOOSE, mensagens trocadas entre equipamentos da subestação e centro de operações, além das mensagens trocadas entre subestações, as normas vigentes [IEC 61850-90-5, IEC 61850-90-2 e IEC 61850-90-1] apresentam grau avançado de maturidade, com grande número de aplicações realizadas em campo que produzirão melhorias nesses documentos. Assim, propõe-se utilizar uma metodologia de testes semelhante à apresentada nessas normas.

Para viabilizar a implementação nas subestações, serão realizadas as atividades:

1) Avaliação das variações existentes na norma [IEC 61850-9-2 2004] para a escolha do melhor formato para transmissão de mensagens SV, considerando os equipamentos disponíveis e as especificidades de cada subestação.

2) Definição da arquitetura do barramento de processo para uma subestação (não a genérica inicial), mantendo níveis adequados de confiabilidade. A norma [IEC 61850-9-2 2004] recomenda algumas alternativas de arquiteturas de barramento de processo, porém não abrange mecanismos de redundância contra possíveis problemas no barramento. Dessa maneira, torna-se interessante considerar na metodologia a realização de testes específicos para definição da arquitetura de barramento de processo, considerando critérios econômicos e de confiabilidade.

3) Sincronismo de tempo entre equipamentos através do barramento de processo. O sincronismo é realizado através de um barramento separado, mas existem normas que sugerem usar o barramento de processo para sincronismo.

4) Em relação à segurança cibernética, depois do laboratório implantado, serão analisadas as vulnerabilidades existentes no SAS. A intenção é cobrir problemas de configuração de IEDs, ataques à rede de comunicação que causam atraso na transmissão de dados, manipulação de dados, *malwares* que permite liberar acesso remoto a invasores e ataques cibernéticos coordenados.

4. Resultados parciais

Conforme descrito na Seção 3, este trabalho de pesquisa concluiu uma arquitetura genérica para aplicação nas subestações. Paralelamente, a pesquisa se encontra em andamento, na fase de *Workstatement*.

Parcialmente, em análise dos riscos, não houve alteração no nível dos mesmos, segundo o disposto na avaliação de riscos da ISO 31000 e PMBOK. A parte de gerenciamento de riscos da automação ainda está sendo elaborada, mas só terá concretização com o funcionamento da plataforma.

5. Conclusão

O presente artigo propôs uma Plataforma Integrada de Automação para Simulação Completa de Subestações Digitais visando a comunicação entre equipamentos de diversos fabricantes e Segurança Cibernética. A união da criação dessa plataforma aliada à interoperabilidade e segurança, resulta em uma solução completa para a digitalização e melhor gestão dos ativos das subestações de distribuição, transmissão e geração.

Evidenciado pela necessidade demonstrada neste artigo, vislumbra-se que é possível realizar uma plataforma com os requisitos supracitados dada a celeridade do andamento do projeto e interesse de variadas empresas e fabricantes de componentes de proteção e automação em auxiliar na concepção do laboratório.

Agradecimentos: Alexandro O. Paula, Ricardo V. Dias, Márcio P. Silva e Mauri G. Ribeiro, Bruno H. Nakata e Natasha A. Knorst agradecem pelo apoio Profissional, meios tecnológicos e financiamentos concedidos pelo projeto de P&D da CEB Distribuição/Aneel (processo SEI-GDF nº 00310-00009617/2019-32).

Referências

ANEEL - Agência Nacional de Energia Elétrica (2020). Retirado do site http://www.aneel.gov.br/documents/656831/14930488/Projetos_PED-ANEEL_%28Res_Norm_316-2008%29-2018-05-23.xls/f02bb791-2810-0b67-1498-faed68e1f6f6, Visitado em Janeiro, 2020.

CGEE – Centro de Gestão e Estudo Estratégicos (2018). Prospecção Tecnológica no Setor Elétrico – volumes 4-8 – Transmissão e 5-8 – Distribuição.

IEC 61850: 2020 SER (2020). Communication networks and systems for power utility automation - ALL PARTS. IEC. Fevereiro.

IEC 61850-9-2 (2004). Specific Communication System mapping (SCSM) – Sampled Values Over ISO/IEC 802-3. IEC. Fevereiro.

IEC 61850-90-1 (2020). Communication networks and systems for power utility automation - Part 90-1: Use of IEC 61850 for the communication between substations. IEC. Março.

IEC 61850-90-2 (2020). Communication networks and systems for power utility automation - Part 90-2: Using IEC 61850 for communication between substations and control centres. IEC. Fevereiro.

IEC 61850-90-5 (2020). Communication networks and systems for power utility automation - Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118. IEC. Maio.

ISO 31000 (2018). Risk Management - Guidelines. Março.

PMI - Project Management Institute (2018). Um Guia do Conhecimento em Gerenciamento de Projetos - Guia PMBOK 6, Project Management Institute, 6ª edição.

Tebekaemi, E. and Wijesekera, D. (2016). Designing an IEC 61850 based power distribution substation simulation/emulation testbed for cyber-physical security studies. In: Proceedings of the First International Conference on Cyber-Technologies and Cyber-Systems. p. 41-49.

Lellys, D., Paulino M., Alves do Carmo U. e Schimitt M. (2010). Process bus (Merging Unit): Conceito, arquitetura e impacto na automação de subestações. Apresentado no XIX Seminário Nacional de Distribuição de Energia Elétrica - SENDI.

Heinisch, A., Leite L., Spyer B. e Rabello M. (2012). Segurança Cibernética para Processos Operativos em Sistemas de Energia Elétrica. Publicado no Centro de Gestão de Tecnologia e Inovação – CGTI.

Costa L. (2020). "Elétrica Energisa busca restabelecer sistemas após ser alvo de ataque cibernético" <https://br.financas.yahoo.com/noticias/el%C3%A9trica-energisa-busca-restabelecer-sistemas-180337556.html>. Reportagem publicada no site Yahoo Finanças. São Paulo.

Fontes, M. (2015). Projeto de plataforma didática compatível com a norma IEC61850 para comissionamento de sistema digital de controle e proteção de subestação de energia elétrica. Dissertação de mestrado. Brasil.

Yang, Y. et al. (2015). Cybersecurity test-bed for IEC 61850 based smart substations. In: Power & Energy Society General Meeting. IEEE. p 1-5.