Implicações Técnicas e de Segurança Cibernética da Perda de Sinal GPS em Sistemas de Controle de Energia Elétrica no Brasil

Marcelo Ayres Branquinho
CEO da TI Safe

19/07/2025

Resumo

A sincronização temporal precisa é um pilar fundamental para a operação segura e eficiente de sistemas SCADA em infraestruturas críticas, como o setor de energia elétrica. O sinal GPS, amplamente utilizado como fonte de tempo universal, desempenha um papel vital na coordenação de eventos, medições fasoriais, atuação de relés de proteção e registro de logs e alarmes. A perda deste sinal pode resultar em descompassos operacionais que afetam diretamente a confiabilidade da rede elétrica, podendo inclusive levar a interrupções no fornecimento de energia.

Além das questões operacionais, essa perda apresenta riscos significativos à segurança cibernética, ao comprometer a integridade de mecanismos como firewalls industriais, sistemas de detecção de intrusão (IDS/IPS), plataformas de análise e resposta (SIEM/SOAR) e os próprios Centros de Operações de Segurança (SOCs). Sem tempo confiável, torna-se impossível correlacionar eventos, reconstruir linhas do tempo de ataques e reagir em tempo hábil a incidentes.

Este artigo explora detalhadamente os impactos técnicos e de segurança decorrentes da ausência do GPS, destacando implicações nos processos operacionais, nos mecanismos de defesa e na conformidade com normas como a IEC 62443, NIST SP 800-82r3 e a RO-CB.BR.01 do ONS. São abordadas também estratégias de mitigação como o uso de PTP, relógios internos de alta precisão, segmentação da rede e testes de resiliência. Ao final, conclui-se que a dependência do GPS deve ser considerada um vetor estratégico de risco cibernético, cuja mitigação demanda integração entre engenharia de controle, arquitetura de redes e segurança da informação em ambientes industriais.

Palavras-chave

GPS, SCADA, Segurança Cibernética, ICS, IEC 62443, SIN, SOCs Industriais, Tempo Sincronizado

1. Introdução

Em infraestruturas críticas, como os sistemas de controle de energia elétrica, a sincronização temporal é um elemento essencial para a operação segura e eficiente da rede. O corte súbito ou prolongado do sinal GPS pode gerar impactos profundos em sistemas SCADA (Supervisory Control and Data Acquisition), os quais são dependentes de marcações de tempo precisas para monitorar, correlacionar eventos e acionar comandos de controle distribuído. A questão que se impõe é: até que ponto um corte de sinal GPS pode comprometer a integridade operacional do setor elétrico a ponto de causar interrupções no fornecimento de energia? A resposta, embasada em normas técnicas e experiências internacionais, é que sim, os efeitos podem chegar a este nível de gravidade.

2. Dependência do GPS em Sistemas Elétricos

A infraestrutura elétrica moderna depende do GPS como fonte primária de tempo sincronizado, que é distribuído por toda a rede operacional. Dispositivos como PMUs (Phasor Measurement Units) utilizam a marcação temporal baseada em GPS para calcular ângulos de fase com alta precisão, sendo fundamentais para o monitoramento da estabilidade de sistemas interligados. IEDs (Intelligent Electronic Devices) e relés de proteção utilizam essa sincronização para detectar e isolar falhas com precisão.

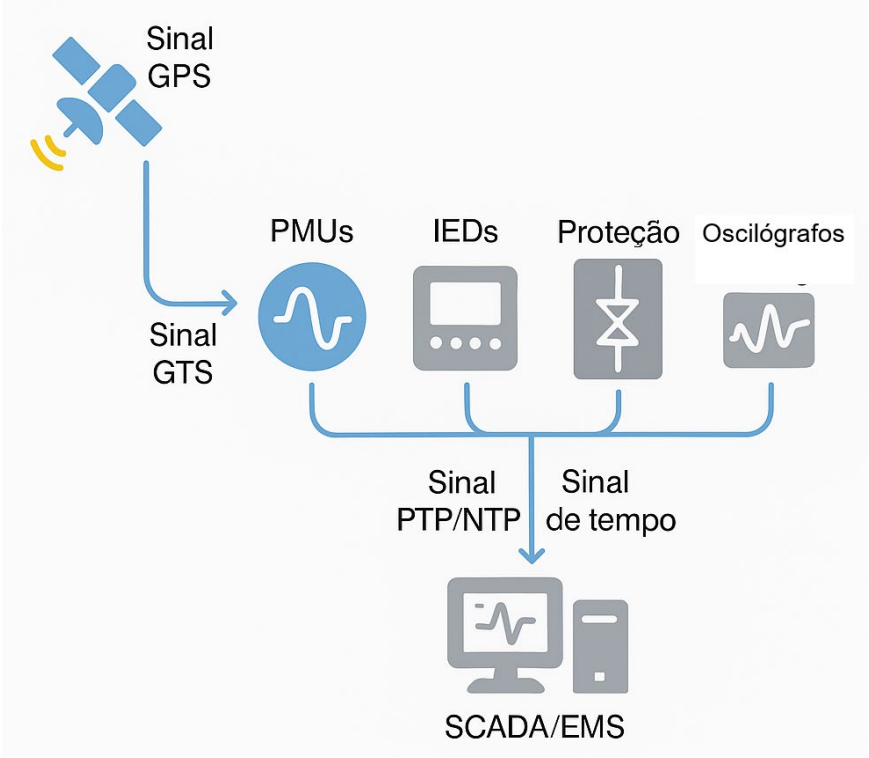

Figura: Arquitetura do Tempo em Sistemas SCADA

Oscilógrafos digitais e registradores de eventos dependem do tempo GPS para gerar registros confiáveis e auditáveis. Os servidores SCADA e EMS também baseiam sua ordenação de eventos em timestamps originados de GPS, o que permite correlações temporais essenciais para a operação coordenada da rede.

3. Impactos Técnicos da Perda de GPS

Se o sinal GPS for interrompido, os dispositivos começam a operar com osciladores internos que, com o passar do tempo, se tornam imprecisos, provocando defasagens nas leituras de ângulo de fase e dificultando ou impossibilitando a detecção de oscilações de potência, ressonância subsíncrona e outros distúrbios elétricos. Nos sistemas de proteção, como os relés diferenciais ou de distância, a temporização exata de eventos entre subestações distintas é fundamental para determinar a localização e a severidade de falhas. A perda dessa capacidade pode levar a falsas atuações, falhas de atuação ou sobreposições indevidas, aumentando significativamente o risco de desligamentos não planejados ou em cascata.

Além disso, os servidores SCADA e EMS, responsáveis por coletar e correlacionar dados de milhares de pontos de medição em tempo real, dependem do tempo sincronizado para ordenar eventos, gerar alarmes e emitir comandos de controle baseados em lógicas temporais. A inconsistência nos timestamps compromete a integridade dos logs, das análises forenses, da resposta a incidentes e do controle remoto coordenado. No caso de redes que operam com topologias complexas, como em sistemas interligados nacionalmente (exemplo: SIN no Brasil), a perda de GPS pode inviabilizar a coordenação de manobras, como o reestabelecimento de blocos ilhados, o black-start ou o balanceamento automatizado de carga e geração.

4. Consequências para a Segurança Cibernética

Diversas normas técnicas reconhecem o risco da perda do GPS em ambientes operativos. O guia NIST SP 800-82r3, referência em segurança para sistemas OT (Operational Technology), identifica a perda de temporização precisa como uma ameaça crítica que pode comprometer diretamente a disponibilidade, integridade e confiabilidade de sistemas de controle industrial. Já a norma IEC 61850, que trata da comunicação em subestações, e sua aplicação em conjunto com a IEC 62443 para segurança cibernética, pressupõem a existência de uma infraestrutura de tempo confiável para sincronização de eventos GOOSE e Sampled Values.

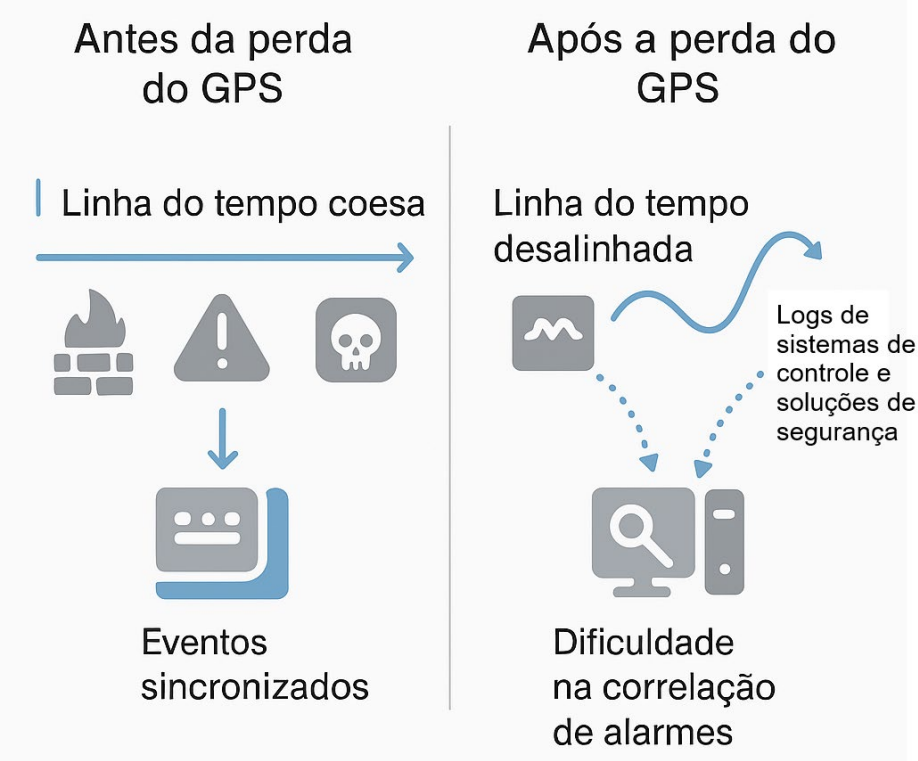

Figura: Impacto da perda de sincronismo na detecção de incidentes

As soluções de segurança cibernética para ambientes industriais também são severamente impactadas pela perda de temporização precisa. Sistemas como firewalls industriais, IDSs e plataformas SIEM usam o tempo

para analisar padrões de tráfego, identificar desvios comportamentais e correlacionar alertas de múltiplas fontes.

Sem GPS, os registros perdem consistência temporal, dificultando ou impossibilitando a correlação de eventos e a identificação de campanhas de ataque em andamento. O SOC (Security Operations Center), responsável por centralizar essas informações e reagir a incidentes, torna-se incapaz de determinar com exatidão a ordem dos eventos, o que compromete a eficácia da resposta. Além disso, ataques com foco em exploração de janelas de tempo, como spoofing de NTP ou replay de comandos legítimos fora de horário, tornam-se mais difíceis de detectar. A integridade das trilhas de auditoria também fica prejudicada, afetando não só a segurança, mas também a conformidade com normativas como IEC 62443, NIST SP 800-82r3 e as exigências da RO-CB.BR.01.

5. Mitigações Recomendadas

A mitigação da dependência do GPS deve ser tratada como prioridade estratégica na arquitetura de segurança de sistemas industriais.

Uma abordagem comum envolve a implementação do Precision Time Protocol (PTP IEEE 1588v2), capaz de fornecer sincronização precisa via rede interna, independentemente do GPS. Servidores NTP internos alimentados por relógios de rubídio ou osciladores de alta estabilidade (OCXO) oferecem fonte de tempo confiável por longos períodos, mesmo em ausência do GPS.

Além disso, mecanismos de monitoramento de integridade temporal devem ser implementados, com alertas em caso de divergência ou spoofing de sinal. A rede deve ser segmentada de forma a conter falhas locais de tempo, mantendo operações mínimas em zonas independentes. Testes regulares, incluindo simulações de perda de GPS, devem ser conduzidos para avaliar a capacidade dos sistemas e do SOC de operarem em modo degradado. Esses testes devem incluir análise forense, tempos de detecção e eficácia da resposta.

6. Conclusão

A dependência do GPS para sincronização temporal em ambientes industriais é um ponto crítico que afeta tanto a operação técnica quanto a segurança cibernética das infraestruturas. A perda desse recurso pode levar a falhas coordenadas de proteção, perda de visibilidade situacional, incapacidade de resposta a incidentes e violações de conformidade regulatória.

Diante desse cenário, é fundamental que organizações do setor elétrico e demais operadores de infraestrutura crítica adotem medidas proativas para garantir resiliência temporal, diversificando suas fontes de tempo e testando suas arquiteturas para cenários de falha.

A TI Safe, através de sua metodologia ICS.SecurityFramework®, tem atuado junto a operadores e agentes regulados para implementar soluções que permitam a continuidade das operações e a manutenção da segurança, mesmo na ausência de sinal GPS. Esta abordagem integrada entre engenharia, segurança da informação e operação deve ser considerada modelo de referência para o enfrentamento dos desafios de segurança cibernética em um cenário de crescente interdependência entre ativos físicos e digitais.