Estudo de Caso: Aplicação de IEC 61850 em uma Subestação de Transmissão de Gana

Charles E. Anderson
Meade Electric Company, Inc.

Salim Zniber, Youssef Botza, David Dolezilek e Justin McDevitt
Schweitzer Engineering Laboratories, Inc.

Apresentado na
PAC World Africa Conference
Cidade do Cabo, África do Sul
30 de julho á 2 de agosto de 2013

Apresentado previamente na
4th Annual Protection, Automation and Control World Conference, junho de 2013

Originalmente apresentado na
Power and Energy Automation Conference, março de 2013

Traduzido para o Português em julho de 2016

Estudo de Caso: Aplicação de IEC 61850 em uma Subestação de Transmissão de Gana

Charles E. Anderson, *Meade Electric Company, Inc.*
Salim Zniber, Youssef Botza, David Dolezilek e Justin McDevitt, *Schweitzer Engineering Laboratories, Inc.*

***Sumário*—Um dos benefícios da implementação do protocolo IEC 61850 consiste em minimizar ou até mesmo eliminar a fiação de cobre usada no campo para troca de dados de proteção e controle entre os dispositivos eletrônicos inteligentes ("Intelligent Electronic Devices" – IEDs) de uma subestação. Por outro lado, a implementação de IEC 61850 introduziu complexidade no comissionamento, testes e manutenção, a qual pode ser minimizada usando uma documentação precisa, além de um planejamento adequado para treinamentos e testes.**

A concepção e a implementação da subestação de transmissão de Kintampo, Gana, exigiram funções de proteção e controle redundantes distribuídas entre os IEDs e uma rede de comunicação robusta para implementação dos protocolos IEC 61850. Para manter um alto nível de disponibilidade, as fontes de alimentação dos dispositivos de proteção primária e de retaguarda são alimentadas por dois carregadores de bateria separados que também alimentam bobinas duais de trip para os disjuntores *ac* de alta tensão de 161 kV. O uso de esquemas de proteção primária dual em ambos os relés de proteção de distância e diferencial e a abertura e religamento monofásicos da linha de transmissão aumentam a disponibilidade, estabilidade e confiabilidade do sistema de transmissão. Os equipamentos instalados ao ar livre, montados em invólucros perto dos disjuntores, coletam e reportam o estado e os alarmes dos disjuntores e das chaves seccionadoras operadas por motores ("Motor-Operated Disconnects" – MODs), assim como fornecem controle das MODs e da chave de aterramento da linha de transmissão.

A subestação de Kintampo possui um sistema de automação da subestação ("Substation Automation System" – SAS) robusto e confiável, incluindo uma interface homem-máquina (IHM) para controle e indicação local, um servidor do sistema de supervisão e aquisição de dados ("Supervisory Control And Data Acquisition" – SCADA) para fornecer dados de medição, controle e estado para a IHM local e para o sistema corporativo remoto da concessionária, e uma rede Ethernet robusta com *switches* nível industrial para comunicações confiáveis que possam suportar esquemas de proteção de alta velocidade para missões críticas.

A rede Ethernet usa uma topologia em anel com o protocolo RSTP ("Rapid Spanning Tree Protocol") e redes de área local virtuais ("Virtual Local-Area Networks" – VLANs) para fornecer redundância de rede, confiabilidade, segregação de dados e controle de tráfego. O SAS usa os protocolos de comunicação MMS ("Manufacturing Message Specification") e GOOSE ("Generic Object-Oriented Substation Event") da norma de comunicação IEC 61850 para controle e aquisição de dados e para os esquemas de proteção *peer-to-peer* de alta velocidade.

Este artigo discute vários aspectos essenciais do projeto elétrico, projeto da rede de comunicação, proteção e controle, além dos testes e comissionamento de uma subestação baseada no IEC 61850.

I. Introdução

Gana está sendo submetida a importantes *upgrades* elétricos, afetando todos os aspectos do sistema de potência, desde a geração até a transmissão e distribuição. A subestação Kintampo vai transmitir e distribuir 400 MW da potência gerada na usina de Bui para centenas de comunidades ao longo de Gana. Duzentas e dezesseis dessas comunidades estão sendo eletrificadas pela primeira vez como parte do programa de eletrificação SHEP ("Self-Help Electrification Program"). Este artigo documenta o uso inovador de sistemas de comunicação padrão internacional com projetos modernos baseados na rede Ethernet para proteção, controle e monitoramento da subestação 161 kV/34,5 kV.

Com o rápido desenvolvimento e conhecimento da norma de comunicação IEC 61850, a concessionária local solicitou, por diversas razões, que vários protocolos e métodos definidos dentro da norma fossem implementados nesta subestação. O principal motivo consistiu em minimizar as conexões de cobre entre o campo e a casa de controle. Isso foi efetivamente atendido por meio da troca de mensagens digitais através de cabos de fibra óptica, atuando como uma fiação virtual entre os dispositivos eletrônicos inteligentes (IEDs) ligados em rede. As práticas de fiação da subestação variam em função do nível de tensão, embora o número de fios (ou seja, o número total de pontos que estão sendo medidos e controlados) seja relativamente constante entre os componentes. O comprimento do cabo e o número de caminhos de dados são reduzidos significativamente por meio da localização dos equipamentos de proteção e controle no pátio [1]. Isso reduz a quantidade de material e mão de obra envolvida e também torna muito mais fácil verificar a precisão da fiação, resultando numa economia significativa de tempo durante a instalação.

Outra razão importante para a escolha de um projeto baseado em IEDs ligados em rede foi a possibilidade de aproveitar os benefícios adicionais tangíveis e intangíveis. Esses benefícios são amplamente baseados no fato de que os IEDs criam e contêm dados precisos e bem organizados sobre os próprios IEDs e equipamentos primários. Os IEDs também possuem recursos de processamento, memória e comunicação para converter os dados em informações sobre as condições e o desempenho do sistema de potência. A capacidade de os IEDs testarem sua própria condição, armazenarem a sequência dos relatórios de eventos ("sequence-of-events" – SOE) e fornecerem detalhes dos ativos e informações de firmware mediante solicitação torna os processos anteriormente tediosos mais simples e automáticos. Sob uma perspectiva de configuração e comunicação, um dos maiores benefícios de

engenharia é a capacidade de autodocumentação dos arquivos SCL ("Substation Configuration Language") do IEC 61850 armazenados diretamente nesses IEDs. O encapsulamento dentro de um IED de um modelo de dados que descreva universalmente cada parte dos dados da subestação e seus atributos consiste numa das maiores vantagens oferecidas por esta tecnologia.

II. Proteção e Controle

A subestação Kintampo é composta de dois pátios de subestação. Um deles é uma subestação de transmissão de 161 kV com quatro linhas de transmissão, dois transformadores abaixadores e nove disjuntores arranjados em um esquema de disjuntor e meio. O outro é uma subestação de distribuição de 34,5 kV consistindo de duas alimentações de entrada dispostas em um esquema "main-tie-main" ("principal-interligação-principal") com oito alimentadores. As duas estações são conectadas através de cabos subterrâneos e estão afastadas em várias centenas de metros. O diagrama unifilar da subestação de transmissão é mostrado na Fig. 1.

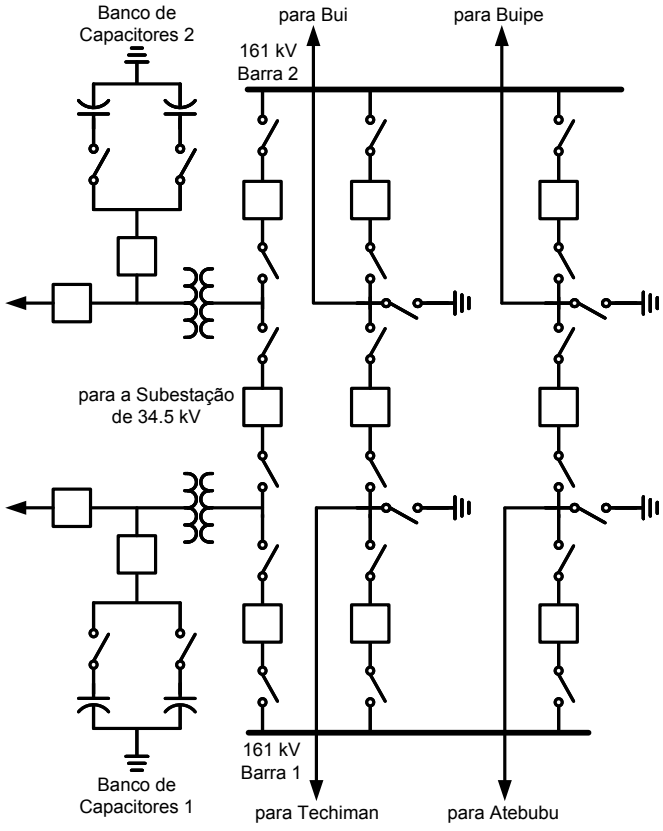

Fig. 1. Diagrama unifilar da subestação de transmissão de Kintampo.

O arranjo elétrico da subestação de transmissão propicia flexibilidade operacional. Se a subestação de transmissão for normalmente operada com cada disjuntor fechado, a perda de um transformador, linha de transmissão ou barra de 161 kV não afeta o fluxo de potência de distribuição. No entanto, o projeto requer esquemas de proteção e controle mais complexos. A proteção redundante é fornecida através da subestação usando IEDs de proteção primária e de retaguarda. Os IEDs são alimentados por sistemas de baterias de retaguarda e circuitos *dc* separados. Cada disjuntor possui capacidade de abertura monopolar e tripolar com bobinas de trip redundantes para cada fase. O IED primário dá trip na Bobina de Trip 1 enquanto o IED de retaguarda dá trip no disjuntor via Bobina de Trip 2.

Este artigo foca nos aspectos de comunicação do sistema. As aplicações de proteção estão fora do escopo, mas são geralmente consistentes com os métodos tradicionais das aplicações de aceleração da proteção através do compartilhamento de informações entre IEDs. Os sofisticados esquemas de proteção e controle de Kintampo dependem de comunicações confiáveis e determinísticas para uma transmissão de dados constante entre IEDs. Esses dados eram transmitidos anteriormente pela conexão ("hardwired") de uma saída física do IED fonte com uma entrada física do IED de destino via condutores de cobre. As comunicações dos IEDs são efetuadas através de mensagens GOOSE ("Generic Object-Oriented Substation Event") entre o IED fonte e um ou mais IEDs de destino. Isso requer uma configuração cuidadosa das mensagens GOOSE dentro dos IEDs e informações sobre onde entregar as mensagens dentro dos *switches* Ethernet. As mensagens GOOSE são *multicast*, significando que elas podem ser entregues para muitos receptores dos IEDs. No entanto, sem uma configuração da rede de área local ("Local-Area Network" – LAN) apropriada, as mensagens *multicast* são enviadas para cada dispositivo individual do sistema. Essas mensagens GOOSE suportam funções de proteção e controle, tais como falha do disjuntor, modo de teste GOOSE e partida do religamento. Talvez o mais importante seja o fato de esta troca de mensagens ser constantemente supervisionada por cada IED receptor visando detectar imediatamente problemas na entrega de mensagens. Se houver problemas, os IEDs receptores revertem para a lógica não dependente das comunicações e alertam os técnicos sobre o problema.

A. Comunicações do Esquema de Falha do Disjuntor

Os IEDs primários duais que controlam cada disjuntor da linha de transmissão e o IED de proteção do transformador que controla o disjuntor do transformador também atuam como proteção contra falha do disjuntor. As mensagens GOOSE transmitem indicações da mudança de estado dos dados Booleanos, tais como estado do disjuntor, valores analógicos como medição, e sequências de bits. Em seguida, os IEDs receptores interpretam e atuam de acordo com as indicações que sejam imediata e diretamente apropriadas à sua condição e outras lógicas e entradas. Dessa forma, os dados GOOSE não são comandos de trip direto, mas são mais propriamente indicações dos estados remotos que são usadas nas equações de trip. A transmissão de informações entre vários IEDs é necessária em dois estágios da proteção contra falha do disjuntor: indicação da partida do esquema de falha do disjuntor e indicação do trip por falha de disjuntor, as quais são obtidas no IED fonte e transmitidas para os relés apropriados. Além disso, nos casos em que as operações monopolar e tripolar são ambas possíveis, as indicações para ambas as operações são transmitidas dentro da mensagem GOOSE. Nos casos onde o IED de retaguarda dá trip no disjuntor antes de o IED primário ativar um trip, o IED de retaguarda envia um sinal de partida do esquema de falha de disjuntor monopolar ou um sinal de partida do esquema de falha de disjuntor tripolar, dependendo do tipo da falta, para o relé primário.

Uma vez que o sinal de partida do esquema de falha do disjuntor tenha sido recebido, o relé primário parte um temporizador de 12 ciclos. Se o disjuntor ainda não interrompeu a falta quando expirar o tempo do temporizador, o IED primário declara uma condição de falha do disjuntor e envia uma indicação de trip para os relés adjacentes dentro de uma mensagem GOOSE. Os IEDs receptores atuam de acordo com esta indicação para dar trip nos respectivos disjuntores visando isolar o disjuntor com defeito. Na subestação Kintampo, ambos os relés primário e de retaguarda também recebem indicações de trip por falha de disjuntor dos IEDs adjacentes, incluindo os relés de proteção da barra de 161 kV, proteção da linha de transmissão oposta, proteção da linha de transmissão adjacente e proteção do transformador.

B. Comunicações no Modo de Teste do GOOSE

Para testar ou comissionar um relé sem afetar os outros IEDs dentro da subestação, um bit de selo ("latch bit" – biestável) do modo de teste do GOOSE foi programado em cada relé. O selo é ativado através de um botão de pressão ("pushbutton") no painel frontal do relé ou através de um bit remoto ("remote bit") da interface homem-máquina (IHM), e está incluído na mensagem GOOSE de saída. Quando o selo está ativado, um usuário pode testar os elementos de proteção do relé e a comunicação com outros relés da zona sem causar a operação de qualquer um dos outros disjuntores. O relé supervisiona o bit selado ("latched bit") na sua própria lógica e publica ("publishes") o bit nas suas publicações GOOSE de saída. Os relés de recepção aceitam a indicação do modo de teste dentro da mensagem GOOSE e são consequentemente programados para bloquear algumas funcionalidades durante os testes para evitar uma operação inadvertida. Por exemplo, se o modo de teste GOOSE estiver habilitado em um relé, os outros relés da zona recebem a indicação desta condição através da indicação do modo de teste GOOSE sendo determinada como verdadeira na mensagem GOOSE. Portanto, quando a indicação do modo de teste GOOSE for usada como permissão para a lógica de bloqueio, conforme mostrado na Fig. 2, os dados recebidos do relé testado são atualizados, mas não têm efeito sobre os IEDs receptores. Se o esquema de falha do disjuntor for ativado num relé que está no modo de teste do esquema de falha de disjuntor do GOOSE, os outros relés que normalmente dariam trip em uma condição de falha do disjuntor não vão operar. No entanto, os outros relés ainda recebem uma indicação do modo de teste do GOOSE e falha de disjuntor, que pode ser verificada através do display do painel frontal. Para fornecer isolação das funções individuais de proteção, indicações do modo de teste do GOOSE são criadas para cada função de proteção exclusiva a ser testada.

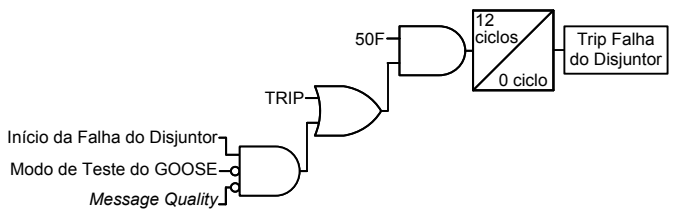

Fig. 2. Lógica de trip por falha do disjuntor.

C. Comunicações para Partida do Religamento

Para a proteção da linha de transmissão da subestação, o relé Principal 1 é usado como religador primário, enquanto o relé Principal 2 é usado como religador de retaguarda. O religamento do Principal 2 é habilitado somente quando o relé Principal 2 detecta uma falha de comunicação do relé Principal 1, o que pode significar que o relé Principal 1 está fora de serviço. Contudo, devido à natureza não determinística da Ethernet, uma falha de recepção da mensagem GOOSE pode indicar *switches* Ethernet ou cabos Ethernet com defeito, bem como um relé defeituoso. Se não houve falha do relé Principal 1, mas sim da recepção GOOSE do mesmo, ambos os relés principais podem iniciar o religamento. Uma falha na recepção da mensagem GOOSE em um relé não significa necessariamente que outros relés não estejam recebendo as mensagens GOOSE *multicast*.

O projeto de religamento global considera ambas as condições de abertura monopolar e tripolar. O religamento é iniciado por ambos os relés principais para faltas monofásicas e multifásicas detectadas pelos elementos de distância, esquema piloto, elementos de sobrecorrente ou diferencial de corrente de linha. O religamento é ajustado em uma tentativa para monopolar seguida por uma tentativa para tripolar. Para uma falta fase-terra, o relé primário emite um sinal de abertura monopolar e religa. Se a falta ainda estiver presente após o religamento monopolar, o relé inicia a abertura tripolar. O intervalo de tempo aberto para a abertura tripolar é de 900 ciclos (15 segundos). Se a falta inicial envolveu múltiplas fases, o relé inicia uma abertura tripolar e apenas efetua uma única tentativa de religamento tripolar se a falta ainda estiver presente. Após o religamento e se a falta ainda estiver presente, o relé efetua uma abertura tripolar e o religador é conduzido para o estado de bloqueio.

Como o relé Principal 2 pode dar trip no disjuntor sem que o relé primário tenha habilitado o trip, uma indicação de partida do religamento é enviada via mensagem GOOSE do relé Principal 2 para o relé Principal 1. O relé Principal 1 inicia, em seguida, a sequência de religamento apropriada, dependendo se a indicação recebida é um religamento monofásico ou multifásico.

III. Fiação Existente na Subestação Versus Novas Práticas

As práticas de fiação das subestações variam em função do nível de tensão, idade dos equipamentos e tecnologia dos dispositivos associados. Tradicionalmente, o cobre é a principal interface entre os componentes do pátio e um relé centralmente localizado dentro de uma casa de controle. A avaliação das instalações tradicionais em operação considera que existem tipicamente 44 condutores entre o pátio e um relé na casa de controle. Normalmente, vários cabos com múltiplos condutores são utilizados; cabos separados são tipicamente instalados para o comando do disjuntor (abrir/fechar) e secundários do transformador de corrente (TC) e transformador de potencial (TP). O percurso da fiação é razoavelmente longo, medindo entre 200 e 500 metros, conforme mostrado na Fig. 3.

Fig. 3. Condutores de cobre removidos das trincheiras de cabos e substituídos pela tecnologia baseada na troca de mensagens digitais.

Os caminhos de dados horizontais para troca de informações entre componentes, denominados "fios" na Fig. 4, representam os pares de fios de cobre conduzindo as informações de medições analógicas, binárias e de estado em tempo real. Neste caso, cada caminho de dados inclui uma fonte de dados no lado esquerdo e um cliente de dados no lado direito.

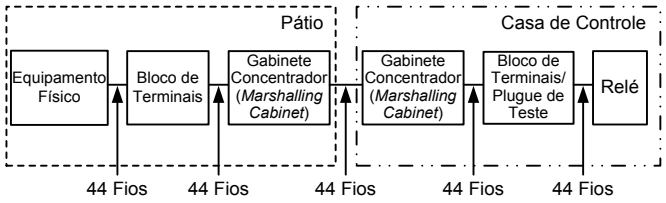

Fig. 4. Método de fiação tradicional com relés na casa de controle.

Embora o número de fios (isto é, o número total de pontos que estão sendo medidos e controlados) seja relativamente constante entre os componentes, o comprimento do fio e o número de caminhos de dados são significativamente reduzidos por meio da instalação dos equipamentos de proteção e controle no pátio, conforme mostrado na Fig. 5 [1]. Isso reduz a quantidade de material e mão de obra envolvida e também facilita a verificação da precisão da fiação, resultando numa economia significativa de tempo durante a instalação.

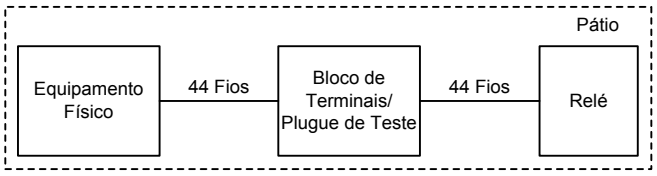

Fig. 5. Método de fiação para relés no pátio.

A instalação dos relés microprocessados no pátio melhora significativamente a funcionalidade global, reduz as dimensões e simplifica a fiação interna dos gabinetes. Contudo, é necessário ter muito cuidado na seleção de IEDs que sejam projetados para o ambiente agressivo das instalações ao ar livre, conforme demonstrado pelas características nominais ambientais rigorosas e garantias extensas do fabricante.

Mesmo sem mover o relé para o pátio, a comunicação digital das I/Os digitais simplifica enormemente as instalações. Mais de 50% dos fios do caminho de dados do pátio até a casa de controle são associados aos sinais de controle do disjuntor. Portanto, é vantajoso usar um método híbrido no qual a fiação dos TCs e TPs é mantida, mas a fiação de controle é substituída por um cabo de comunicação e módulo do transceptor de entradas/saídas (I/Os) baseado em fibra óptica, conforme mostrado na Fig. 6.

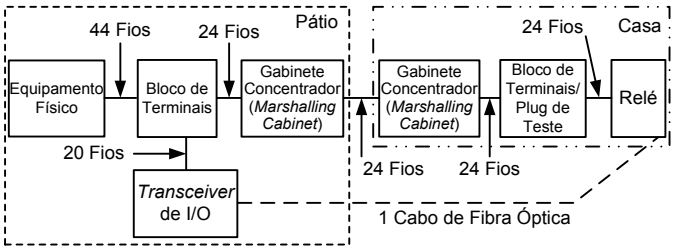

Fig. 6. Projeto híbrido mostrando a quantidade de fios de cobre substituídos pela tecnologia do módulo de I/Os baseada em fibra óptica.

O método baseado no módulo de I/Os propicia uma economia significativa na fiação e introduz a capacidade de monitorar as condições de funcionamento da conexão dos dados. Esta prática tem sido comprovada no campo por mais de uma década, baseando-se nas normas de comunicação digital desenvolvidas para este propósito, criadas pelas SROs ("Standards-Related Organizations" – "Organizações Associadas a Normas") e oferecidas através de uma licença "razoável e não discriminatória" ("reasonable and nondiscriminatory license"), tal como as comunicações MIRRORED BITS®. Adicionalmente, protocolos criados por SDOs ("Standards Development Organizations" – Organizações para Desenvolvimento de Normas), tais como IEEE e IEC, são de grande utilidade. Uma das duas formas de mensagens GOOSE via IEC 61850 padronizadas tem sido usada no campo por mais de uma década, e outras normas estão em uso, tal como a IEEE C37.94. Conforme mencionado, os dispositivos usam o estado indicativo das condições da conexão para supervisionar o caminho de dados digitais e diferenciar entre silêncio devido à inatividade e silêncio devido a um condutor rompido. A confiabilidade é melhorada em função da redução no número de caminhos de dados, dispositivos, processos e componentes não supervisionados. Os módulos de I/Os minimizam o número de caminhos de dados não supervisionados entre as fontes do campo e os clientes de dados dos componentes. Este método melhora enormemente o valor dos dados ao confirmar a disponibilidade e confiabilidade dos métodos através dos quais eles são coletados e ao emitir um alarme quando um caminho de dados é interrompido. Finalmente, os cabos de fibra óptica também oferecem isolação galvânica dos caminhos de dados entre os componentes.

A redução na fiação da subestação é obtida na subestação Kintampo através do protocolo IEC 61850 GOOSE em tempo real, especificamente otimizado para uma transmissão de dados confiável e oportuna. Sua utilização é melhor compreendida analisando o exemplo de redução da fiação através das I/Os digitais. A Fig. 6 ilustra uma abordagem simples e direta do uso das mensagens GOOSE via IEC 61850 para digitalizar e transmitir informações bidirecionais entre os

equipamentos do pátio da subestação e o controlador da casa de controle.

Baseando-se na preferência do usuário, outros projetos envolvem mover o relé como um todo para dentro do quiosque de campo, conforme mostrado na Fig. 7 [2]. Isso ilustra uma forma simples para transmissão de dados entre um relé instalado no quiosque de campo e um controlador da estação instalado na casa de controle.

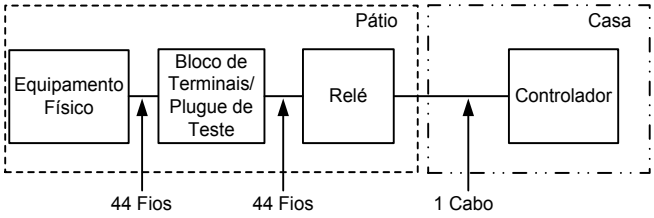

Fig. 7. Diagrama simplificado mostrando a redução potencial dos cabos através da tecnologia da fiação virtual baseada na Ethernet.

Embora conceitualmente muito simples, o projeto da Fig. 7 não aproveita totalmente as vantagens dos recursos da rede Ethernet. O link Ethernet entre o relé e o controlador da casa de controle é instalado como uma interface ponto a ponto dedicada.

Uma abordagem geral interoperável baseada em padronizações com um *switch* Ethernet, LAN e comunicações entre vários dispositivos é mostrada na Fig. 8

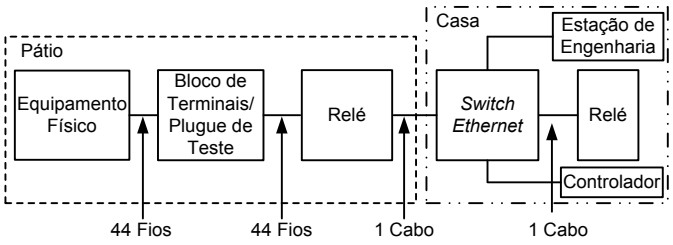

Fig. 8. Instalação do relé baseada na Ethernet com um *switch* Ethernet.

IV. IEDs Instalados no Campo Fornecem Alarme dos Disjuntores e Chaves Seccionadoras Operadas por Motor

Os modernos quiosques pré-fabricados para instalação no campo e as casas de controle modulares usadas em Kintampo seguem a separação dos projetos mostrada na Fig. 6. Todos os componentes necessários para a aplicação no pátio são pré-instalados em um quiosque de campo pré-fabricado, e todos os itens comumente instalados em uma casa construída no local são pré-instalados em um edifício de controle pré-fabricado. Este método pré-projetado reduz enormemente o tempo do projeto global.

Esta opção foi basicamente escolhida para Kintampo porque simplifica enormemente o processo de aquisição e instalação e simplifica a preparação do local e o comissionamento. O sistema tornou-se uma solução pré-projetada, pré-testada e repetível, desenvolvida de acordo com as especificações do usuário de forma similar aos equipamentos primários.

Os requisitos do usuário foram tais que o controle do disjuntor foi implementado usando um módulo de chaves de controle com indicação localizado na casa controle e conectado ("hardwired") até o disjuntor do pátio, conforme mostrado na Fig. 9.

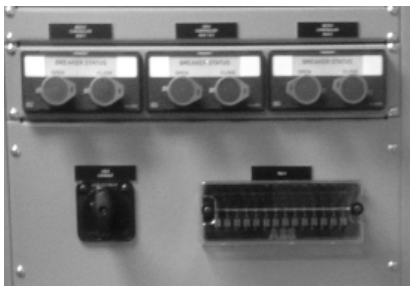

Fig. 9. Módulo de chaves de controle com indicação localizado na casa de controle.

Os alarmes dos disjuntores e o controle e estado das chaves seccionadoras operadas por motores ("Motor-Operated Disconnects" – MODs) são conectados ("hardwired") aos equipamentos instalados ao ar livre, montados em invólucros, e transmitidos via mensagens IEC 61850 através de cabo de fibra óptica, conforme indicado na Fig. 6 e ilustrado na Fig. 10. Isso eliminou uma quantidade significativa de fiação entre o pátio e a casa de controle. Os alarmes dos disjuntores, incluindo baixa pressão de SF6, chave de controle remoto e monitoramento da bobina de trip, são reportados para a IHM a partir dos IEDs do quiosque de campo utilizando o protocolo MMS ("Manufacturing Message Specification") baseado em pergunta e resposta via IEC 61850.

Além disso, os controles de abertura e fechamento das MODs são implementados através de fiação, conectando a saída do módulo da chave de controle a uma entrada do relé do disjuntor associado no mesmo painel. Uma vez que a entrada seja ativada, o relé da casa de controle envia uma mensagem GOOSE para o equipamento externo para executar a ação apropriada de abertura ou fechamento e, em seguida, envia o estado da MOD de volta para a IHM e relé. O relé então, por sua vez, fornece um contato de saída a uma entrada no módulo de controle para fornecer uma indicação.

As chaves de aterramento localizadas próximas aos disjuntores da linha de transmissão possuem sua indicação de aberta/fechada através de fiação até o equipamento ao ar livre. Esta informação também é enviada para a lógica de controle do disjuntor dentro dos relés da casa de controle via GOOSE para evitar o fechamento do disjuntor quando a chave de aterramento estiver fechada.

Fig. 10. Instalação típica de um quiosque de campo com IEDs.

V. Projeto Ethernet e Considerações

A Ethernet encontrou um lugar nos sistemas industriais com segurança crítica e nas redes de subestações para missões críticas. Qualquer discussão sobre a Ethernet (que define as camadas dos links de dados e físicas do modelo de comunicação OSI ["Open Systems Interconnection"] de sete camadas) será incompleta se não incluir as topologias de rede e os protocolos da camada superior criados por SROs e SDOs, tais como IEEE e IEC. Na indústria de sistemas de potência, a Ethernet é frequentemente identificada através do conjunto de protocolos IEC 61850, bem como dos protocolos IEEE C37.118 para transmissão de sincrofasores e protocolos usados apenas para aquisição de dados e controle supervisório (somente SCADA), tais como DNP3/IP ("Distributed Network Protocol/Internet Protocol" – "Protocolo de Rede Distribuída/Protocolo Internet") e IEC 60870-5-104. Ao contrário do caminho da mensagem das mensagens diretas seriais, que seguem o mesmo caminho do cabeamento físico entre dispositivos, as mensagens Ethernet trafegam por caminhos ditados por métodos como RSTP ("Rapid Spanning Tree Protocol"), que habilita os circuitos de dados virtuais através da rede Ethernet. As redes Ethernet, independentemente do cabeamento redundante, sempre selecionam um único caminho ativo para o tráfego de mensagens entre os dispositivos da rede. Portanto, o projeto do cabeamento e dos *switches* deve ser efetuado por projetistas conscientes das implicações da tecnologia do projeto dos caminhos da rede Ethernet subjacente, visando garantir que os caminhos sejam adequados às aplicações que requerem troca de dados. As redes Ethernet têm que ser cuidadosamente projetadas—não simplesmente montadas.

A confiabilidade da tecnologia operacional ("Operational Technology" – OT) é maximizada pela escolha de IEDs com duas portas Ethernet operando no modo *failover* e conectadas a *switches* redundantes. Para a OT do sistema de potência, as aplicações mais exigentes requerem uma troca de mensagens rápida e segura entre os *peers* para execução da teleproteção, intertravamento e automação de alta velocidade. As normas internacionais relativas à confiabilidade das aplicações de teleproteção dos sistemas de potência permitem que entre 0 e 9 mensagens sejam descartadas em um período de 24 horas de trocas de mensagens GOOSE, exigem que as mensagens sejam entregues em menos de 4 milissegundos em 99,99% do tempo e requerem que os restantes 0,01% das trocas experimentem um tempo de transmissão máximo menor do que 10, 20 ou 30 milissegundos, dependendo do esquema de proteção específico [3]. Simplificando, as exigências do tráfego das mensagens são:

- Caminhos de mensagens redundantes, no caso de falha do caminho primário.
- Baixa latência.

O projeto baseado na redundância fornece um caminho secundário após uma falha do segmento ou do *switch*. O projeto com baixa latência minimiza o número de *switches* através dos quais a mensagem tem que passar no trajeto entre dispositivos.

As mensagens *multicast* dentro dos IEDs, tais como mensagens GOOSE via IEC 61850, são enviadas para um ou mais IEDs para compartilhar dados visando acelerar a teleproteção, intertravamento e automação de alta velocidade. As melhores práticas de configuração de IEDs e *switches* para uma operação correta das mensagens GOOSE são discutidas na Seção VI, Subseção C. A segregação da LAN Virtual (VLAN) é importante não apenas para gerenciar o tipo e a quantidade de tráfego enviada para cada IED, mas também para gerenciar a quantidade de tráfego dentro dos próprios *switches*. Ao manter o tráfego restrito ao que é adequado e necessário em cada segmento de rede, a saturação da largura de banda é menos provável.

VI. Arquitetura de Rede

A. Topologia de Rede

A LAN da subestação Kintampo é projetada para fornecer uma plataforma confiável e determinística para os esquemas de proteção baseados nas comunicações da subestação. A LAN da subestação possui uma configuração em anel de *switches* Ethernet industriais robustos e próprios para subestações. Todos os IEDs possuem duas portas Ethernet operando no modo *failover* com duas conexões separadas para dois *switches* diferentes. As conexões dos IEDs são feitas em fibra óptica multimodo 100BASE-FX. Uma topologia em anel foi escolhida porque, quando combinada com RSTP, esta topologia propicia redundância para a rede no caso de uma falha de conexão ou do *switch*. Além disso, é fácil de compreender, testar e instalar no campo. A quantidade de IEDs é suficientemente pequena, de forma que quando conectado no modo *failover*, este projeto corresponde ou supera qualquer outra escolha de topologia em relação à confiabilidade e recuperação. Com esta topologia, nenhuma falha individual na rede (ou duas ou mais falhas, em alguns casos) resulta em perda de comunicação. Anéis amplos

experimentam tempos longos de recuperação após uma falha do link ou *switch*; logo, outras topologias devem ser consideradas em sistemas maiores e diferentes. A Fig. 11 exibe uma parte do *layout* da rede de Kintampo. Ao projetar conexões *switch*-para-*switch*, recomenda-se usar conexões de latência igual ou similar de forma que tenham o mesmo desempenho e que o comportamento do tráfego não mude radicalmente quando a reconfiguração da rede mover o tráfego de um segmento para seu parceiro redundante. A latência de cada segmento é determinada pela sua velocidade (ou seja, a velocidade de trânsito das mensagens, descrita como capacidade) ou largura de banda.

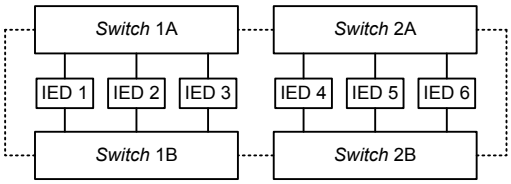

Fig. 11. Diagrama com uma amostra do *layout* da rede.

B. Projetando o RSTP

Especial cuidado deve ser tomado durante o desenvolvimento de uma rede que usa o RSTP para recuperação no caso de uma falha. Gastar certo tempo para configurar os diversos ajustes do RSTP garante que a rede se recupere da melhor maneira no caso de uma falha. Um dos *switches* da rede atua como a ponte raiz ("root bridge") ou *switch* raiz ("root switch") para ser o ponto de partida para todas as decisões de topologia da rede. Como é preciso haver um ponto de partida, se o usuário não fizer a escolha, os *switches* escolhem entre eles mesmos para selecionar uma, e somente uma, raiz. Deixando a escolha por conta dos mesmos, os *switches* usam os endereços do controle de acesso à mídia ("Media Access Control" – MAC) para efetuar a decisão. Os engenheiros de rede devem escolher um *switch* raiz de forma que eles conheçam definitivamente a topologia e estejam aptos a prever as alterações de topologia. A designação do *switch* raiz pode ser atribuída a um dispositivo ajustando-se a prioridade da ponte para um número suficientemente baixo.

O processo do RSTP reconhece a raiz como o ponto focal lógico da rede, e todos os segmentos são identificados com base na sua proximidade com a raiz. O RSTP minimiza a distância que as mensagens têm que trafegar a partir de todos os pontos da rede até a raiz. Portanto, todos os IEDs próximos à raiz estão próximos uns dos outros, com menos cabos e *switches* através dos quais as mensagens têm que passar. Se a rede tiver uma topologia em estrela ou "hub-and-spoke", então o *switch* do centro deve ser designado como a ponte raiz. Em Kintampo, nenhum *switch* é fisicamente mais central do que o outro, uma vez que eles estão conectados em anel, logo o *switch* com mais IEDs conectados a ele foi selecionado como a ponte raiz.

C. Projeto de VLAN para GOOSE

Os *switches* Ethernet da subestação Kintampo são configurados através de VLANs para segregar o tráfego na rede. Cada interface da rede de IEDs tem que processar todas as mensagens Ethernet recebidas, incluindo as mensagens GOOSE via IEC 61850 frequentes, mesmo se não for o destinatário planejado. Como as mensagens IEC 61850 GOOSE são baseadas no tráfego Ethernet *multicast*, os *switches* Ethernet tentam enviá-las para cada interface Ethernet da LAN do sistema. No entanto, os *switches* da LAN de Kintampo são projetados para passar ou negar o identificador de VLAN (ID) de cada mensagem GOOSE baseando-se em qual IED está conectado às portas dos *switches*. Uma VLAN exclusiva foi criada para cada mensagem IEC 61850 GOOSE e os *switches* foram definidos em conformidade, de forma que a mensagem seja entregue apenas para os dispositivos que estão configurados para recebê-la. Restringindo as VLANs em cada porta do *switch* para as mensagens GOOSE que são configuradas para serem recebidas pelo IED em uma porta específica, todos os outros tráfegos GOOSE são bloqueados. Isso minimiza a quantidade de tráfego que cada IED tem que processar, maximizando, como resultado, o desempenho das portas Ethernet dos IEDs. Isso também reduz a probabilidade de saturação da largura de banda em qualquer segmento da rede ao reduzir o tráfego desnecessário. Cada porta do IED no *switch* foi configurada com o mesmo ID da VLAN nativa da porta ou ID da VLAN baseada na porta para todos os outros tráfegos não associados ao GOOSE.

A lista completa das melhores práticas de engenharia para uso da fiação virtual Ethernet através de mensagens digitais para substituir os condutores de cobre é bastante extensa [3]. Os projetistas que usam IEDs de Proteção, Controle e Monitoramento ("Protection, Control, and Monitoring" – PCM) e redes para mensagens *multicast* Camada 2 têm que respeitar as seguintes regras para projetar e configurar mensagens e parâmetros de engenharia de rede:

- Atribuir a cada mensagem GOOSE uma VLAN exclusiva baseada em IEEE 802.1Q, referida como QVLAN.
- Atribuir a cada mensagem GOOSE um endereço MAC multicast exclusivo conforme IEC 15802-1.
- Atribuir a cada mensagem GOOSE um identificador exclusivo da aplicação (app ID).
- Atribuir um identificador GOOSE descritivo (GOOSE ID) ao invés de um ID genérico no IED para melhorar a documentação e a solução de problemas.
- Etiquetar os conteúdos de payload da mensagem GOOSE com nomes descritivos ao invés de genéricos no IED para melhorar a documentação e a solução de problemas.
- Projetar cuidadosamente os conteúdos e o tamanho do payload para facilitar o processamento do aplicativo GOOSE apropriado— mind the gap.
- Escolher cuidadosamente IEDs que processem as mensagens GOOSE recebidas suficientemente rápido para as aplicações da classe de proteção—mind the gap.
- Não publicar mensagens multicast na rede sem etiquetas ("tags") QVLAN.

- Desabilitar todas as portas de comunicação de PCM não utilizadas.
- Monitorar os atributos das mensagens GOOSE para derivar a qualidade da mensagem ("message quality").
- Usar os atributos de GOOSE referentes ao número de sequência e número de estado para determinar se todas as mensagens desejadas chegam até o receptor.
- Monitorar, registrar e emitir alarme para falha na qualidade das mensagens GOOSE.
- Fornecer relatórios GOOSE com informações de estado, configuração e estatísticas relativas às mensagens GOOSE que estão sendo publicadas e subscritas pelo IED.
- Registrar e emitir alarme para falha na qualidade das mensagens GOOSE para uso em aplicações locais e remotas.
- Exibir o estado das subscrições GOOSE e alertar os operadores sobre uma falha.
- Configurar cada porta do switch para bloquear a entrada de mensagens indesejadas e permitir mensagens multicast desejadas via filtragem MAC e VLAN. Isso reduz o tráfego multicast através da rede para apenas o que é necessário.
- Configurar cada porta do switch para bloquear a saída de mensagens indesejadas e permitir mensagens multicast desejadas via filtragem MAC e VLAN. Isso evita que mensagens não desejadas cheguem até os IEDs.
- Usar switches projetados para ambientes agressivos e multicast Camada 2 entre PCM IEDs de uma rede com endereço fixo.
- Não permitir a reconfiguração dinâmica; isso leva a configurações de rede desconhecidas.
- Usar switches que forneçam o estado em tempo real da configuração da rede e do desempenho do tráfego.

VII. Sistema de Automação da Subestação

A. Componentes do Sistema de Automação da Subestação

O sistema de automação da subestação (SAS) de Kintampo inclui uma IHM para fornecer controle e indicação local dos componentes da subestação e uma unidade terminal remota (UTR) para fornecer dados do SCADA para a IHM local e centro de controle remoto da concessionária. A UTR executa a aquisição e controle dos dados dos IEDs da subestação via protocolo de comunicação MMS que faz parte da norma IEC 61850. A UTR fornece dados do SCADA remoto via protocolo de comunicação IEC 60870-5-104. O SAS de Kintampo possui vários recursos exclusivos, não comuns a um SAS típico, incluindo redundância quádrupla *hot-standby*, controle de acesso do usuário altamente personalizável, histórico das tendências dos dados de medição e recuperação automática do evento.

B. Redundância Hot-Standby

A maioria dos projetos SAS separa a UTR e a IHM em duas diferentes plataformas de hardware para o propósito de redundância no caso de falha de uma delas. Em Kintampo, a UTR e a IHM são instaladas dentro do mesmo pacote de software e localizadas na mesma plataforma de hardware, mas o software possui redundância quádrupla *hot-standby* incorporada. Existem quatro plataformas computacionais robustas para subestações no SAS de Kintampo, as quais são configuradas exatamente da mesma forma. As quatro instâncias de software transmitem constantemente entre si os respectivos estados através de um sinal *heartbeat* via Protocolo de Controle de Transmissão/Protocolo Internet ("Transmission Control Protocol/Internet Protocol" – TCP/IP). Em qualquer determinado instante, somente uma das quatro plataformas computacionais está efetuando ativamente o controle e a aquisição de dados. Quando a plataforma ativa tem uma falha de comunicação ou hardware, a próxima é automaticamente ativada e inicia a partir de onde a primeira parou. Para preservar a consistência e a coerência dos dados em todas as quatro plataformas computacionais, a mesma comunicação que fornece o sinal *heartbeat* também transmite quaisquer alterações nos dados para as outras três plataformas computacionais inativas. O software garante automaticamente que todas as quatro plataformas computacionais tenham a mesma configuração e dados.

C. Controle de Acesso

A subestação Kintampo é compartilhada por duas concessionárias separadas: Ghana Grid Company Limited (GRIDCo) e Northern Electricity Distribution Company (NEDCo). A GRIDCo opera a parte de transmissão da subestação e a NEDCo opera a seção de distribuição. Um dos requisitos do usuário consiste na capacidade de controle do acesso à IHM através de contas de usuário separadas para cada concessionária. O software da UTR e IHM suporta múltiplos usuários com direitos de acesso e credenciais exclusivas. A subestação Kintampo possui dois edifícios de controle, um para a distribuição e um para a transmissão, requerendo dois painéis *touchscreen* separados em cada edifício. O painel *touchscreen* do edifício de controle da distribuição é configurado para exibir automaticamente a parte de distribuição da IHM na inicialização, e o painel *touchscreen* do edifício de controle da transmissão é configurado para exibir automaticamente a parte de transmissão da IHM na inicialização. Quando os usuários efetuam o *login* na IHM de qualquer uma das telas, eles são solicitados a fornecer as credenciais de *login*. Os usuários de ambas as concessionárias podem visualizar ambas as seções da IHM, mas eles apenas estão aptos a efetuar operações na respectiva seção da subestação.

D. Tendências

O software da UTR e IHM suporta o histórico das tendências dos dados de medição e é configurado para amostrar e armazenar várias grandezas de medição, incluindo potência, corrente e tensão. Estes dados amostrados são armazenados no computador da subestação e salvos por 30 dias. Os grupos de dados ("datasets") históricos são circulares, baseados no método FIFO ("first in, first out"). O intervalo de amostragem e o período de retenção determinam

o tamanho dos arquivos. A IHM é configurada com gráficos personalizáveis para permitir a visualização e comparação dos dados que são armazenados em *datasets* históricos. Os usuários podem abrir múltiplos gráficos simultaneamente e editar os períodos de tempo que são exibidos nos gráficos. Os dados das tendências também podem ser importados dos arquivos de *datasets* para Microsoft® Excel® visando efetuar uma análise posterior usando um *plugin* do Microsoft Excel. Esses recursos das tendências consistem em ferramentas de grande utilidade ao efetuar uma tentativa de previsão dos requisitos de carga e fornecer aos usuários informações adicionais sobre o desempenho histórico do sistema.

E. Recuperação Automática do Evento

O SAS é equipado com um software que executa a recuperação automática dos registros de evento dos IEDs da subestação. Este software está instalado na mesma plataforma computacional robusta para subestações que contém a IHM e a UTR. Os registros dos eventos de proteção são registros históricos de múltiplas leituras de dados de múltiplas medições de sensores efetuadas antes, durante e após o disparo de um evento, tal como uma falta no sistema de potência. Este software efetua periodicamente a conexão via Telnet com todos os IEDs da subestação baseando-se no algoritmo *round-robin* em um intervalo configurável pelo usuário. O software armazena os arquivos dos registros de eventos no armazenamento local dos computadores da subestação e pode também ser configurado para armazenar os arquivos de eventos em servidores remotos. Embora a estação possua funcionários, este software de recuperação automática do evento permite que os operadores acessem o SAS e coletem todos os registros de evento para enviar ao departamento de engenharia. No futuro, esta coleta de informações pode ser automatizada e efetuada remotamente através desta aplicação de software.

VIII. Teste de Aceitação de Fábrica

Um teste de aceitação de fábrica foi efetuado em um ambiente de escritório visando fornecer aos usuários finais familiaridade com os equipamentos, testes e treinamento em um ambiente seguro. Devido à dimensão deste projeto e ao número de painéis de proteção e integração, um teste de aceitação de fábrica completo não era apropriado. Portanto, foi efetuada uma réplica da subestação em escala reduzida com um *bay* de transmissão completo incluindo a extremidade remota juntamente com um painel do transformador e dois painéis de 34 kV. Os usuários finais testemunharam o teste completo deste sistema reproduzido, permitindo que os engenheiros e os usuários finais testassem o sistema e efetuassem ajustes finais antes do transporte transoceânico.

Os simuladores dos disjuntores foram usados para simular a abertura e o fechamento dos disjuntores e MODs, e efetuar testes completos, verificando todas as lógicas e comunicações.

IX. Conclusão

Este artigo discute aspectos essenciais do projeto elétrico e projeto de proteção, controle e rede de comunicação de Kintampo. O trabalho demonstra que a utilização de quiosques de campo reduz significativamente a quantidade de fiação entre a casa de controle e o pátio. Até mesmo a fiação entre painéis foi enormemente reduzida usando mensagens GOOSE via IEC 61850 para partida e abertura através do esquema de falha de disjuntor. O projeto da rede foi escolhido de forma a fornecer redundância de rede, confiabilidade e controle de tráfego. A IHM local fornece aos operadores o controle e indicação local, proporcionando ao mesmo tempo o acesso remoto para os operadores do SCADA.

Em consequência de a aceitação das comunicações IEC 61850 pelas concessionárias estar aumentando, a adoção deste tipo de projeto em larga escala deverá também crescer. Assim como ocorre com os projetos *hardwired* completos, é necessário efetuar um projeto de engenharia especial nos estágios iniciais de um projeto de implementação de IEC 61850. Em particular, o projeto da arquitetura de rede é fundamental para garantir que o sistema possa suportar pontos únicos de falha dos equipamentos de rede e IEDs. Outro desafio que permanece consiste no treinamento adequado dos operadores que, no final, têm que responder rapidamente às emergências noturnas. Por exemplo, o teste de aceitação de fábrica provou ser inestimável, pois forneceu aos engenheiros e operadores um treinamento e familiaridade com novas tecnologias, tais como lógicas de teleproteção, LAN, desempenho e operação do sistema. Uma solução de sistema que é repetível, pré-projetada, pré-testada e desenvolvida de acordo com as especificações é extremamente importante, pois fornece ao usuário uma solução padronizada que pode ser implementada em todo o sistema, minimizando projetos diferentes.

X. Referências

[1] T. Tibbals and D. Dolezilek, "Case Studies: Replacement of Copper Field Wiring With Interoperable Digital Communications Over Fiber," proceedings of the GCC Power Conference, Doha, Qatar, October 2010.

[2] S. Kimura, A. Rotta, R. Abboud, R. Moraes, E. Zanirato, and J. Bahia, "Applying IEC 61850 to Real Life: Modernization Project for 30 Electrical Substations," proceedings of the 10th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2008.

[3] D. Dolezilek, N. Fischer, and R. Schloss, "Improvements in Synchronous Wide-Area Data Acquisition Design and Deployment for Telecontrol and Teleprotection," proceedings of the 14th Annual Western Power Delivery Automation Conference, Spokane, WA, March 2012.

XI. Biografias

Charles E. Anderson é Vice-Presidente de Engenharia da Meade Electric Company, Inc. Ele recebeu um BSEE da University of Notre Dame em 1980 e detém licenças de eletricista máster em sete Estados. Charles tem experiência na concepção, construção e comissionamento de usinas de geração de energia elétrica, subestações de alta tensão, sistemas de distribuição de energia de média tensão para ambas as instalações industriais e de concessionárias.

Salim Zniber ingressou na Schweitzer Engineering Laboratories, Inc. como engenheiro de proteção em 2010. Ele esteve envolvido em vários projetos na divisão de serviços engenharia, que fornece serviços de engenharia de proteção, automação e redes para clientes industriais e concessionárias. Salim trabalhou em projetos que incluem a engenharia, projeto e implementação de IEC 61850 e IEEE C37.118. Ele tem um BSEE e um MS em engenharia elétrica da University of North Carolina em Charlotte.

Youssef Botza recebeu seu BSEE da University of North Carolina em Charlotte com honras e atualmente trabalha como supervisor de engenharia na Schweitzer Engineering Laboratories, Inc. Ele tem vários anos de experiência em sistemas de potência, fornecendo soluções de proteção e automação e atuando como um líder técnico e gerente de projetos na divisão de serviços de engenharia. Youssef tem trabalhado em projetos de tecnologia de ponta, especializando-se em soluções IEC 61850. Ele é um engenheiro profissional registrado no estado da Carolina do Norte e membro do IEEE.

David Dolezilek recebeu seu BSEE da Montana State University é o diretor de tecnologia de pesquisa e desenvolvimento na Schweitzer Engineering Laboratories, Inc. Ele tem experiência em proteção, automação e integração de sistemas de potência, bem como em sistemas de comunicação, controle, SCADA e EMS. É autor de diversos artigos técnicos e continua a efetuar pesquisas em tecnologias inovadoras de interesse para nossa indústria. David é um inventor patenteado e participa de diversos grupos de trabalho e comitês técnicos. Ele é membro do IEEE, da IEEE Reliability Society, grupos de trabalho do CIGRE, e dois Comitês Técnicos da International Electrotechnical Commission (IEC) criados para abordar a segurança e padronização global de sistemas e redes de comunicação de subestações.

Justin McDevitt ingressou na Schweitzer Engineering Laboratories, Inc. como engenheiro de automação associado em 2010. Ele esteve envolvido em vários projetos na divisão de serviços engenharia, que fornece serviços e sistemas de engenharia de automação de subestações e SCADA para clientes industriais e concessionárias de sistema de potência. Justin é responsável pelo desenvolvimento de sistemas de automação, controle e redes, projeto de IHM, ajustes de processadores de comunicação, lógicas de relés e comunicações, e comissionamento. Ele trabalhou em vários projetos de automação de subestação via IEC 61850 com esquemas de proteção, automação e comunicação de alta complexidade. Ele tem um BS em engenharia de computação do Georgia Institute of Technology.