Segurança Através da Simplicidade em Sistemas Secundários Digitais

Joe Casebolt

INTRODUÇÃO

Sistemas secundários digitais distribuídos ampliam a fronteira digital além do limite tradicional da casa de controle para até os equipamentos primários no pátio da subestação. Realizando a conversão analógico-digital no ponto da medição e carregando essa informação digital através de cabeamento de fibra ótica pode criar um ambiente de trabalho mais seguro e diminuir os custos operacionais. Transferindo a informação digitalmente, níveis perigosos de tensão podem ser retirados da casa de controle. Custos de material podem ser minimizados pela troca de centenas de metros de cabos de cobre por um único cabo de fibra ótica, o que também reduz os requisitos de espaço físico nas canaletas. Custos com mão-de-obra podem ser reduzidos por menos trabalho em fazer canaletas, menos pontos de terminação da fiação e uma redução nas atividades de manutenção.

A Figura 1 mostra um projeto tradicional de uma subestação. Instalações modernas como a mostrada na Figura 2 dependem de tecnologias de comunicação e de equipamentos dedicados para digitalizar os dados e distribuí-los do ponto de medição até os dispositivos eletrônicos na casa de controle que realizam a proteção, controle e monitoramento. As tecnologias da IEC 61850 e Link no Domínio do Tempo (Time Domain Link - TiDL®) da SEL são duas opções disponíveis para estes tipos de serviço de comunicação. Este documento proporciona uma breve visão geral das duas tecnologias e avalia a postura em relação a cibersegurança de cada uma.

Figura 1 Projeto Tradicional de uma Subestação

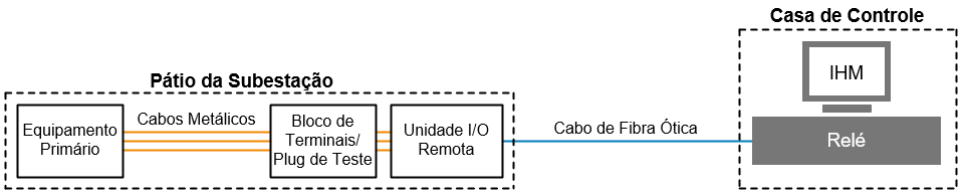

Figura 2 Projeto Moderno de um Sistema Secundário Digital

VISÃO GERAL DA TECNOLOGIA

Sistemas secundários digitais distribuídos requerem a comunicação de três tipos básicos de informação:

- Tempo — Sistema de sincronismo de tempo.
- I/O Discretos — Monitoramento e controle de I/O discretos.
- Entradas CA — Medições CA dos transformadores de instrumento.

O TiDL e a IEC 61850 abordam os quesitos de arquitetura de rede e métodos de comunicação para troca de informação de maneiras diferentes. O TiDL usa conexões privadas ponto-a-ponto com cada equipamento, enquanto a IEC 61850 usa uma rede Ethernet com switches. Além da diferença de arquitetura de rede, as duas tecnologias usam diferentes protocolos para comunicar os três tipos básicos de informação, como mostra a Tabela 1.

Tabela 1 Métodos de Comunicação

Tecnologia	Tempo	I/O Discretos	Entradas CA
IEC 61850	Não especificado (Precision Time Protocol [PTP] citado como o método preferido)	Generic Object-Oriented Substation Event (GOOSE)	Sampled Values (SV)
TiDL	EtherCAT®[1]	EtherCAT	EtherCAT

A solução TiDL utiliza uma conexão direta, ponto-a-ponto, entre o relé e o modulo I/O remoto, como mostrado na Figura 3.

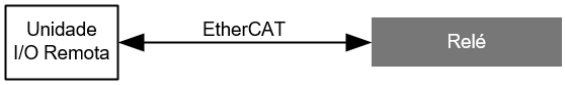

Figura 3 Sistema TiDL com uma única conexão I/O

Quando múltiplos módulos I/O são necessários, cada um se conecta isoladamente de maneira ponto-a-ponto com o relé, como mostra a Figura 4.

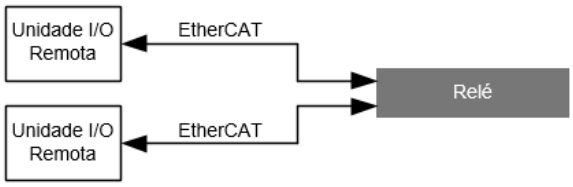

Figura 4 Sistema TiDL com múltiplas conexões I/O

[1] EtherCAT® é uma marca registrada e uma tecnologia patenteada, licensiada por Beckhoff Automation GmbH, Alemanha.

Uma solução IEC 61850 usa os mesmos tipos de equipamentos, mas também inclui um switch Ethernet e algum método de distribuir tempo para todos os equipamentos da rede (uma solução PTP é mostrada na Figura 5).

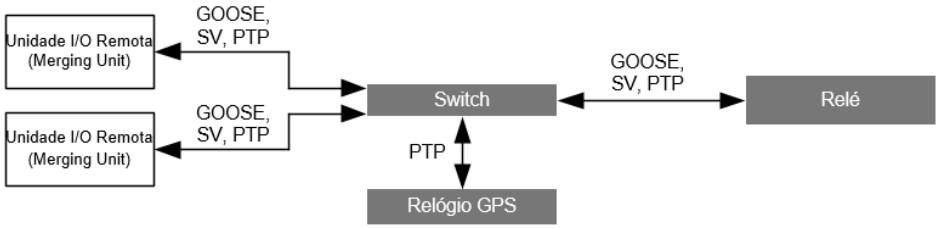

Figura 5 Solução IEC 61850 Simplificada

AVALIAÇÃO DE CIBERSEGURANÇA

Criptografia

Os sistemas TiDL e IEC 61850 estão localizados e comunicam dentro do Perímetro Físico de Segurança (PFS) e do Perímetro Eletrônico de Segurança (PES). Isso reduz a necessidade de criptografar a comunicação. Por mais que a criptografia reforce a robustez de uma solução de sistema secundário digital e pode ser usada para estabelecer a confiança entre máquinas, nenhuma das duas tecnologias têm segurança criptográfica (criptografia e autenticação) implementados em seus protocolos.

Simplicidade

A segurança tende a degrader-se à medida que os sistemas ficam mais complexos e interconectados. A simplicidade da tecnologia TiDL cria uma postura de segurança mais forte, se comparado com a solução IEC 61850, por reduzir o número de equipamentos que podem ser alvo de ataques, inerentemente restringindo acessos externos, limitando o número de protocolos que podem ser potencialmente explorados e eliminando a necessidade de uma fonte de tempo externa.

Equipamentos

Cada equipamento em uma rede é um potencial alvo de ataque. Reduzindo o número de tipos de equipamentos a serem gerenciados e protegidos, reduz-se a superfície de ataque. Cada tipo de equipamento do sistema necessita de sua própria avaliação de segurança. Ambas as soluções empregam relés e unidades de I/O remotas, mas a solução IEC 61850 também introduz switches e relógios GPS que requerem gerenciamento e avaliações de segurança próprios.

Acessibilidade

Ambas as tecnologias comunicam usando a Camada 2 do Modelo OSI (Open Systems Interconnection). Por conta do TiDL utilizar uma arquitetura ponto-a-ponto, o endereçamento MAC (Media Access Control) não é obrigatório, e as entidades em uma rede EtherCAT não precisam ter (e raramente têm) endereços MAC únicos. Isso impede que os sistemas TiDL sejam conectados a redes que usam switches, limitando, assim, a acessibilidade da comunicação ao acesso físico somente. A solução IEC 61850 usa o endereçamento MAC padrão para redes com switches. Para limitar a acessibilidade através dos switches, a solução requer que as portas e o acesso às portas sejam gerenciados por meio de políticas, projetos de rede e disciplina da engenharia.

Uma arquitetura IEC 61850 comum para limitar o acesso isola a comunicação do barramento de processos da comunicação do barramento de estação, como mostra a Figura 6.

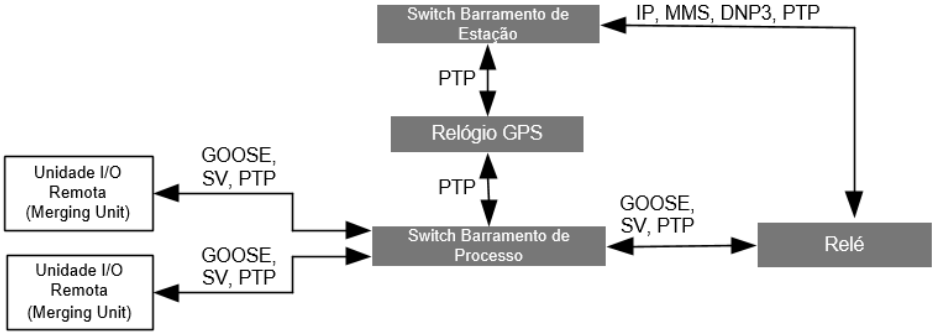

Figura 6 Topologia com o Barramento de Processos e o Barramento de Estação Separados

A comunicação do barramento de estação geralmente contém comunicações de Camada 3 que vão além da PFS e PES. Esses sistemas são projetados de modo que a comunicação com as unidades de I/O remotas através do barramento de estação é proibida.

Protocolos

A solução TiDL utiliza um único protocolo: EtherCAT. O protocolo EtherCAT é projetado para uso único e privado, onde outros protocolos não existem na rede. Isso torna a comunicação determinística por padrão, porque os pacotes EtherCAT são os únicos pacotes presentes na rede. A solução IEC 61850 inclui três protocolos independentes. Sistemas simples que usam somente GOOSE, SV, e PTP podem garantir a entrega dos dados baseado nos requisitos baixos de largura de banda. Redes Ethernet maiores e genéricas requerem integradores de sistemas para estudar alocação de banda e dependência de engenharia da solução.

Distribuição de Tempo

Em um sistema TiDL, o tempo é distribuído usando o protocolo EtherCAT. O tempo usado para sincronizar os sistemas TiDL é um sistema de tempo relativo distribuído pelo relé, não um tempo absoluto. Não é afetado por influências naturais externas (raios solares, por exemplo) ou influências potencialmente maliciosas (GPS spoofing, por exemplo) que podem afetar a confiabilidade do sistema.

A performance da solução IEC 61850 depende do sincronismo de tempo absoluto entre os equipamentos da rede. Isso coloca uma alta criticidade em como o tempo é distribuído dentro da rede. A operação das funções de proteção, controle e monitoramento depende da qualidade, confiabilidade e disponibilidade da distribuição de tempo. A IEC 61850 não especifica esses requisitos de tempo, somente diz que os dados devem conter uma estampa de tempo precisa.

Serviços da Porta

Minimizar os serviços e capacidades das portas dos equipamentos, reduz a superfície de ataque de uma solução. Somente serviços que contribuem para o sistema secundário digital devem estar disponíveis nas portas dos equipamentos. Para o TiDL, o EtherCAT é o único serviço disponível nas portas, devido ao seus requisitos de rede dedicados. Tipicamente, uma porta habilitada para a IEC 61850 é uma porta Ethernet comum, capaz de múltiplos serviços. Muitos fabricantes possibilitam que serviços nessas portas sejam desabilitados por software. Se isso for possível, fazê-lo é uma boa prática recomendada de segurança.

Regulamentação NERC CIP

Usuários comissionando tecnologias de comunicação de sistemas secundários digitais na América do Norte devem entender como essas soluções afetam sua conformidade com a North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP). Ambos, TiDL e IEC 61850, trazem novas comunicações digitais e equipamentos à equação. No momento, a Versão 5 do padrão NERC CIP é a corrente. A Versão 5 reconhece a distinção entre protocolos que operam na Camada 3 (camada de endereçamento IP) ou superiores e aqueles que operam na Camada 2. No NERC CIP, os equipamentos são categorizados como sendo com ou sem Comunicações Roteáveis Externas (External Routable Communication - ERC). "Routable communication" refere-se aos protocolos que usam a Camada 3 e superiores e são bidirecionais. "External" refere-se às conexões de comunicação que se encontram fora do PES. Um equipamento que se comunica na Camada 3 ou superiores com protocolos roteáveis bidirecionais para fora do PES da subestação é categorizado como sendo com ERC. Tais equipamentos estão sujeitos a diversos requisitos adicionais (acesso de usuário, autenticação, gerenciamento de atualizações e requisitos de log, para nomear alguns).

Para o TiDL, os equipamentos I/O remotos são inerentemente categorizados como sendo sem ERC. Para as soluções IEC 61850, o status ERC de um equipamento depende dos protocolos que ele suporta, assim como dos switches Ethernet e das outras conexões feitas com ele. Se um switch têm conexões para fora do PES que permitem tráfego de protocolos da Camada 3 e superiores, então o equipamento I/O remoto da IEC 61850 pode ser considerado como sendo com ERC. Entretanto, se eles são ou não está além do escopo desse documento, uma vez que a determinação depende do uso de pontos de acesso eletrônicos e se o acesso remoto interativo com esses nós remotos é possível. É recomendável que o tráfego da Camada 2 usado nas soluções IEC 61850 seja isolado das outras redes em uma subestação. Isso pode ser atingido pelo uso de switches fisicamente separados (barramento de estação e barramento de processos) ou pelo uso de tecnologias de redes definidas por software (SDN, sigla em inglês).

Qualquer outra comunicação com as unidades I/O remotas, tanto em soluções TiDL quanto em soluções IEC 61850, requerem uma avaliação de conformidade com a NERC CIP.

Sumário de Cibersegurança

Tabela 2 mostra um comparativo dos fatores de cibersegurança para avaliar essas duas soluções para um sistema secundário digital,

Tabela 2 Comparação das Tecnologias

Atributos	TiDL	IEC 61850
Topologia de Rede	Ponto-a-ponto	Com Switch
Camada do Modelo OSI	Camada 2	Camada 2
Segurança Inerente (Criptografia e Autenticação)	Não	Não
Compatível com o Endereçamento MAC 802.1*x*	Não	Sim
Módulos I/O Remotos com ERC	Não	Depende do fabricante e da aplicação
Número de Protocolos	1	3
Suporte para Outros Protocolos na Rede	Não	Sim

Número de Tipos de Equipamentos	2	4
Sincronismo de Tempo	Inerente	Projetado
Determinismo Inerente do Frame	Sim	Não

CONCLUSÕES

Mais equipamentos, mais conexões e mais protocolos significam mais engenharia, maior potencial de falha, mais pontos de acesso para um ataque, mais testes, mais atualizações e postura geral de segurança diminuída. A simplicidade da solução TiDL e o fato de ter uma rede dedicada se destacam na avaliação de cibersegurança. Soluções IEC 61850 podem ser seguras controlando-se o acesso via redes separadas e via tecnologias emergentes, como as redes definidas por software (SDN), que garantem confiabilidade e comunicação dedicada. Com a variedade de soluções de sistemas secundários digitais crescendo, a principal preocupação é que sistemas críticos não podem ser construídos sobre redes de comunicação genéricas. Uma solução para um sistema de proteção precisa assumir completa responsabilidade sobre todos os aspectos de operação.

BIOGRAFIA

Joe Casebolt é o vice-presidente de pesquisa e desenvolvimento de sistemas de potência na Schweitzer Engineering Laboratories, Inc. (SEL). Ele se formou bacharel em Engenharia da Computação na Universidade de Idaho em 2001. Ele ingressou na SEL em 2001, e sua experiência inclui projeto de sistemas embarcados, cibersegurança, protocolos e soluções de controle e automação. Atualmente Joe possui diversas patentes na área de processamento digital de sinais e comunicação.

SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 USA
Tel: +1.509.332.1890 • Fax: +1.509.332.7990
www.selinc.com • info@selinc.com

LWP0021-01