As Redes Definidas por Software Atendem aos Requisitos do Sistema de Controle

Rakesh Bobba, *University of Illinois at Urbana-Champaign*
Donald R. Borries, Rod Hilburn e Joyce Sanders, *Ameren Illinois*
Mark Hadley, *Pacific Northwest National Laboratory*
Rhett Smith, *Schweitzer Engineering Laboratories, Inc.*

***Sumário*—As redes representam uma função central, geralmente essencial, nas infraestruturas críticas atuais. Infelizmente, a maioria das tecnologias relacionadas às redes existentes é otimizada para produtos da tecnologia de informação corporativa ou residencial e não necessariamente para infraestruturas críticas que exigem diferentes casos de uso e focam em diferentes prioridades. Especificamente, a infraestrutura crítica requer garantias de confiabilidade, segurança *deny-by-default* e latência, além de capacidades de transporte determinísticas. A tecnologia Ethernet tradicional é inadequada para as comunicações das proteções de sistemas de potência em tempo real. Uma abordagem completamente nova pode ser a melhor maneira de resolver estas lacunas. Por outro lado, a tecnologia existente também oferece inúmeras oportunidades de interoperabilidade que não queremos perder. Precisamos, portanto, de um caminho para conciliar estas questões.**

Este artigo discute o uso de redes definidas por software (SDN: "Software-Defined Network"), uma nova arquitetura na tecnologia de redes, visando preencher a lacuna entre a interoperabilidade e os requisitos de transporte das comunicações de alta confiabilidade para o sistema de potência. Apresentamos uma visão geral da SDN e os benefícios do uso desta tecnologia, abordando quais desafios precisam ser entendidos antes que este método possa ser adotado pelo setor de energia.

Um projeto patrocinado pelo Departamento de Energia dos Estados Unidos (DOE: "Departamento of Energy"), denominado Projeto SDN, foi iniciado em outubro de 2013 para projetar, desenvolver e testar um controlador de fluxo baseado em SDN para o setor de energia. O objetivo do Projeto SDN, construído no topo do Projeto Watchdog também patrocinado pelo DOE, consiste em validar se uma SDN pode ajudar a tornar o setor de energia mais confiável, econômico e seguro.

I. Introdução

O ambiente de rede nasceu da necessidade de manipular computadores com múltiplos propósitos executando várias funções através de uma única conexão física de comunicação. Isso habilitou um ambiente de negócios multitarefa e dinâmico com mudanças consistentes, acelerando a conclusão dos trabalhos em níveis nunca antes vistos. Em total contraste, os sistemas de controle do setor de energia consistiam em dispositivos mecânicos especificamente projetados ou dispositivos incorporados que foram construídos com finalidades específicas, a maior parte dos quais tendo apenas uma função para ser executada. Hoje, esses mesmos sistemas de controle são construídos com dispositivos multifunção incorporados com demandas similares àquelas de redes corporativas, mas com diferentes prioridades e desempenhos. Logo, a pergunta óbvia é: a tecnologia de redes corporativas pode ser usada na infraestrutura do sistema de controle? A resposta é não, caso não haja um projeto cuidadoso com limitações bem conhecidas. Os profissionais da indústria de energia estão exigindo uma infraestrutura de tecnologia de rede mais escalável, confiável e fácil de usar. A maioria dos objetivos da engenharia de rede é a mesma, ou seja, evitar o buraco negro, atenuação do loop, velocidades de convergência rápidas, controle de prioridades e suporte para múltiplos serviços, todos operando através de um único canal físico de comunicação. No entanto, isto ainda deixa lacunas nas capacidades exigidas pelos engenheiros projetistas desta infraestrutura crítica, as quais não são atendidas pelas tecnologias de redes corporativas. Os exemplos destas lacunas incluem: caminhos de entrega pré-configurados nos modos primário e *failover* fim-a-fim ("end-to-end"); latência calculada e repetível resultando em um determinismo gerenciado; e capacidade de monitoramento e visualização detalhada de todo o sistema, bem como a segurança "deny-by- default" ("negar por default") em todas as camadas do sistema de comunicação.

Na busca de respostas para abordagem destas lacunas, a equipe do Projeto SDN pesquisou uma nova arquitetura de rede em desenvolvimento denominada Rede Definida por Software (SDN: "Software-Defined Network"). Baseando-se nesta pesquisa, acreditamos que a arquitetura SDN nos permita manter as partes da atual tecnologia de rede que funcionam na infraestrutura crítica e abandonar as partes que não são efetivas, substituindo-as por soluções projetadas para atender às nossas demandas de comunicação.

Este artigo visa destacar as vantagens trazidas pela SDN para melhoria da confiabilidade e segurança cibernética das redes de sistemas de controle. A SDN permite aos proprietários do sistema projetar e manter a rede em termos de fluxos, que são os atributos lógicos que compõem a sessão de comunicação associada a aplicativos específicos. Por exemplo, o DNP3/IP tem uma sessão TCP/IP entre um relé de proteção

e o sistema de controle supervisivo e aquisição de dados (SCADA) master. Os pacotes que trafegam entre o relé e o master criam um fluxo. Para cada fluxo, a SDN fornece caminhos de envio estritamente definidos, melhor escalabilidade e controle de alterações, melhorando ao mesmo tempo a percepção situacional e disponibilizando capacidades de monitoramento próximas do tempo real para os operadores. A SDN também permite um modelo de segurança cibernética *deny-by-default*. Combinados, esses recursos tornam a SDN uma escolha atrativa para ser usada na infraestrutura de sistemas de controle.

Em 2011, o Departamento de Energia dos Estados Unidos (DOE) publicou o Roteiro para Obtenção de Segurança Cibernética nos Sistema de Distribuição de Energia ("Roadmap to Achieve Energy Delivery Systems Cybersecurity") [1]. Este documento fornece uma estratégia para lidar com as necessidades de segurança cibernética no setor de energia, contendo a seguinte visão: "Até 2020, sistemas de distribuição de energia resilientes serão projetados, instalados, operados e mantidos para sobreviver a um incidente cibernético e manter ao mesmo tempo as funções críticas" [1]. O Projeto SDN aborda duas áreas como metas dentro do roteiro. Em primeiro lugar, as arquiteturas do sistema de distribuição de energia de próxima geração fornecem "defesa em profundidade" e utilizam componentes que são interoperáveis, extensíveis e capazes de continuar operando em condições degradadas durante um incidente cibernético. Em segundo lugar, a colaboração entre as áreas industriais, acadêmicas e governamentais permite manter os avanços da segurança cibernética.

II. Definição da SDN

A SDN é uma nova abordagem para gestão, configuração e operação dos sistemas de redes. Esta mudança arquitetônica está revolucionando o gerenciamento de redes corporativas de larga escala, infraestruturas baseadas na nuvem e redes de data centers, visando fornecer melhor suporte para mudanças dinâmicas necessárias várias vezes ao dia. Além disso, a SDN tem sido amplamente adotada no mundo corporativo porque acreditamos que sua implantação possa ter um impacto significativo na gestão das redes de sistemas de controle. A SDN suporta uma plataforma de controle de alterações através de programação, a qual permite que a rede inteira seja gerenciada como um único ativo, simplifica o entendimento da rede e possibilita o monitoramento contínuo com mais detalhes. As redes de sistemas de controle são frequentemente mais estáticas, enquanto o ambiente corporativo é mais dinâmico. Em outras palavras, os fluxos do sistema de controle são mais consistentes e contínuos do que a natureza sempre em mudança de um instantâneo ("snapshot") do fluxo da rede corporativa. Isto é devido principalmente ao fato de o sistema de controle ser baseado em comunicações máquina a máquina, enquanto as comunicações corporativas são principalmente homem-máquina. Logo, a arquitetura SDN será aplicada de forma diferente. No entanto, a boa notícia é que a arquitetura SDN é capaz de otimizar ambas as situações. A mudança fundamental na tecnologia de redes trazida pela SDN consiste no desacoplamento dos sistemas que decidem para onde o tráfego é enviado (isto é, o plano de controle) a partir dos sistemas que executam o encaminhamento do tráfego na rede (isto é, o plano de dados).

O processo de implantação de uma rede tradicional começa com o projeto da topologia, configuração dos vários dispositivos de rede e, finalmente, definição dos serviços de rede necessários. Para possibilitar a utilização ideal dos recursos da rede, os dados dos aplicativos têm que fluir na direção das rotas determinadas pelos protocolos de roteamento e comutação ("switching"). Em redes de grande porte, a tentativa de compatibilizar o caminho descoberto na rede com um caminho de dados desejado do aplicativo pode envolver alterações nas configurações de centenas de dispositivos com diversas características e parâmetros de configuração. Além disso, os administradores de rede frequentemente precisam reconfigurar a rede para evitar loops, ganhar velocidade de convergência de rotas e priorizar uma determinada classe de aplicativos.

Esta complexidade no gerenciamento resulta do fato de que cada dispositivo de rede (ex., um switch ou roteador) possui a lógica de controle e a lógica de encaminhamento de dados integradas juntas. Por exemplo, em um roteador de rede, protocolos de roteamento como RIP ("Routing Information Protocol") ou OSPF ("Open Shortest Path First") constituem a lógica de controle que determina como um pacote deve ser encaminhado. Os caminhos determinados pelo protocolo de roteamento são codificados em tabelas de roteamento, que são então utilizadas para encaminhar os pacotes. De forma similar, em um dispositivo da Camada 2, tal como uma ponte ("bridge") de rede (ou switch de rede), parâmetros de configuração e/ou algoritmo STA ("Spanning Tree Algorithm") constituem a lógica de controle que determina o caminho dos pacotes. Dessa forma, o plano de controle de uma rede tradicional é distribuído na estrutura de *switching* (dispositivos de rede); em consequência, alterar o comportamento de encaminhamento de uma rede envolve mudanças nas configurações de muitos (potencialmente todos) dispositivos de rede.

SDN é uma nova arquitetura na tecnologia de redes que simplifica o gerenciamento da rede através da abstração do plano de controle do plano de encaminhamento de dados. A Fig. 1 ilustra os blocos de construção da SDN, os quais são discutidos nas subseções seguintes.

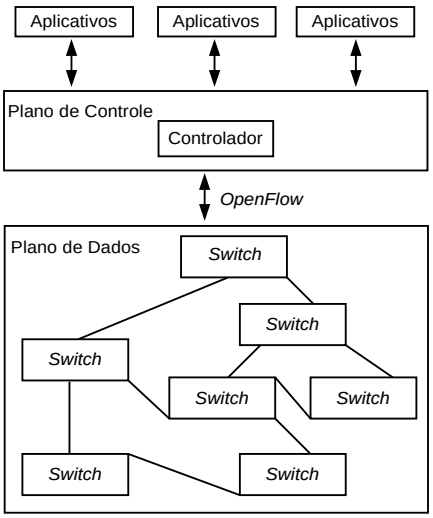

Fig. 1. Visão Geral da Arquitetura da SDN

A. Plano de Controle

No coração da SDN, há um controlador que incorpora o plano de controle. Especificamente, o software do controlador determina como os pacotes (ou *frames*) devem fluir (ou serem encaminhados) na rede. O controlador transmite essas informações para os dispositivos de rede, que constituem o plano de dados, definindo suas tabelas de encaminhamento. Isso habilita a configuração e a gestão centralizadas da rede. Muitos controladores de código aberto, tais como *Floodlight* (http:www.projectfloodlight.org/floodlight/), *NOX* (http:www.noxrepo.org) e *Ryu* (http://osrg.github.io/ryu/), para citar alguns, estão agora prontamente disponíveis.

B. Plano de Dados

O plano de dados consiste em dispositivos de rede que substituem os switches e roteadores. Na SDN, estes componentes são dispositivos muito simples para encaminhamento de pacotes Ethernet através de uma interface de comunicação com o controlador que recebe as informações de encaminhamento. Muitos fornecedores atuais oferecem dispositivos de encaminhamento de pacotes habilitados para SDN.

C. Interface do Plano de Controle e Plano de Dados

A SDN requer uma interface de comunicação entre os dispositivos de rede e o controlador, como é evidente a partir da descrição dos planos de controle e dados. Uma interface padronizada entre eles permitirá a um controlador interoperar com diferentes tipos de dispositivos de rede e vice-versa. O protocolo OpenFlow é uma dessas interfaces padronizadas que é gerenciada pela ONF ("Open Networking Foundation"), tendo sido adotada pelos principais fornecedores de switches e roteadores. No entanto, deve-se observar que o OpenFlow é apenas um bloco componente da arquitetura SDN e que há normas abertas da IETF ("Internet Engineering Task Force") ou padrões específicos de fornecedores que já estão disponíveis ou estão sendo desenvolvidas.

D. Serviços da SDN

Na arquitetura SDN, o controlador pode conter uma interface de programação de aplicativos (API: "Application Programming Interface") que os serviços podem usar para configurar a rede. Neste cenário, o controlador pode atuar apenas como uma interface para a estrutura de *switching*, enquanto a lógica de controle reside nos serviços que estão usando o controlador. Dependendo do controlador usado na SDN, as interfaces podem ser diferentes. Os controladores e suas interfaces de aplicativos podem ser adaptados para atender às necessidades no domínio do aplicativo. Um controlador que é projetado e otimizado para data centers, por exemplo, pode não ser adequado para redes de controle no setor elétrico e vice-versa. O domínio de um aplicativo específico para a indústria onde é usado determinará os requisitos do sistema global. As compensações ("trade-offs") entre otimizações como velocidade de instrução única ou processamento paralelo determinam as melhores interfaces a serem usadas.

Embora a SDN seja normalmente usada para monitoramento e alterações programáticas nas configurações de rede, sua natureza centralizada é também bastante adequada para atender aos requisitos de segurança, desempenho e operação das redes de sistemas de controle. As redes dos sistemas de controle são projetadas para efetuar trabalhos específicos por muitos anos com o mínimo de alteração possível. Com a ajuda da SDN, os operadores podem obter vantagens deste conhecimento para pré-configurar os caminhos da rede e efetivamente criar circuitos virtuais em uma rede de comutação de pacotes. As empresas de energia podem projetar os circuitos virtuais necessários para a comunicação entre certos dispositivos e restringir ("lock down") o caminho das comunicações. Este tipo de abordagem pode melhorar a segurança, reduzindo a superfície de ataques e fornecendo padrões de referências ("baseline") claras e aprovadas que podem ser continuamente monitoradas para garantir que nunca sejam alteradas.

III. Desafios Não Atendidos pela Atual Tecnologia da Informação de Redes Corporativas Tradicionais

Esta seção analisa as lacunas no atendimento às demandas da rede de sistemas de controle pela atual tecnologia de redes corporativas. Existem cinco categorias principais nas quais podemos organizar as lacunas da rede.

A primeira delas se refere às etapas de planejamento, concepção e testes de novos projetos. Os sistemas de controle que compõem nossa infraestrutura de energia crítica são sistemas desenvolvidos para atender a propósitos específicos, exigindo altos níveis de confiabilidade e operação contínua. Estes sistemas dependem da rede para efetuar a comunicação entre dispositivos de monitoramento e controle, bem como entre os operadores e dispositivos de controle. Todas essas ações são pré-concebidas e precisam seguir rigorosamente o programa de ação. As redes que transportam essas mensagens

críticas precisam ser compatíveis com o modelo de alta confiabilidade baseado na execução de um plano de ação pré-concebido. Os projetistas têm que desenvolver cada circuito de comunicação e circuito redundante (“failover”), demonstrar a confiabilidade através de princípios de engenharia profissionais, e efetuar testes metodicamente para certificar-se que o sistema vai executar todas as ações desejadas antes de ser colocado em operação.

A segunda categoria lida com o controle de alterações e escalabilidade da rede após ter sido implantada e comissionada. Para os sistemas de controle do setor de energia, é desejável minimizar a quantidade de mudanças necessárias para manter o sistema operacional. Quando mudanças forem necessárias, é preciso que haja uma maneira programática para efetuar essas alterações em todo o sistema, num instante desejado, causando o menor impacto possível no sistema como um todo.

A terceira categoria aborda a engenharia dos circuitos de comunicação e o desempenho exigido, bem como as ferramentas para monitorar e proteger este desempenho. O objetivo é projetar o caminho de envio completo da maneira que desenvolvemos os circuitos de distribuição de energia e respectivos circuitos redundantes, garantindo que não haja sobrecarga de qualquer segmento do circuito. A pré-concepção dos circuitos de encaminhamento para todas as comunicações também pressupõe que o caminho de envio tenha a mesma latência, fornecendo uma referência para cálculo dos parâmetros determinísticos das mensagens e confirmação de que elas foram recebidas pelo sistema. Uma rede tradicional sobre uma infraestrutura de pacotes comutados baseia-se na abordagem de mais tentativas dos aplicativos e maior largura de banda, tornando os serviços de entrega *best-effort* suficientemente adequados. Esta abordagem de nuvem desconhecida não é aceitável para uma infraestrutura crítica. Há também um desejo de maximizar a utilização dos ativos da rede, eliminando o bloqueio ou outras tecnologias de degradação.

A quarta categoria inclui a visualização e supervisão contínua de toda a rede para monitoramento e gestão operacional. Os operadores de sistemas de controle precisam monitorar e responder às condições da rede assim como é feito para as condições do sistema de potência. Para isso, eles precisam entender os fluxos do sistema e o desempenho esperado, ser alertados quando houver mudança nestes comportamentos, e ter as ferramentas e treinamentos necessários para saber o que fazer para colocar o sistema de volta nas condições normais de operação.

A quinta categoria crítica é a segurança cibernética da rede. As redes dos sistemas de controle são redes controladas remotamente, muitas vezes instaladas em lugares difíceis de serem acessados fisicamente. Os engenheiros que projetam e implantam estes sistemas querem ter capacidade de aprovar todos os serviços em execução na rede e negar todos os outros fluxos por default. Qualquer novo fluxo de comunicação deve ser aprovado antes de ter sua conexão autorizada.

IV. Início, Desenvolvimento, Implantação e Testes do Projeto

Um projeto de rede com sucesso é muito mais do que apenas a tecnologia, mas inclui a interação entre a tecnologia e os operadores e engenheiros responsáveis pelo cuidado e manutenção do sistema. Logo, vale a pena verificar como estes processos são integrados à arquitetura da tecnologia SDN. Inicialmente, é determinada a necessidade de uma nova rede para um segmento de negócio particular. Em seguida, um *business case* é desenvolvido, incluindo uma estimativa de orçamento preliminar que fornece à liderança do projeto a capacidade de aprovar o financiamento para a iniciativa.

Uma vez que a aprovação preliminar do financiamento tenha sido recebida, um engenheiro de projetos ou gerente de projetos é designado para o projeto, o qual desenvolve um escopo do projeto, incluindo os recursos necessários (fabricantes de equipamentos originais, um engenheiro de rede, serviços telefônicos, uma equipe para o servidor, e assim por diante) para sua execução com sucesso.

Assim que os recursos necessários tenham sido identificados, a equipe responsável se reúne para desenvolver um conjunto de requisitos necessários para implementação do projeto, apresentando um projeto inicial de alto nível com uma visão geral dos componentes necessários para criar um projeto eficaz. Em seguida, uma avaliação ambiental (incluindo possíveis visitas ao local) é efetuada para determinar se uma infraestrutura adequada está disponível para suportar o escopo do projeto. Uma vez que o projeto de alto nível e as avaliações ambientais estejam concluídas, uma avaliação mais detalhada dos custos é realizada para garantir que o dinheiro do orçamento seja suficiente e esteja disponível para dar continuidade ao projeto. O projeto de alto nível, incluindo a avaliação de custos mais detalhada, é submetido à liderança para efeito de aprovação.

Após o projeto ter recebido a aprovação final, a equipe responsável começa a atividade de detalhamento, incluindo a identificação das exigências de cada segmento para execução do projeto. Isto envolve não apenas os equipamentos e sistemas necessários que serão incorporados ao projeto, mas também a determinação dos recursos de mão de obra (interna, externa e uma solução híbrida) de cada segmento. O aspecto final do processo de detalhamento do projeto inclui o desenvolvimento de planos sobre como implantar e manter a solução do projeto proposto, ou seja, o desenvolvimento de um cronograma de construção e plano de testes, abordando os seguintes itens:

- Desenvolver planos de implementação e restauração (“backout”). Com a SDN, os proprietários da tecnologia podem acessar mais facilmente o hardware de implantação através da configuração central do controlador ao invés de arquivos de configuração ou ajustes complexos em cada dispositivo de campo.
- Efetuar uma avaliação de prontidão operacional. A SDN fornece as medidas de avaliação necessárias para

fazer uma análise completa visando validar se todos os circuitos estão prontos para a nova carga de comunicação.
- Executar um plano de gestão de mudanças. A SDN pode rastrear programaticamente ordens de alteração para os indivíduos e integralmente através do controle de acesso do usuário e conjunto de alterações dos fluxos da rede.
- Receber a aprovação final para prosseguir com a execução do projeto.
- Iniciar a operação e fornecer suporte de implementação. Os proprietários da tecnologia podem monitorar o status da implantação on-line e efetuar alterações no comissionamento centralmente, eliminando a carga de trabalho das equipes de campo.
- Verificar a integridade da produção. A SDN pode coletar as medidas de avaliação de desempenho e os diagnósticos da rede centralmente em tempo quase real para que os operadores possam validar a integridade do sistema.
- Conduzir uma análise pós-implementação para garantir que os requisitos do negócio estejam sendo atendidos.
- Utilizar ferramentas de monitoramento; realizar manutenção trimestral conforme necessário. A SDN fornece recursos de monitoramento contínuo, e a manutenção pode acontecer conforme a necessidade, ao invés de ter que esperar pela emissão das ordens de trabalho trimestrais.

A SDN deve melhorar os processos e recursos de uma nova solução de rede, fornecendo os seguintes itens:

- Maior facilidade no processo de verificação e análise para garantir que configurações corretas foram implantadas nos novos dispositivos usando o controlador para monitorar todos os fluxos de comunicação e diagnósticos dos circuitos.
- Redução dos tempos de recuperação de falha do link através dos caminhos de entrega pré-configurados nos modos primário e *failover* para cada comunicação.
- Maior facilidade na configuração de redes devido à abstração de *overhead* baseada no sistema de marcação (“tagging”) da rede. A configuração é feita através dos caminhos de fluxos ao invés de redes locais virtuais (VLANs: “Virtual Local-Area Networks”), listas de controle de acesso, filtros MAC (“Media Access Control”), ou tabelas de roteamento.
- Melhor visualização do sistema como um todo porque há um ponto de coleta central que é visível para todos os dispositivos de rede.
- Configuração de uma rede de referência (“baseline”) para verificar a configuração correta da rede. A SDN tem um ponto central no controlador onde residem todos os caminhos de envio de cada comunicação, e a rede global é gerenciada como um único ativo.
- Centro de operação centralizada com visibilidade de todas as redes (LAN corporativa, LAN da subestação, despacho da distribuição, e assim por diante) para uma gestão mais efetiva dessas redes.

V. Os Benefícios da SDN Permitem que as Redes dos Sistemas de Controle Abordem as Lacunas Identificadas

Cada novo circuito de transmissão e distribuição de energia instalado em qualquer sistema de potência requer muito cuidado e planejamento. De forma similar, os circuitos de comunicação têm que ser projetados para transportar mensagens para os destinos pretendidos dentro da janela de tempo esperada e da forma mais confiável possível. Desde o início, a maior vantagem percebida na tecnologia SDN pela equipe do projeto foi a capacidade de projetar todos os fluxos de tráfego num nível circuito-por-circuito, impondo o exato caminho de envio para o tráfego de uma mensagem desde a fonte até o destino. Ao contrário dos requisitos dinâmicos de data centers que impulsionam a revolução da SDN, a indústria de sistemas de controle se beneficia enormemente de sua configuração baseada em circuitos com segurança *deny-by-default*, a qual pode ter sua operação restrita (“locked down”) a uma topologia muito estática. Combinada com esta funcionalidade de evaporação da nuvem (“cloud evaporating”), revelar os caminhos exatos de envio da mensagem baseado em circuitos representa a forma de operação mais avançada para monitoramento e identificação visual do que está acontecendo na rede em tempo muito mais real do que ocorria anteriormente.

Atualmente, a concepção de redes SDN é baseada em princípios simples de projetos de circuitos orientados fisicamente. Isso habilita os engenheiros de sistemas de potência a executar o que costumavam fazer para linhas de transmissão com linhas de comunicação e projetar o caminho específico através do qual eles querem que os elétrons fluam. A engenharia de tráfego permite que o proprietário da rede tenha maior controle sobre como a rede opera, maximizando assim os recursos dos ativos da rede. Não há mais necessidade de protocolos de negociação dinâmica designando ou bloqueando caminhos de envio, mas todas as portas físicas podem ser usadas para o encaminhamento de pacotes. Isso ajuda a balancear os serviços de segregação e largura de banda, maximizando o potencial dos ativos da rede.

As redes de sistemas de controle são implantadas em locais controlados remotamente visando reduzir ao mínimo a necessidade de visitas ao local. Outra razão importante para o grande potencial da SDN no setor de energia é a redução da gestão de *patches* nos dispositivos de rede. Um dos motivos para liberação das ordens de trabalho é a atualização (“patch” ou “update”) dos equipamentos de campo baseados na eletrônica de potência. Quanto menos manutenção de *patches* for necessária, maior será a economia para o proprietário do sistema de potência. A arquitetura SDN reduz a quantidade de

códigos requerida pelos dispositivos de rede do campo porque não é mais necessário gerenciar os recursos do plano de controle e serviço de descoberta de rotas de envio. Esses códigos, por sua vez, residem no controlador de fluxo e não no dispositivo de rede do campo. Em teoria, a arquitetura SDN reduz a quantidade necessária de gestão de *patches* no campo. Simplificando, um número menor de códigos implantados requer menor gestão de *patches*, tornando o sistema mais confiável.

O controle de mudanças na rede é difícil de ser gerenciado quando protocolos dinâmicos como RSTP ("Rapid Spanning Tree Protocol") controlam as decisões de encaminhamento da rede baseando-se em topologias físicas ou lógicas e não em serviços que estão sendo executados nos circuitos. Em contraste, a SDN permite que as decisões de encaminhamento sejam baseadas nos aplicativos que requerem comunicações e não na topologia. Os circuitos de encaminhamento são independentes da topologia, significando que não importa como os switches estejam conectados, a configuração do caminho de envio será selecionada e definida de acordo com os atributos de transporte desejados. Quanto mais conexões houver entre switches, mais opções existem para os caminhos de aplicação; não deverá mais haver quaisquer portas vazias. A engenharia do circuito redundante ("failover") específico é tão difícil quanto a tecnologia RSTP tradicional. A SDN habilita o engenheiro a selecionar o circuito de encaminhamento primário e projetar N – 1 circuitos *failover* para falhas de um link ou switch. Isto permite então que o engenheiro confie no projeto e confirme se o projeto está lidando com os casos de falha planejados através de procedimentos de teste mais simples. Este *failover* deverá ser mais rápido na SDN devido à eliminação dos tempos de reconvergência e descoberta da topologia de rede exigida pelo RSTP em todas as falhas de um link ou switch.

Efetuar alterações na configuração da rede ao escalar para sistemas maiores, ou reduzir em tamanho ("downsizing"), pode ser entediante porque um engenheiro de rede precisa levar em consideração cada dispositivo de rede que pode ser afetado pela mudança. Tradicionalmente, isto tem sido feito por meio de pacotes caros de software de automação ou scripts caseiros que fazem interface com a linha de comando de cada dispositivo de rede. Com a abstração do plano de controle para um local central, as mudanças na rede consistem em alterações mais simples efetuadas através de programação; estas alterações são inseridas no controlador de fluxo que, por sua vez, atualiza todas as tabelas de encaminhamento em cada dispositivo de rede. Isso se baseia no princípio de que o controlador já entende as associações entre os dispositivos de rede e vai capturar todos os dispositivos afetados, atualizando-os adequadamente para suportar a nova mudança. Estas alterações podem ser testadas antes do tempo, introduzidas, confirmadas e programadas para serem aplicadas em todo o sistema, havendo pouca preocupação sobre a ordem na qual as mudanças de configuração são aplicadas.

Uma enorme vantagem percebida pela equipe com o melhor controle de alterações da SDN consiste na capacidade de controle que os proprietários do sistema têm durante a ocorrência de mudanças. Não haverá mais interrupções da rede cada vez que um cabo for conectado ou desconectado (por exemplo, quando um técnico conectar acidentalmente um cabo a uma porta não utilizada entre switches); as interrupções só acontecerão quando as alterações de configuração forem submetidas ao controlador de fluxo. As portas não utilizadas são desativadas porque a rede não está programada para enviar quaisquer pacotes da porta e quaisquer novas tentativas de comunicação que aparecerem naquela porta têm que ser permitidas pelo controlador de fluxo ou pré-programadas para a porta. O RSTP vai interromper a rede toda vez que a topologia for alterada (cabos conectados ou desconectados), impactando todo o sistema. Com a SDN, somente serão impactados os circuitos nos quais houver falha do link ou alterações. Com o RSTP atual, negociação e descoberta acontecem quando ocorrem falhas ou alterações em determinadas portas; isto é denominado processo de convergência. Durante o tempo em que esta convergência estiver acontecendo, pode haver interrupções de comunicação em outros circuitos, não apenas no circuito em que a alteração foi efetuada. Isso melhora a confiabilidade do sistema de entrega de mensagens global.

Nos sistemas de potência, é fundamental compreender o estado do sistema em tempo real ou tempo quase real. Isto é normalmente feito através do SCADA ou de outras medições de estado como os sincrofasores. Estes dispositivos medem o estado do fluxo de potência através do sistema. A infraestrutura de comunicação entre todos os ativos do sistema de potência é muito importante para efetuar o monitoramento e controle dos mesmos, visando manter o sistema estável e saudável. Hoje, isso é muito difícil devido à arquitetura do plano de controle distribuído. Cada ativo de rede individual tem sua própria visão do ambiente e das conexões de redes adjacentes. A tentativa de reunir todas essas pequenas janelas para fornecer o estado do sistema global é um desafio.

Existem soluções centradas no fornecedor para configuração e monitoramento dos switches de rede de toda a empresa. Um exemplo é o produto Cisco® Network Assistant. Estas ferramentas atendem parcialmente às necessidades do administrador de rede para visualizar e configurar os equipamentos de rede. Dependendo das capacidades do software e dos switches de rede que estão sendo gerenciados, um administrador pode projetar uma topologia de rede, monitorar a utilização de recursos, habilitar ou desabilitar portas de switches, ativar uma configuração salva para um switch, ativar uma atualização de firmware, ou fazer o backup da configuração de um switch. Embora todos esses recursos pareçam ótimos, eles não contêm um conjunto completo de funções. Por exemplo, o software do fabricante opera tipicamente apenas com equipamentos de switch de rede do mesmo fornecedor. Outra deficiência é a necessidade de configurar individualmente os switches; não há nenhuma

configuração padrão para todos os switches. Com a SDN, as diferenças entre fornecedores são unificadas sob o conjunto de regras da tabela de encaminhamento regidas pelo protocolo de comunicação entre o dispositivo de rede e o controlador de fluxo. Por exemplo, se múltiplos fornecedores suportarem o protocolo OpenFlow 1.3, os vários produtos dos fornecedores podem ser todos programados pelo mesmo controlador. O operador que estiver inserindo as configurações da rede não precisa saber se os dispositivos de rede do campo são todos do mesmo fornecedor ou de vários fornecedores. Isso melhora a segurança da cadeia de fornecimento e permite aos proprietários do sistema usarem sempre a melhor tecnologia de hardware no momento da compra.

Usando a SDN, há um único ponto de controle para o encaminhamento através de todos os dispositivos de rede; dessa forma, os proprietários do sistema têm uma visão global de toda a rede, podendo monitorá-la como um único ativo. Esta vantagem de visualização disponibiliza cenários de operação de todo o sistema, fornecendo informações sobre quais comunicações são permitidas, onde elas estão sendo efetuadas, e qual o caminho usado para chegar ao destino. Isso abstrai a natureza complexa das redes interconectadas, fornecendo um método para estruturação e manutenção da ordem. A SDN também fornece diversos recursos avançados de monitoramento e solução de problemas que eram difíceis ou impossíveis de serem resolvidos com as redes tradicionais. Estas características avançadas incluem o seguinte:

- Espelhamento (“mirroring”) de qualquer fluxo selecionado ao invés da porta toda.
- Emissão de alarme sobre a largura de banda quando estiver perto da saturação.
- Fornece várias medidas de avaliação de desempenho para cada fluxo. Na SDN, essas medidas são os contadores e medidores. Os medidores fornecem, por exemplo, funções como qualidade de serviço ou limitação da taxa; os contadores rastreiam a contagem de pacotes, erros, perdas ou *overruns* (“saturações”).
- Permite que os operadores monitorem a infraestrutura de comunicações considerando os aplicativos ao invés de VLANs ou endereços MAC.

É muito mais fácil para as pessoas perguntarem “Onde estão todos os meus fluxos DNP3?” ao invés de “Onde estão todas as minhas 100 portas VLAN?”. Sempre que removemos um potencial erro de interpretação, o sistema se torna mais confiável. Isto significa que a visualização da rede não está limitada à Camada 2 ou Camada 3; ela não é absolutamente limitada às camadas. Os operadores terão a capacidade de projetar todos os circuitos virtuais onde todos os fluxos de comunicação vão trafegar, pré-configurar as ações de resposta aos eventos, monitorar os fluxos de comunicação e reagir ao desempenho indesejado para manter os sistemas críticos operacionais. A tecnologia fornecerá aos operadores uma representação visual rápida do que aconteceu, quais comunicações estão impactadas, e de que forma elas foram impactadas. Isso varia desde qual fio foi cortado até qual segmento de rede está experimentando um ataque de negação de serviço (DoS: “Denial-of-Service”).

A abstração não é nova na indústria de energia; vamos tomar, como exemplo, os valores de medição amostrados (SMVs: “Sampled Measured Values”). Esta é a abstração da conversão analógica-digital dos aplicativos e serviços que utilizam esses dados. O objetivo é encurtar o tempo de implantação dos novos serviços a serem aplicados no sistema de potência. A adoção de novos serviços é lenta no setor de energia porque a ameaça de consequências inesperadas impactando negativamente o sistema é muito grande para se arriscar. No entanto, se os novos serviços pudessem ser aplicados de forma a não impactar, através de seu projeto, o sistema energizado, estes novos serviços poderiam ser aplicados mais rapidamente. A SDN é similar à abstração dos SMVs, onde qualquer novo serviço executado com dados de medidas de avaliação da rede pode ser aplicado no controlador de fluxo e pode coletar os dados sem ameaça de o novo serviço afetar as comunicações ativas. Isso também elimina a necessidade de atualizar o firmware de todos os dispositivos de rede implantados no campo para execução do novo serviço. É importante abordar o impacto na rede da ocorrência de uma falha do controlador ou da incapacidade de o controlador se comunicar com o dispositivo de rede. Neste caso, o dispositivo de rede continua a operar de forma normal e confiável, enviando todas as comunicações aprovadas. O único impacto para o sistema ocorre quando tem início novas comunicações não configuradas, as quais não serão encaminhadas. Normalmente, novas aplicações só devem aparecer quando novos dispositivos forem adicionados à rede. Esta é uma implantação muito controlada no setor de energia e deve ser planejada com antecedência.

A segurança cibernética é outra razão pela qual a equipe do projeto está animada com o impacto positivo que a SDN terá nas redes do setor de energia. Os proprietários do sistema terão finalmente uma solução de controle de acesso de rede *deny-by-default* para fluxos de tráfego, e não apenas para portas e endereços MAC. Mais uma vez, a tecnologia SDN não é limitada às Camada 2 ou Camada 3 de controle de segurança da rede, sendo estabelecida mais em função dos fluxos de comunicação entre *hosts* e quais tipos de fluxos são permitidos, baseando-se nos diversos atributos daquele fluxo. Qualquer fluxo que o switch não tenha visto antes é enviado para o controlador com o propósito de aprovação antes de receber autorização para ser encaminhado. Isto não apenas protege o sistema de fluxos nocivos, mas permite aos operadores do sistema perceberem quando dispositivos são conectados ao sistema, onde eles estão, e o que estão tentando fazer. Os fluxos podem ser descartados, alterados ou registrados. A SDN fornece recursos para que a rede de comunicações seja monitorada e baseada num padrão de referência. A resposta às intrusões cibernéticas pode ser pré-definida para manter os sistemas críticos operacionais. A maior vantagem da segurança cibernética para a indústria de

energia consiste em ser muito estática por natureza, permitindo aos proprietários de ativos adotar um padrão de referência de estados adequados e conhecidos, e monitorar esses estados para garantir que não mudem.

VI. Segurança cibernética com SDN

Este artigo discutiu os diversos benefícios de segurança cibernética avançada fornecidos pela SDN em comparação à tecnologia de redes tradicionais. Basicamente, o potencial desta segurança cibernética está no fato de a equipe de engenharia e operações poder configurar exatamente quais fluxos de comunicação devem existir na rede e qual caminho devem seguir, bem como negar todos os outros fluxos. Isto baseia-se na prática de segurança de conhecer bem o sistema, adotar uma referência de estados adequados e conhecidos, e observar a ocorrência de alterações.

A arquitetura SDN permite um modelo de segurança baseado numa lista branca ("whitelist") dominante, mas também suporta listas negras ("blacklist"), conforme percebido pela equipe. Com a integração de ferramentas como Snort®, isto não é somente possível, mas também fácil. Esta abordagem de lista branca e lista negra é ainda mais simplificada pela capacidade que a SDN fornece ao usuário final para gerenciar as comunicações através do fluxo e não de pacotes, tornando mais fácil a compreensão e gestão a longo prazo. A SDN tem capacidade de efetuar alterações nos pacotes de saída, permitindo aos operadores do sistema pré-determinar ações de resposta a serem efetuadas em certas intrusões ou eventos de confiabilidade. Existem dois métodos que podem alcançar este objetivo. O Método 1 da Fig. 2 mostra o dispositivo *Snort* para inspeção profunda de pacotes (DPI: "Deep Packet Inspection") conectado à interface do controlador de fluxo. O processo do Método 1 é o seguinte:

- O switch identifica DNP3/IP e envia todos os pacotes para o servidor Snort.
- O Snort examina DNP3/IP para aprovação do uso.
- O Snort informa o controlador de fluxo sobre como lidar com o fluxo DNP3/IP (ex., descartar).
- O controlador de fluxo transmite a ação para o switch.
- O switch executa a ação (ex., descartar o tráfego).

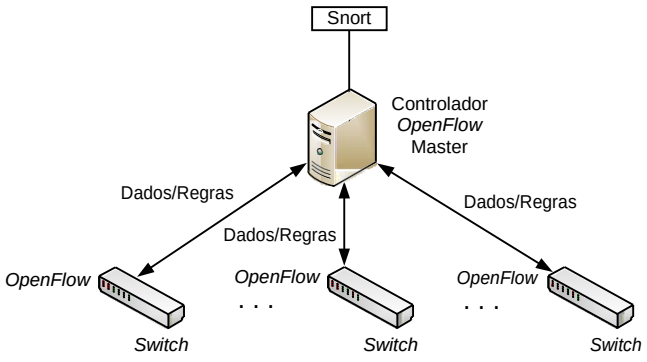

Fig. 2. Dispositivo Centralizado para Inspeção Profunda de Pacotes.

O Método 2 mostra a ferramenta Snort DPI local para o dispositivo de rede e os respectivos fluxos controlados pelo controlador de fluxo. Acreditamos que isto vai melhorar o desempenho da taxa de transferência ("throughput") e latência da funcionalidade DPI. O Método 2 é mostrado na Fig. 3 e opera da seguinte maneira:

- O switch identifica DNP3/IP e envia todos os pacotes para o servidor Snort local.
- O Snort examina DNP3/IP para aprovação do uso.
- O Snort informa o controlador OpenFlow local sobre como lidar com o fluxo DNP3/IP (ex., descartar).
- O controlador OpenFlow local transmite a ação para o switch.
- O switch executa a ação (ex., descartar o tráfego).

No Método 2, observe que o controlador OpenFlow local é configurado como um controlador de fluxo redundante e contém uma cópia da configuração do controlador de fluxo master. O controlador OpenFlow local consiste no *failover* para o master da instalação local em caso de perda de comunicação. Os dois métodos podem ser usados juntos, onde as regras enviadas para o dispositivo de rede são armadilhas para vulnerabilidades específicas e o dispositivo DPI central controla as comunicações da lista branca.

Ter capacidade de visualizar toda a rede como um único ativo representa uma enorme proteção de segurança cibernética. Isso habilita os operadores a monitorar e reagir com precisão às interrupções ou alterações. A SDN permite que o especialista num determinado assunto use as informações. É fundamental que os dados certos estejam nas mãos da pessoa certa para que decisões apropriadas possam ser tomadas. Por exemplo, a SDN permite que dados operacionais sadios sejam transmitidos para os operadores da sala de controle; dessa forma, quando há uma falha no link ou evento SCADA, são eles que vão determinar a solução adequada para o problema. No entanto, se houver um ataque DoS ou novos dispositivos aparecerem na rede, a equipe de tecnologia da informação usa esses dados para adotar contramedidas defensivas para conter os segmentos comprometidos.

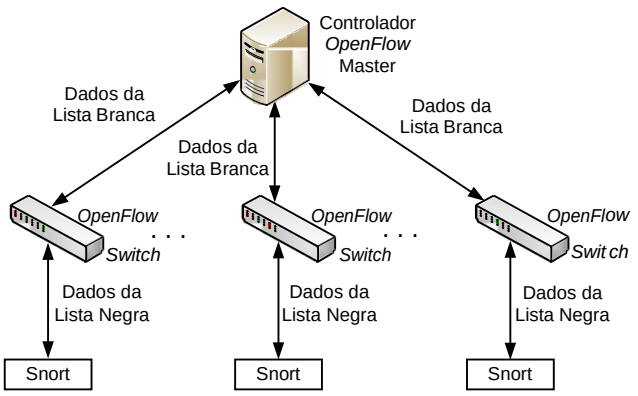

Fig. 3. Dispositivo Distribuído para Inspeção Profunda de Pacotes

Embora a SDN forneça muitos benefícios em comparação às redes tradicionais, algumas das vulnerabilidades das redes tradicionais persistem na SDN, originando novos problemas exclusivos deste domínio. Em particular, as mesmas características da SDN que são desejáveis (gestão e configuração centralizada, por exemplo) se tornam alvos de ataques. Especificamente, alguns dos ataques da rede tradicional podem resultar em danos mais significativos à SDN devido à natureza centralizada do plano de controle. Esta seção discute cada um dos blocos da topologia que compõem a arquitetura SDN, seus desafios de segurança e possíveis atenuações.

O controlador SDN torna-se um alvo de ataques atrativo, pois derrubar o controlador ou obter controle sobre o mesmo pode ter um impacto significativo na rede de controle. Em particular, obter o controle de um controlador pode permitir a um adversário aprender informações sensíveis sobre a rede, efetuar alterações diretas nos dispositivos de rede, interferir em fluxos críticos, e assim por diante. De forma similar, derrubar o controlador pode afetar a continuidade da operação dos serviços dependentes da rede, especialmente se as regras de encaminhamento tiverem períodos de *time-out*. A redundância de controladores ou controladores distribuídos pode atenuar este risco; adicionalmente, a comunidade científica está trabalhando ativamente para resolver esta questão.

Os aplicativos em execução no topo do controlador serão responsáveis pela maior parte da funcionalidade do plano de controle, tais como emissão de alarmes críticos em caso de falha de um componente, ou cálculo de rotas de backup. O compromisso desses aplicativos pode ser igualmente prejudicial se o controlador não limitar os privilégios de autorização para tais aplicativos e fornecer acesso não verificado à API para a rede. Múltiplos aplicativos operando no topo do controlador também podem interferir uns com os outros e resultar em regras conflitantes. O controle de acesso apropriado para aplicativos pode atenuar esta ameaça, sendo que soluções como FortNOX estão disponíveis.

A segurança de transporte do tráfego entre o controlador e os switches pode ser comprometida se não forem tomadas as devidas precauções. Um invasor pode disfarçar-se como um controlador e direcionar os switches para executarem qualquer ação (isto é, assumir a rede essencialmente). Um invasor também pode fingir ser um switch e enviar uma rajada (“burst”) de pacotes falsos em direção ao controlador para lançar um ataque DoS. Mesmo que sejam usados o TLS (“Transport Layer Security”) ou SSL (“Secure Sockets Layer”) com o propósito de proteger o OpenFlow, existem muitos problemas, tais como gestão de infraestrutura de chaves públicas, uso de dispositivos legados dos sistemas SCADA, ou uso de uma implementação de TLS ou SSL vulnerável. Para uma comunicação segura, a questão se torna ainda mais complicada se alguns dispositivos intermediários (“middlebox”) forem inseridos entre o controlador e o switch (tal como FlowVisor) para efetuar o corte da rede em fatias (“slicing”). A gestão cuidadosa de chaves ou certificados e a utilização apenas de comunicações criptograficamente seguras entre o controlador e todos os dispositivos de rede representam as melhores maneiras de atenuação deste risco.

O dispositivo de rede ganhou um grande impulso em seu perfil defensivo simplesmente devido à abstração das computações do plano de controle. O resultado representa menos códigos para o dispositivo e deve minimizar o número de protocolos que precisa suportar para configuração ou acesso da engenharia. Ao convergir todas as configurações de entrada através de apenas algumas interfaces, a tecnologia de monitoramento e proteção defensiva pode ser focada. Conforme identificado anteriormente, a remoção da funcionalidade do plano de controle das caixas de campo e sua centralização no controlador de fluxo reduz o gerenciamento de *patches* para aqueles dispositivos de campo e o risco de alterações não planejadas durante processos de atualização.

VII. Conclusão

Qualquer avanço no setor de energia tem que começar com a necessidade do negócio e suportar as normas de segurança e confiabilidade existentes ou melhorá-las. A interconexão de redes não é diferente. A rede precisa ser projetada para efetuar a comunicação de aplicativos específicos necessários nos sistemas de controle do setor de energia, mantendo ao mesmo tempo os mais altos níveis de confiabilidade. A necessidade de melhoria da segurança e confiabilidade do negócio, com simultânea redução dos custos de operação, exige uma tecnologia mais centralizada e uma força de trabalho mais informada. A SDN é uma tecnologia promissora que fornece tanto visualização quanto gestão de mudanças centralizadas, permitindo ao mesmo tempo que a força de trabalho configure, teste e mantenha a rede de acordo com uma abordagem orientada a serviços e não orientada a pacotes. Ela também integra os ambientes das linhas de transmissão de energia ou *pipeline*s com as redes. Os engenheiros podem aplicar os mesmos princípios de concepção e validação dos fluxos de energia elétrica, petróleo ou comunicações. Mover os elétrons ou pacotes do Ponto A para o Ponto B torna-se uma solução de engenharia que pode ser projetada e testada para N – 1 ou N – 2 condições, com medidas de avaliação de desempenho efetuadas antes de ser aplicada no sistema energizado. É mais fácil para os operadores monitorar e reagir aos serviços e fluxos, prevenindo os aplicativos e atacando diretamente a causa raiz, ao invés de eventos mais abstratos como convergências RSTP ou interrupções de links.

Olhando para o futuro, as demandas de negócios estão acelerando com a automação de respostas à demanda e ações corretivas; logo, a tecnologia tem que habilitar a escalabilidade. A SDN fornece os links necessários para conexão de mais serviços de aplicativos para coleta de medidas de avaliação de desempenho da rede ou dados reproduzidos, como se fossem processados, abstraindo ao mesmo tempo o impacto no sistema energizado. Isso permite

que os proprietários do sistema apliquem, de forma mais agressiva, novas ferramentas de software sem ameaça de impactos no sistema ativo. Tais avanços podem levar à automação preditiva, evitando paralisações nas comunicações ou operando no modo *failover* para caminhos alternativos antes de o caminho primário ser interrompido (resultando em zero perda de pacotes); ou seja, passaremos para um nível de confiabilidade nunca visto antes.

O projeto com compartilhamento de custos do DOE liderado pela Schweitzer Engineering Laboratories, Inc. em parceria com a Ameren Illinois, Pacific Northwest National Laboratory e Universidade de Illinois em Urbana-Champaign está trabalhando para integrar as demandas específicas do setor de energia em um controlador de fluxo SDN que estará disponível comercialmente até 2016. Este trabalho baseia-se no desenvolvimento de um projeto com compartilhamento de custos anterior denominado Watchdog Project, que foca na pesquisa e desenvolvimento de um switch Ethernet habilitado para SDN do setor de energia. O switch Watchdog é ambientalmente robusto e incluirá as interfaces SDN que serão usadas nas comunicações do Projeto SDN, visando fornecer uma solução SDN completa para o setor de energia. Os Projetos SDN e Watchdog ajudam a atender aos objetivos do Roteiro para Obtenção de Segurança Cibernética nos Sistemas de Distribuição de Energia ("Roadmap to Achieve Energy Delivery Systems Cybersecurity") até 2020, ou seja, ter sistemas de distribuição de energia resilientes projetados, instalados e operacionais que possam sobreviver a um incidente cibernético e sustentar as funções críticas.

VIII. Referência

[1] U.S. Department of Energy, Energy Sector Control Systems Working Group, *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, September 2011. Available: http://energy.gov/oe/downloads/roadmap-achieve-energy-delivery-systems-cybersecurity-2011.

IX. Biografias

Rakesh Bobba é professor assistente de pesquisas no Information Trust Institute (www.iti.illinois.edu) na University of Illinois em Urbana-Champaign com nomeações conjuntas nos departamentos de engenharia elétrica e computacional e ciência computacional. Ele obteve seu Ph.D em 2009 da University of Maryland em College Park. Seus interesses de pesquisa são nas áreas de concepção de sistemas computacionais distribuídos e redes seguras e confiáveis, com um foco atual em infraestruturas físicas críticas na área cibernética. Ele é membro do IEEE, IEEE Computer Society, e IEEE Power and Energy Society.

Donald R. Borries é o engenheiro de supervisão no centro de aplicações de tecnologia da Ameren Illinois, localizado ao lado da University of Illinois em Champaign, Illinois. Suas responsabilidades atuais incluem a análise de novos dispositivos de redes inteligentes e avaliação de equipamentos, variando desde segurança cibernética até dispositivos elétricos de 69 kV. Durante sua carreira na Ameren, Donald trabalhou extensivamente nas áreas de geração de energia, sistemas de relés de proteção e manutenção de subestações. Ele recebeu seu B.S. em engenharia elétrica da University of Illinois e atuou na Guarda Costeira dos EUA como "Chief Warrant Officer 4" em engenharia eletrônica.

Rod Hilburn é o gerente do centro de aplicações de tecnologia da Ameren Illinois. Ele tem 28 anos de experiência na indústria de concessionárias de energia elétrica, onde ocupou cargos na engenharia de sistemas de distribuição, projeto de subestações, e construção e manutenção de subestações. Em 1985, recebeu seu B.S. em engenharia elétrica da Missouri University of Science & Technology.

Joyce Sanders recebeu seu diploma de engenharia da University of Missouri – Columbia em 1985. Ela trabalhou na Ameren por 29 anos. Começou sua carreira na indústria nuclear no Callaway Energy Center. Em 1997, mudou para a área de tecnologia da informação, trabalhando no ambiente de troca de mensagens via e-mails. Em 2007, foi promovida para a área de TI na posição Project Management Office (PMO) e recebeu a certificação de Project Management Professional (PMP) em 2008. Ela foi promovida a supervisora de segurança cibernética em 2012. Atualmente, supervisiona sete analistas de segurança e um engenheiro de consultoria, que são responsáveis principalmente pela segurança de sistemas de controle. Isto inclui segurança cibernética para vários aspectos dos sistemas de transmissão e distribuição de eletricidade e gás, geração do centro de energia (incluindo nuclear), e infraestrutura de medição avançada de redes inteligentes (AMI) e gestão de dados de medidores (MDM). Ela recebeu a certificação GIAC Security Leadership Certification (GLSC) em 2012.

Mark Hadley é pesquisador de segurança cibernética no grupo Secure Cyber Systems no Pacific Northwest National Laboratory. Em 1987, recebeu seu B.S. em matemática e ciência computacional da University of Puget Sound. Mark tem mais de 25 anos de experiência em desenvolvimento de aplicativos, engenharia de redes e pesquisas de segurança cibernética para infraestrutura crítica.

Rhett Smith é gerente de desenvolvimento no grupo de pesquisa e desenvolvimento de soluções de segurança e redes de área local na Schweitzer Engineering Laboratories, Inc. (SEL). Em 2000, recebeu seu B.S. em tecnologia de engenharia eletrônica, graduando-se com louvor. Antes de ingressar na SEL, foi engenheiro de aplicação na AKM Semiconductor. Rhett é um profissional com certificado CISSP ("Certified Information Systems Security Professional").

20140423 • TP6655-01