Vantagens da SDN para Controle Baseado em Ethernet

Marcos Cabral, Mauricio Silveira e Ryan Urie
Schweitzer Engineering Laboratories, Inc.

© 2019 por Schweitzer Engineering Laboratories, Inc. Todos os direitos reservados.

Todos os nomes de marcas ou produtos que aparecem neste documento são marcas comerciais ou registradas de seus respectivos proprietários. Nenhuma marca registrada da SEL pode ser usada sem permissão por escrito. Os produtos da SEL que aparecem neste documento podem estar cobertos por patentes dos EUA e estrangeiras. 20190627

Introdução

Existem muitas opções disponíveis para interconectar redes Ethernet. No entanto, a interconexão de redes de tecnologia da operação (TO) que usam o controle baseado em Ethernet apresenta desafios únicos. Por exemplo, gerenciar e otimizar o fluxo de mensagens GOOSE IEC 61850 (mensagens *multicast* de alta prioridade para comunicação peer to peer) em redes requer uma precisa engenharia em redes tradicionais que usam o *Rapid Spanning Tree Protocol* (RSTP).

Este artigo examina os benefícios do uso da tecnologia de redes definidas por software (sigla em inglês, SDN) para facilmente interconectar e gerenciar o tráfego em redes Ethernet TO que se comunicam usando a tecnologia IEC 61850. Um estudo de caso da Usina de Itaipu, na América do Sul, uma das maiores instalações hidrelétricas do mundo, é usado para ilustrar esses benefícios [1].

Visão Geral da SDN

Redes SDN foram originalmente desenvolvidas para gerenciar redes de tecnologia da informação (TI) com grandes volumes de tráfego e frequentes alterações de topologia de rede. No entanto, foi aplicada mais recentemente em redes TO em subestações e sistemas de controles industriais com grande sucesso. Ao contrário das redes de TI, as redes TO não sofrem alterações frequentes. Embora as redes TI sejam dinâmicas e flexíveis, as redes TO são responsáveis por processos críticos e tomadas de decisão em alta velocidade, que exige uma rede de comunicação muito mais previsível e determinística. A Tabela 1 compara as características desses dois ambientes de rede.

Tabela 1 Comparação das Características Ideais de Redes de TI e TO

IT	**OT**
Frequentes alterações na topologia da rede	Redes projetadas especificamente para um propósito
Conexões p*lug-and-play*	Segurança *Deny-by-default (*negar como padrão)
Conectividade não-bloqueada	Fluxo em lista de permissões (*whitelist*)
RSTP para caminhos de *backup*	Caminhos de *failover* pré-definidos
Serviços intermitentes com curta vida útil	Serviços contínuos com vida útil longa

Em redes tradicionais, os switches que encaminham pacotes também determinam o caminho da rede para enviar esses pacotes, usando protocolos como o RSTP. Todavia, numa rede SDN, as funções de tomada de decisões são removidas dos switches e, ao invés disto, tratadas por um controlador SDN centralizado, que é um software que toma todas as decisões para a rede. Os switches, por sua vez, recebem instruções de encaminhamento de pacotes do controlador SDN. Isso permite que eles se concentrem apenas no encaminhamento físico de pacotes.

Uma rede SDN permite que usuários pré-definam os caminhos principais e de backup para cada fluxo de comunicação na rede a partir do controlador SDN. Como tal, as redes SDN TO podem ser projetadas da mesma maneira que os próprios sistemas de potência. Cada dispositivo sabe antecipadamente o que fazer em caso de falha na rede. Como não há necessidade de negociar caminhos de encaminhamento, como em uma rede Ethernet RSTP, quase não há atraso no encaminhamento de pacotes quando há uma falha, o que acelera a recuperação e minimiza a perda de pacotes.

Em uma rede SDN, os engenheiros de redes podem definir diferentes caminhos de encaminhamento para diferentes aplicações (por exemplo, acesso à rede de engenharia, GOOSE ou SCADA). Isso permite que eles priorizem o tráfego crítico ou os enviem em um *link* dedicado. Em uma rede Ethernet tradicional, todos as aplicações usam os mesmos *links*, o que limita o uso agregado de largura de banda ao do *link* mais lento na rede. Como uma rede SDN pode atribuir a cada aplicação seu próprio caminho, toda a largura de banda da rede pode ser utilizada.

Os switches SDN usam a segurança *deny-by-default*, na qual todos os pacotes sem um caminho predefinido e autorizado são rejeitados. Cada caminho de comunicação e tipo de pacote devem ser autorizados com antecedência, o que evita tráfego indesejado ou mal-intencionado na rede.

O determinismo e a segurança de uma rede SDN fornecem os seguintes benefícios:

- Gerenciamento otimizado do tráfego de redes através da eliminação de tráfego desnecessário, priorização de tráfego crítico, controle total de caminhos de rede e a capacidade de definir limites de largura de banda e taxa de dados.
- Melhor conscientização da situação, devido a capacidade de monitorar todo o fluxo de dados. Isso permite que os proprietários do sistema saibam em tempo quase real o que está acontecendo em sua rede.
- Tempo de recuperação de falhas extremamente rápido. Como os caminhos de *backup* são predefinidos, os switches podem redirecionar o tráfego assim que uma falha de rede é detectada (geralmente menos de 100 µs, contra 10–30 ms para redes tradicionais).
- Maior segurança cibernética devido a arquitetura *deny-by-default* e a habilidade de controlar todos os pacotes na rede. A SDN também elimina vetores de ataque comuns encontrados em redes tradicionais, como envenenamento de cache do ARP (*Address Resolution Protocol*), falsificação de BPDU (*Bridge Protocol Data Unit*), tabelas MAC (*Media Access Control*), RSTP e ataques de difusão DoS (*Denial of Service* – Negação de Serviço).
- Testes e documentação mais precisos. Como cada caminho é criado explicitamente, é possível verificar cada um deles durante o comissionamento e o teste de rede (incluindo os caminhos de *failover*) e documentar o conjunto completo de caminhos, protocolos e aplicações.

Para mais detalhes sobre a estrutura, função e histórico de redes SDN, consulte as referências [2] a [9].

SDN pela SEL

A solução SDN da SEL consiste em um switch de Rede Definida por Software tipo SEL-2740S e um controlador de fluxo de Rede Definida por Software SEL-5056, que pode ser hospedado em um computador tipo SEL-3355, como mostrado na Figura 1 ou em um computador ou servidor Microsoft Windows equivalente.

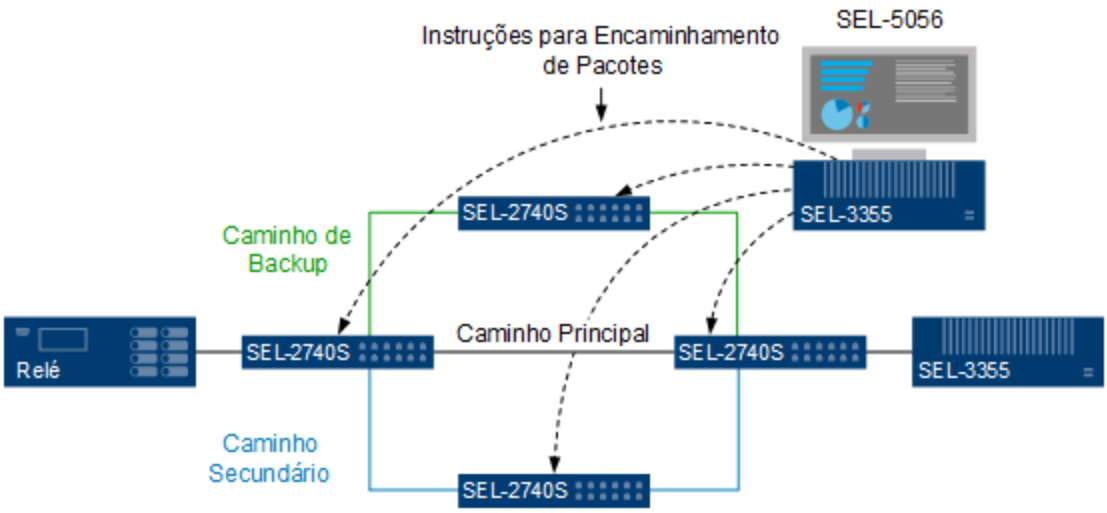

Figura 1 Configuração Básica da Rede SDN da SEL

Depois que todas as regras de fluxo forem configuradas no controlador de fluxo SEL-5056, elas serão enviadas para cada switch SEL 2740S sem interrupções do serviço. Uma vez que as regras são enviadas a cada switch, o SEL-5056 pode então monitorar as conexões e os fluxos através da rede

O controlador de fluxo SEL-5056 proativamente configura caminhos redundantes não apenas para o caminho principal, mas também para o caminho secundário. Isso permite que os switches SEL-2740S restaurem a rede sem a necessidade de se comunicarem com o SEL-5056. Se o caminho principal falhar, os switches SDN transferem automaticamente esses fluxos de dados para o caminho secundário. Se o caminho secundário também falhar, eles chaveiam os fluxos para o caminho de backup. Essa redundância fornece um alto grau de confiabilidade de rede.

A solução SDN da SEL oferece alta confiabilidade e desempenho, gerenciamento e teste de rede simplificados, segurança cibernética aprimorada e conhecimento completo da situação.

Estudo de Caso da Usina de Itaipu

Desafio de Interconexão

A represa de Itaipu atravessa a fronteira entre o Brasil e o Paraguai e é co-administrada pelas duas nações. Em 2016, estabeleceu um recorde mundial para a energia produzida por uma única instalação e atualmente está classificada apenas atrás da Barragem das Três Gargantas na China para a capacidade geral de geração [10] [11].

A proteção contra isolamento forçado (FIP) é um tipo de esquema de controle de emergência em Itaipu. Utiliza painéis na subestação da barragem de Itaipu (FIP-01) e na subestação de Hernandarias (FIP-02) a cerca de um quilômetro de distância. O painel FIP-02 da subestação de Hernandarias abre a interligação do sistema elétrico entre Itaipu e a Administração Nacional de Eletricidade (ANDE) do Paraguai quando há variações indesejáveis de tensão e frequência ou uma reversão no intercâmbio de energia entre Itaipu e ANDE. Ambas as subestações se comunicam com um sistema integrado de redes industriais (SIRI), que é um centro de operação e controle para todas as subestações de Itaipu e semelhante a um sistema SCADA. Este esquema é mostrado na Figura 2.

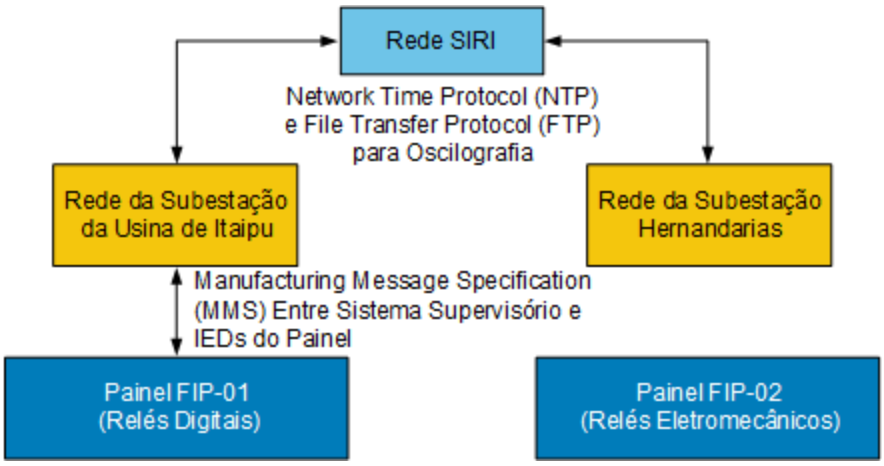

Figura 2 Sistema Inicial de Itaipu

Os engenheiros de Itaipu planejaram modernizar o painel FIP-02 trocando relés eletromecânicos por relés digitais que são compatíveis com a norma IEC 61850 para corresponder aos já usados no painel FIP-01. Eles queriam conectar o painel FIP-02 ao sistema supervisório através da subestação de Hernandarias para que os relés de FIP-02 pudessem enviar os níveis de intercâmbio de energia entre Itaipu e a ANDE para o painel FIP-01 usando mensagens GOOSE

No entanto, não foi permitido nenhuma alteração de configuração no FIP 01, incluindo novas VLANs, já que essas mudanças foram consideradas um alto risco para a grande barragem em serviço. Os requisitos para o novo sistema são mostrados na Figura 3.

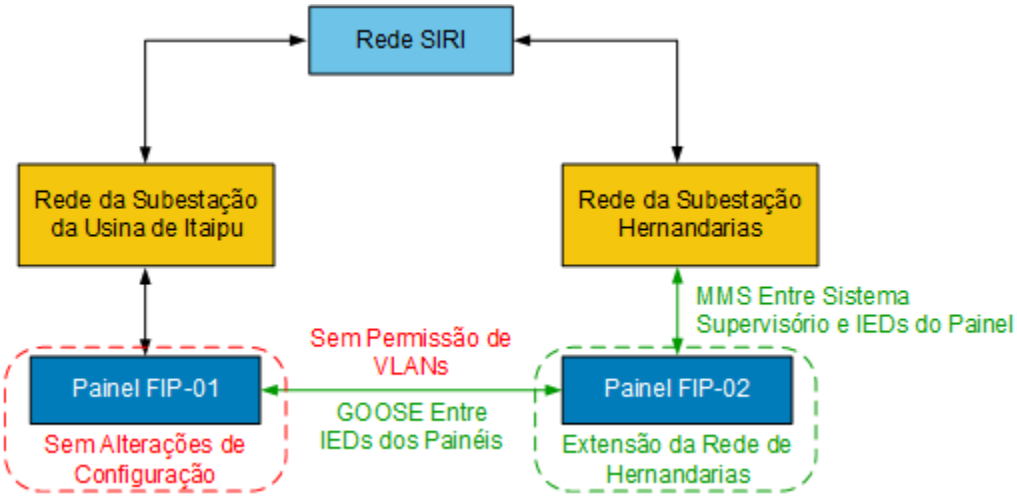

Figura 3 Novos Requisitos do Sistema

Solução possível: Rede RSTP Independente para FIP-02

A integração direta do FIP-02 à rede da subestação de Hernandarias teria tornado o sistema de Itaipu vulnerável a ataques cibernéticos, já que o painel daria acesso à rede da usina. Em vez disso, a primeira opção considerada pelos engenheiros da Itaipu para interconectar as redes FIP-01 e FIP 02 foi criar uma extensão de rede RSTP para FIP-02, semelhante à do FIP-01.

Neste cenário (mostrado na Figura 4), os relés de FIP-02 se comunicariam com o sistema de supervisão usando mensagens MMS, se comunicariam entre si usando mensagens GOOSE e se comunicariam com o FIP-01 usando mensagens GOOSE e ARP.

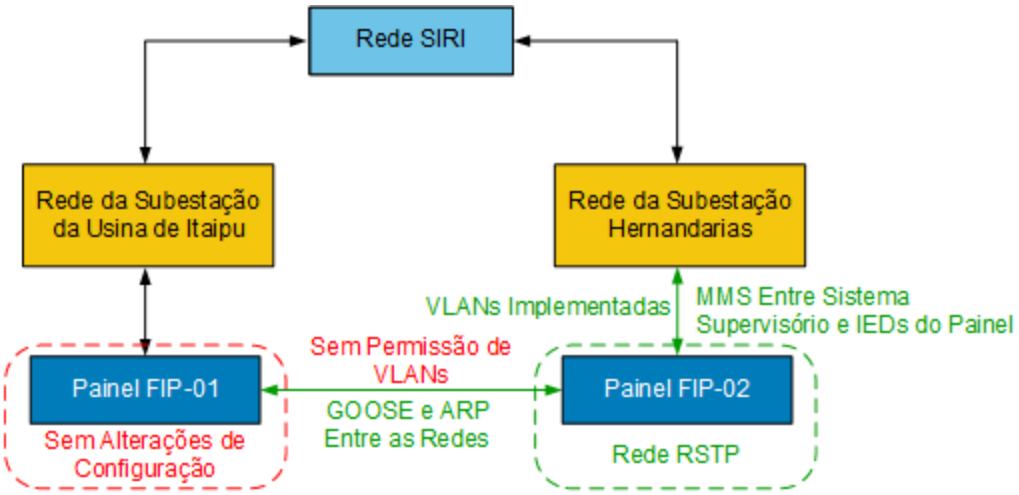

Figura 4 Rede RSTP Independente para o Painel FIP-02

No entanto, esta opção apresentou vários desafios de interconexão de rede devido às limitações das tecnologias de rede convencionais. Como a configuração do FIP-01 não pôde ser alterada, não havia como criar novas VLANs entre FIP-01 e FIP-02 para controlar o tráfego GOOSE e ARP e evitar a formação de loops RSTP por meio do SIRI. Além disso, essa opção aumentaria o risco de perda de pacotes devido aos altos tempos de reconfiguração e *failover* da rede e poderia comprometer a segurança cibernética, pois ambas as redes de subestações seriam acessadas a partir do mesmo ponto (FIP-02).

Além disso, qualquer falha na rede existente causada pela interconexão com a rede FIP-02 poderia comprometer o sistema de proteção da linha de transmissão da usina, que seria uma situação inaceitável.

Melhor Solução: SDN da SEL para FIP-02

Para superar esses desafios, os engenheiros de rede de comunicação decidiram separar a lógica das redes de FIP 01 e FIP 02 sem alterar a operação da rede RSTP do painel FIP-01. Isso foi conseguido usando a tecnologia SDN para conectar as duas redes, sem alterar a lógica da rede existente.

A Figura 5 mostra o projeto do sistema. Os switches SDN na rede do painel FIP-02 interconectam com FIP-01, permitindo que certos pacotes GOOSE sejam roteados entre as redes. A separação lógica das redes impede a difusão de mensagens (inundação) ARP, BPDU e GOOSE entre as redes e previne ainda a formação de loops enviando apenas mensagens GOOSE específicas.

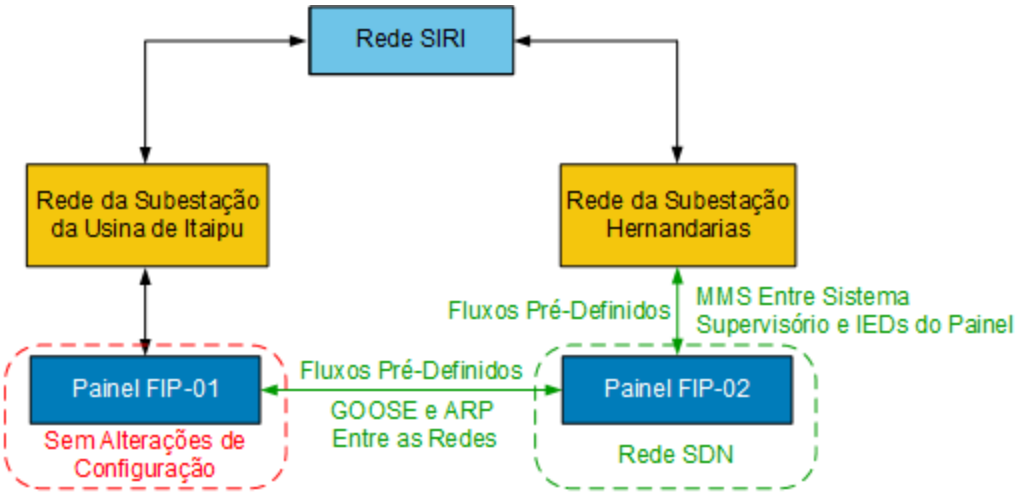

Figura 5 Rede SDN para o Painel FIP-02

Os switches SDN também adicionaram altos níveis de segurança cibernética e possibilitaram baixos tempos de convergência de rede. Embora os tempos de *failover* sejam muito importantes para as mensagens GOOSE, o principal motivo da escolha pela solução SDN por parte de Itaipu foi facilitar o gerenciamento de tráfego para seus sistemas de controle baseados em Ethernet e habilitar a conectividade GOOSE entre redes. Os benefícios de segurança e tempo de recuperação foram bônus. As vantagens da solução SDN são resumidas da seguinte forma:

- Controle sobre tráfego GOOSE e ARP.
- Eliminação de loops.
- Tempos rápidos de recuperação de falhas.
- Redução da complexidade do gerenciamento de tráfego em relação ao RSTP.
- Controle rigoroso das mensagens GOOSE entre FIP-01 e FIP-02.
- Melhor segurança cibernética.

Devido a esses benefícios e à simplicidade da solução SDN, Itaipu está implantando amplamente a SDN, mesmo em novos links onde eles poderiam usar VLANs para mensagens GOOSE.

Engenharia de Rede e Testes

Foi necessária uma intensiva engenharia de redes para configurar os switches SDN no FIP-02. Como os switches SDN usam a segurança *deny-by-default*, os engenheiros de redes precisaram predefinir totalmente os fluxos de comunicação de todas as aplicações do sistema e analisar cuidadosamente os protocolos usados. Além disso, eles pré-definiram caminhos secundários e de backup para prever todos os fluxos e caminhos. Como o volume de dados para a configuração de switches SDN é significativo, os engenheiros precisaram planejar e documentar cuidadosamente a configuração em detalhes.

Os engenheiros de redes também testaram totalmente o sistema SDN na fábrica da SEL usando uma plataforma que reproduzia as condições de campo. Eles testaram sistematicamente cada fluxo de comunicação para garantir que todas as aplicações do sistema funcionassem conforme o esperado. A rede foi testada em condições normais de operação e com falhas simuladas nos switches, na conexão do controlador SDN e nos links de rede. Além disso, o sistema de segurança cibernética foi testado com testes de invasão usando uma ferramenta de varredura de portas.

Esse teste demonstrou que é possível interconectar a rede RSTP do painel FIP-01 com a rede SDN do painel FIP-02 usando o sistema de mensagens GOOSE sem quaisquer modificações na rede existente da subestação da represa de Itaipu.

Conclusão

A interligação entre o painel FIP-01 e o painel FIP-02 está em operação desde dezembro de 2018. Este sistema é a primeira aplicação da tecnologia SDN nos setores elétricos brasileiro e paraguaio.

A tecnologia SDN possibilitou interconectar duas redes IEC 61850 baseadas em Ethernet sem reconfigurar os switches existentes e simultaneamente forneceu ao sistema altos níveis de segurança cibernética e baixos tempos de recuperação de falhas de rede.

Referências

[1] P. Garcia, E. M. Nyznyk, M. A. Yamamoto, M. Cabral, M. Silveira, J. Chiaradia, B. M. Fontes, H. Larangeira, A. Insfrán, and D. F. Amarilla, “Application of SDN Technology in the Modernization of Part of the Schemes of Emergency Control of the 50 Hz Sector of Itaipu Binacional,” proceedings of the 14th Technical Seminar on Protection and Control, Paraná, Brazil, October 2018.

[2] P. Robertson, “Software-Defined Networking Changes the Paradigm for Mission-Critical Operational Technology Networks,” January 2017. Available: selinc.com.

[3] R. Hill and R. Smith, “Purpose-Engineered, Active-Defense Cybersecurity for Industrial Control Systems,” August 2017. Available: selinc.com.

[4] R. Meine, “A Practical Guide to Designing and Deploying OT SDN Networks,” proceedings of the Power and Energy Automation Conference, Spokane, WA, March 2019.

[5] C. Gray, “How SDN Can Improve Cybersecurity in OT Networks,” proceedings of the 22nd Conference of the Electric Power Supply Industry, Kuala Lumpur, Malaysia, September 2018.

[6] M. Hadley, D. Nicol, and R. Smith, “Software-Defined Networking Redefines Performance for Ethernet Control Systems,” proceedings of the Power and Energy Automation Conference, Spokane, WA, March 2017.

[7] Q. Yang and R. Smith, “Improve Protection Communications Network Reliability Through Software-Defined Process Bus,” proceedings of the Power and Energy Automation Conference, Spokane, WA, March 2019.

[8] D. J. Dolezilek, “Using Software-Defined Network Technology to Precisely and Reliably Transport Process Bus Ethernet Messages,” proceedings of the 14th International Conference on Developments in Power System Protection, Belfast, United Kingdom, March 2018.

[9] N. Feamster, J. Rexford, and E. Zegura, “The Road to SDN: An Intellectual History of Programmable Networks,” *ACM SIGCOMM Computer Communication Review*, Vol. 44, Issue 2, April 2014, pp. 87–98.

[10] Itaipu Binacional, “Itaipu Had Its Best Year in 2016, With the Production of 103.1 Million MWh.” Available: www.itaipu.gov.br/en/press-office/video/world-record-2016.

[11] Z. Xin, “Three Gorges Project Reaches 1 Trillion kWh Milestone,” *China Daily*, March 2017. Available: www.chinadaily.com.cn/business/2017-03/01/content_28396395.htm.

Biografias

Marcos Cabral recebeu o grau de bacharel em engenharia elétrica pela Universidade Estadual de Campinas (UNICAMP) em 2008. Ele começou a trabalhar na General Electric como engenheiro de automação em 2008 e trabalha na Schweitzer Engineering Laboratories, Inc. (SEL) desde 2010. Ele é responsável por treinamento e suporte a clientes, configuração, teste em fábrica e comissionamento. Depois de dez anos de experiência com automação de sistemas elétricos, Marcos é agora um líder técnico na SEL trabalhando em projetos como sistemas especiais de proteção, esquemas de emergência e redes definidas por software. Marcos completou um curso de especialização em sistemas de automação de subestações no Instituto Nacional de Telecomunicações (INATEL) em 2014.

Mauricio Silveira é engenheiro eletricista e recebeu seu bacharelado pela Universidade Estadual de São Paulo em 2013. Desde 2014, ele trabalha na Schweitzer Engineering Laboratories, Inc. (SEL), onde ocupou cargos em serviços de engenharia e vendas e atendimento a clientes, trabalhando em comissionamento, testes em fábrica e suporte a clientes. Atualmente é engenheiro de integração e automação em P&D. Seu trabalho inclui o desenvolvimento e teste de protocolos para aplicações críticas, projeto de redes, avaliação de segurança cibernética e testes de relés digitais.

Ryan Urie recebeu o grau de bacharel em artes pelo Colégio de Idaho em 2004 e mestrado em ciências em planejamento bioregional pela Universidade de Idaho em 2010. Ele ingressou na Schweitzer Engineering Laboratories, Inc. (SEL) em 2013 como editor técnico. Além de editar vários artigos técnicos, guias de aplicação e apresentações, ele é autor de diversos artigos e estudos de caso.