Sistemas de Informação e Telecomunicação para Sistemas Elétricos

19 a 22 de outubro de 2025

RELATÓRIO ESPECIAL PRÉVIO

RODRIGO LEAL DE SIQUEIRA
Yona Lopes, Rodrigo Leal de Siqueira, Diogo Guimarães Alves

1.0 CONSIDERAÇÕES GERAIS

De forma geral este ano tivemos temas de interesse com foco em Inteligência Artificial (IA), conectividade com soluções em 5G, MPLS, satélites e outras tecnologias, e em cibersegurança.

O setor caminha na direção da digitalização, orientada por inovações tecnológicas, com a IA assumindo papel central nesse processo como vetor de eficiência. Observa-se que a IA tem sido empregada não apenas como uma ferramenta de automação, mas como um meio de aprimorar processos críticos, auxiliando a operação, a manutenção e a proteção do Sistema Elétrico.

A crescente adoção da IA no desenvolvimento de modelos preditivos que incorporam, de forma simultânea, as etapas de previsão e decisão é uma observação importante. Essa abordagem pode representar uma evolução significativa, permitindo que os sistemas operem de maneira mais alinhada às condições reais do sistema elétrico. Seja na identificação de anomalias operativas, na previsão de comportamentos de ativos ou na melhoria dos tempos de atuação de equipamentos críticos, a IA se mostra uma tendência de aborda estratégica para apoiar as decisões no setor.

Outro ponto importante observado é o fortalecimento das discussões e práticas relacionadas à segurança cibernética aplicada às infraestruturas críticas do setor elétrico. Nesse contexto, destaca-se também o surgimento de soluções de IA aplicadas à cibersegurança, tanto no monitoramento quanto na detecção de ameaças, evidenciando uma tendência de integração entre tecnologia operacional (TO) e inteligência artificial

Observa-se que embora haja avanços significativos, ainda persistem desafios expressivos, especialmente no que tange à proteção de ambientes que operam com sistemas legados, gestão de vulnerabilidades e integração segura de novas tecnologias como redes 5G privadas, IoT e sistemas de automação cada vez mais interconectados.

Um tema bem explorado tem sido no avanço e aplicações concretas da tecnologia 5G. O 5G é visto como alicerce essencial para a modernização das redes elétricas e existe um movimento de avaliação técnica e econômica comparando 5G com outras tecnologias sem fio (LTE, WiFi6).

Um abordagem importante mas que não foi observado nos trabalho é práticas mais efetivas unindo equipamentos reais de subestações como IEDs e rede reais de operadoras 5G.

2.0 - Classificação dos Informes Técnicos

De forma geral este ano tivemos temas de interesse com foco em Inteligência Artificial (IA), conectividade com soluções em 5G, MPLS, satélites e outras tecnologias, e em cibersegurança.

O setor caminha na direção da digitalização, orientada por inovações tecnológicas, com a IA assumindo papel central nesse processo como vetor de eficiência. Observa-se que a IA tem sido empregada não apenas como uma ferramenta de automação, mas como um meio de aprimorar processos críticos, auxiliando a operação, a manutenção e a proteção do Sistema Elétrico.

A crescente adoção da IA no desenvolvimento de modelos preditivos que incorporam, de forma simultânea, as etapas de previsão e decisão é uma observação importante. Essa abordagem pode representar uma evolução significativa, permitindo que os sistemas operem de maneira mais alinhada às condições reais do sistema elétrico. Seja na identificação de anomalias operativas, na previsão de comportamentos de ativos ou na melhoria dos tempos de atuação de equipamentos críticos, a IA se mostra uma tendência de aborda estratégica para apoiar as decisões no setor.

Outro ponto importante observado é o fortalecimento das discussões e práticas relacionadas à segurança cibernética aplicada às infraestruturas críticas do setor elétrico. Nesse contexto, destaca-se também o surgimento de soluções de IA aplicadas à cibersegurança, tanto no monitoramento quanto na detecção de ameaças, evidenciando uma tendência de integração entre tecnologia operacional (TO) e inteligência artificial

Observa-se que embora haja avanços significativos, ainda persistem desafios expressivos, especialmente no que tange à proteção de ambientes que operam com sistemas legados, gestão de vulnerabilidades e integração segura de novas tecnologias como redes 5G privadas, IoT e sistemas de automação cada vez mais interconectados.

Um tema bem explorado tem sido no avanço e aplicações concretas da tecnologia 5G. O 5G é visto como alicerce essencial para a modernização das redes elétricas e existe um movimento de avaliação técnica e econômica comparando 5G com outras tecnologias sem fio (LTE, WiFi6).

Um abordagem importante mas que não foi observado nos trabalho é práticas mais efetivas unindo equipamentos reais de subestações como IEDs e rede reais de operadoras 5G.

2.1 - Tecnologias Emergentes de telecomunicações e tecnologia da informação - 4
2.2 - Aplicações de novas tecnologias e soluções nos sistemas de tecnologia da informação e telecomunicação - 7
2.3 - Aplicações de Internet das Coisas (IoT) - 1
2.4 - Uso de Inteligência Artificial para Sistemas Elétricos - 6
2.5 - Segurança Cibernética - 6
2.6 - Aspectos de inovação na manutenção e operação dos sistemas de informação e telecomunicações - 6

- Sistema de Visão Computacional Tridimensional Baseado em IA para Prevenção de Acidentes em Manutenção de Redes de Transmissão e Distribuição de Energia
- Ferramenta baseada em Inteligência Artificial para gestão da manutenção e operação de ativos de telecomunicações. Estudo de Caso de detecção de falhas no processo de Inspeção de Torres de Telecomunicações.
- Método DCT-Bootstrap para detecção de falhas em unidades geradoras
- Estruturação de Telecom e SPCS para atendimento do projeto SEP N-NE-SE
- Orquestrador multimodelos para manutenção preditiva em usinas hidrelétricas.
- Desafio da manutenção da disponibilidade do sistema de telecomunicações durante a crise Enchentes RS

- Avaliação de Inteligência Artificial com Mecanismo de Atenção na Detecção de Ataques de Injeção de Dados Falsos em Sistemas de Potência
- Estudos de cibersegurança utilizando plataforma de simulação ciberfísica.
- Aplicação de um Modelo de Análise de Ferramentas de Segurança Cibernética no Projeto de Atualização da Subestação da Margem Direita da ITAIPU Binacional
- Repositório de incidentes de segurança cibernética para investigação de ameaças no setor elétrico
- Solução de segurança de rede em um Sistema Especial de Proteção de grande porte: SEP das Interligações Norte-Nordeste-Sudeste
- Cibersegurança para Hidrelétricas: Desafios e Soluções Atuais, Envolvendo Estudos de Caso

- Aplicação de Técnicas de Inteligência Artificial na Estratégia Adaptativa como ferramenta para superar desafios na Proteção do Sistema Elétrico de Potência
- Uso de Modelos não supervisionados para redução de falsos positivos em modelos de predição de falhas e de digital Twins em Hidrogeradores
- ApplicationDrivenLearning.jl: Uma Biblioteca de Alto Desempenho para Treinamento de Modelos Preditivos no Contexto de Tomada de Decisão
- Uso de Inteligência Articial (IA) para Identificação dos Tempos Envolvidos nas Manobras de Disjuntores a SF6 da Subestação de Tijuco Preto
- Aplicação de Inteligência Artificial para Detecção de Intrusões e Anomalias em Tempo Real em Sistemas de Controle Industrial
- ChatDGA - Uma ferramenta contextual para auxílio no aprendizado técnico e análise dos resultados do ensaio DGA

- Experiência da EVOLTZ no desenvolvimento de ferramenta para monitoramento e aumento da resiliência de Linhas de transmissão através de IoT

- Implantação de novo ambiente de Software Defined Datacenter (SDDC) para Sistemas de Tecnologia da Automação da Itaipu Binacional.
- Cibersegurança nas mensagens GOOSE: estratégias para mitigação de riscos
- Transformação Digital no Centro de Operações da ISA Energia Brasil: Integração de IA e SCADA para eficiência, agilidade e segurança ao consultar Documentos Operativos em Tempo Real
- Redes MPLS-TP: Resiliência com Hitless Switching para Teleproteção
- Utilização prática de sensoreamento de efeitos não-lineares em fibras ópticas: Estudo de Caso das aplicações em suporte à vigilância patrimonial, operação de equipamentos elétricos, monitoramento de redes locais e remotas e outras aplicações em subestações.

- Estudo comparativo de novas tecnologias de comunicação sem fio para empresas do setor elétrico. Análise técnica e econômica sobre aplicações do WiFi6, LTE e 5G para a atual demanda de serviços.
- Realidade Virtual e Gestão de Ativos, suportadas por modelagem granular aderente a Sistemas HVDC

- Desenvolvimento de Ferramenta de Transcrição Automatizada Bilíngue para Suporte à Operação de Itaipu
- Um Sistema para Recuperação de Informações e Reconstrução Topológica de Diagramas Unifilares utilizando Visão Computacional e Aprendizado Profundo
- Uso de Infraestrutura 5G e Edge Computing para Implementação de IA na Prevenção de Falhas em Redes de Distribuição de Energia
- Análisis comparativo del comportamiento de las funciones de misión crítica diferencial de línea y tele protección usando tecnologías de comunicación SDH vs MPLS-TP

3.0 - Relatório sobre os Informes Técnicos

Título - Desenvolvimento de Ferramenta de Transcrição Automatizada Bilíngue para Suporte à Operação de Itaipu
Entidade(s) - Fundação Parque Tecnológico Itaipu - Brasil,ITAIPU BINACIONAL,Itaipu Binacional,ITAIPU Binacional
Autor(es) - Jhoan Rodrigo Pérez Vargas,Guilherme Zat,Isabela Aguiar Dias,Vinicius de Oliveira Jimenez,Hilton Carlos Miranda Lessa,Filipe Ventura Muggiati,Fernando Enrique Villalba,Ramón Andrés Cardozo
Resumo
A operação da Usina Hidrelétrica de Itaipu envolve diversas equipes que gerenciam, em tempo real, os sistemas elétricos brasileiro e paraguaio, em meio a um elevado volume de estímulos visuais e sonoros. Esse cenário dificulta a leitura de documentos e a busca por informações em gravações telefônicas durante as atividades de supervisão e controle da usina e das subestações. Nesse contexto, este trabalho apresenta os resultados parciais do desenvolvimento de uma ferramenta computacional que realiza a transcrição automática bilíngue, com o objetivo de incorporá-la a uma aplicação piloto que será integrada às soluções de supervisão e comunicação já existentes. A meta é reduzir o esforço cognitivo dos operadores e aprimorar a consciência situacional, contribuindo para uma operação mais ágil.
Perguntas e Respostas

Apesar da proposta do trabalho ser melhorar a consciência situacional e reduzir esforço cognitivo dos operadores, não houve validação empírica, mesmo preliminar, com usuários reais da aplicação Todos os resultados são baseados em métricas automatizadas (WER e SER), sem menção a testes com usuários ou feedback qualitativo. Foi planejada uma etapa de validação com operadores ou pelo menos entrevistas para avaliar usabilidade, compreensibilidade e impacto real na operação?
A observação é muito pertinente. É fundamental distinguir o escopo do nosso projeto da aplicação final que será desenvolvida.
O objetivo central do nosso trabalho é entregar a tecnologia de base, ou seja, uma

API de transcrição robusta e um ecossistema que permita a sua avaliação e evolução contínua. Os resultados que apresentamos, baseados em métricas como WER e SER, validam a performance técnica desta tecnologia.
No entanto, reconhecemos que a validação do impacto em fatores humanos, como a melhoria da consciência situacional e a redução do esforço cognitivo, depende diretamente da forma como essa tecnologia será integrada à rotina dos operadores. Para viabilizar essa etapa futura, que caberá à Itaipu conduzir, nosso projeto contempla duas frentes:

- Ferramentas para Validação: Conforme planejado, desenvolveremos uma aplicação web de referência e uma API com funcionalidades específicas para a validação com usuários. Isso inclui um módulo de feedback qualitativo, no qual os operadores poderão revisar, pontuar e corrigir as transcrições em um ambiente controlado. Esses são os recursos que permitirão à Itaipu medir o impacto da ferramenta na operação.
- Melhoria Contínua do Modelo: Paralelamente, estamos criando um ambiente para o treinamento incremental dos modelos. Esse sistema será alimentado por novos áudios e, crucialmente, pelos áudios que receberem menor avaliação dos operadores, criando um ciclo de feedback que refina progressivamente a precisão do sistema.

Em resumo, nosso projeto entrega a API com os mecanismos e as ferramentas necessárias para a avaliação de usabilidade e impacto. A condução dos testes empíricos para quantificar especificamente a melhoria na consciência situacional e a redução do esforço cognitivo será uma etapa posterior, de responsabilidade da Itaipu, ao integrar a API na aplicação final utilizada por seus operadores.

O trabalho utiliza WER (Word Error Rate) e SER (Sequence Error Rate) como métricas de desempenho. Embora essas sejam métricas padrão para ASR, elas podem falhar em transcrever nomes de equipamentos, comandos operacionais ou nomes de operadores — informações que têm peso desproporcional no contexto elétrico. Vocês pensaram em utilizar outras métricas, com ênfase em vocabulário técnico, baseada em termos ou semanticas próprias?
Reconhecemos que métricas como WER e SER, embora indispensáveis para benchmarking geral, são agnósticas ao contexto e podem mascarar erros críticos. Um erro na transcrição de um artigo ou preposição tem o mesmo peso de um erro no nome de um disjuntor, o que não reflete o impacto real na operação da Itaipu.
Para endereçar essa lacuna, nosso plano de trabalho já inclui o desenvolvimento de uma métrica complementar, inspirada em abordagens da literatura para avaliação de ASR em domínios críticos.
A solução que estamos desenvolvendo é a implementação de um WER Ponderado por Criticidade. O conceito é definir, em conjunto com a equipe da Itaipu, um vocabulário crítico, incluindo nomes de equipamentos, verbos de comando, siglas e operadores, e atribuir um peso de penalidade maior para erros (substituição, inserção ou deleção) que ocorram nesses termos.
Por exemplo, um erro na palavra "desligar" ou no nome de uma unidade geradora teria um impacto na métrica final significativamente maior do que um erro em uma palavra de conexão, como "o" ou "para".
A adoção desta métrica nos permitirá direcionar o ajuste fino do modelo, focando especificamente nos erros de maior impacto para a operação. Como o desenvolvimento de uma métrica customizada é um desafio técnico, estamos

atualmente na fase de estudo e prototipação, mas este é o caminho que se mostrou mais promissor para uma avaliação verdadeiramente alinhada às necessidades da Itaipu.

Embora o resumo e a conclusão mencionem possível integração com soluções de supervisão e comunicação, o corpo do trabalho não apresenta detalhe técnico ou arquitetural sobre como essa integração será feita, se haverá API, quais requisitos da arquitetura atual precisam ser respeitados ou como serão tratadas questões de segurança — que são essenciais em sistemas de controle em tempo real. Vocês já definiram a arquitetura de integração?
A arquitetura para a solução adotará uma arquitetura modular, conforme foi definido e documentado no projeto. Dentre os módulos que serão desenvolvidos estão duas aplicações web e duas APIs:

- API IVO: responsável pela autenticação, roteamento e integração com os demais sistemas da Itaipu e demais módulos desenvolvidos;
- API STT/TTS: dedicada aos modelos de inteligência artificial, especialmente, os modelos de STT e TTS, possibilitando a transcrição e a síntese de fala;
- IVO web: aplicação web na qual os usuários poderão realizar as transcrições e sínteses de fala;
- Aplicação de treinamento: aplicação web para iniciar treinamentos de novos modelos de STT, gestão das novas versões geradas e visualização de todos os áudios transcritos pelo sistema.

Os endpoints da API IVO serão disponibilizados exclusivamente via protocolo HTTPS, garantindo maior segurança à aplicação. Toda a documentação das rotas será fornecida através do OpenAPI, permitindo que os usuários visualizem claramente os parâmetros de entrada e saída de cada endpoint.
As principais rotas públicas disponíveis para qualquer usuário da Itaipu são:

- GET /audios/conversions/mp3 – converte áudios da web para o formato MP3;
- GET /versions/approved – retorna as versões aprovadas de modelos treinados;
- GET /stt – realiza a transcrição de áudios;
- GET /tts – realiza a síntese de fala.

A arquitetura permite que cada módulo funcione de forma independente e segura, usando autenticação com Keycloak, armazenamento em SQL Server e MinIO, e execução por containers com Podman.

Título - Um Sistema para Recuperação de Informações e Reconstrução Topológica de Diagramas Unifilares utilizando Visão Computacional e Aprendizado Profundo
Entidade(s) - Centro de Pesquisas de Energia Elétrica CEPEL, Evoltz Participações S.A.,CENTRAIS ELÉTRICAS BRASILEIRAS S. A.,CENTRAIS ELETRICAS BRASILEIRAS SA ELETROBRAS
Autor(es) - Victor Navarro Araujo Lemos, Luiz Fernando dos Reis de Oliveira, João Victor Daher Daibes, Rodrigo Lopes de Moraes, Angelo Andelnyr Sampaio Alves, LEVI CIRQUEIRA SANTOS JUNIOR
Resumo

Algumas das informações essenciais para as atividades de empresas do setor elétrico são usualmente descritas na forma de diagramas unifilares. Apesar disso, não estão disponíveis meios práticos de interpretá-los de forma automatizada e fatores como a complexidade das instalações representadas e a falta de padrão nos símbolos utilizados para representação dos componentes elétricos entre empresas e mesmo em uma única empresa, tornam a intervenção humana necessária e laboriosa.

Para abordar adequadamente a complexidade dos diagramas unifilares e transformá-los em descrições computacionais precisas, este artigo apresenta uma ferramenta que oferece um sistema avançado de análise e reconstrução de diagramas utilizando uma combinação de técnicas de aprendizado profundo, visão computacional e métodos convencionais de processamento de imagem. Este sistema tem foco no consumo por técnicos e engenheiros do setor elétrico, proporcionando uma solução abrangente.

Para a validação da aplicação, utilizamos diagramas de empresas do setor (Evoltz e Eletrobras), alcançando altos índices de precisão mesmo em diagramas complexos com muitos elementos. Provisionada de forma conveniente e compartimentalizada, servida como aplicação web, a aplicação visa integrar a digitalização de diagramas unifilares com sistemas supervisórios e de controle, otimizando processos e melhorando a eficiência operacional das empresas do setor elétrico.

O resultado obtido possibilitará, por exemplo, a utilização dos dados gerados pela plataforma na configuração de base dados SCADA e EMS (Energy Management Systems) e na geração de telas unifilares para sistemas de automação e controle entre outras aplicações.

Perguntas e Respostas

Porque o sistema é caracterizado como um framework? Isto é, o que o diferencia?

Caracterizamos o trabalho como um framework pois ele consiste em uma série de etapas conceituais que, em execução conjunta, são capazes de resolver o problema de extração de informação relevantes provenientes das imagens de diagramas unifilares. O ferramental utilizado na implementação é, em princípio, apenas uma das possíveis instâncias a serem utilizadas. Por exemplo, a etapa de OCR consiste na localização dos textos e seus conteúdos. As técnicas utilizadas para realizar esse procedimento podem ser adaptadas a depender do contexto e do desejo do utilizador. Ao buscar a implementação da solução, exploramos diversas técnicas que realizavam este procedimento e, ao final, encontramos um método em específico que atingiu a eficácia esperada. O mesmo se estende aos demais elementos descritos.

O sistema conta com uma interface gráfica de edição e visualização como etapa central do processo (semiautônomo), porém não há avaliação de usabilidade, desempenho da aplicação web (latência, escalabilidade) ou testes com usuários. Como essa etapa é essencial para validação final dos resultados, vocês pensaram em incluir testes de usabilidade ou, ao menos, coleta de feedback com usuários reais para identificar pontos de melhoria?

Agradecemos pela observação. De fato, reconhecemos que a interface gráfica desempenha um papel relevante no processo semiautônomo proposto.

No entanto, como o foco principal deste trabalho foi demonstrar a viabilidade da solução para um cenário específico — com uso inicial restrito a equipes técnicas

responsáveis pela configuração de sistemas SCADA/EMS — optamos por não realizar testes formais de usabilidade ou avaliações de desempenho como latência e escalabilidade. A aplicação foi concebida para operar em ambientes com poucos usuários simultâneos, e, nesse contexto, mostrou-se adequada. Apesar disso, ela foi desenvolvida em ambiente conteinerizado, de forma que pode ser facilmente replicada e ter carga de trabalho balanceada.
Ainda assim, realizamos sessões de demonstração e posterior coleta de feedback com profissionais das equipes da EVOLTZ e da Eletrobras FURNAS. Essas interações foram fundamentais para identificar necessidades operacionais e orientar melhorias na interface, contribuindo diretamente para a versão apresentada.
Concordamos plenamente que uma etapa mais estruturada de testes com usuários finais será indispensável em fases futuras, especialmente se houver intenção de ampliar o escopo de uso da plataforma. Essa etapa permitirá não apenas validar a robustez da ferramenta frente a diferentes cenários, mas também aprimorar a experiência do usuário e a confiabilidade da solução.

Durante os testes da ferramenta, quais foram os principais erros cometidos pelo sistema na identificação de símbolos, textos ou conexões, e como esses erros impactam a confiabilidade da solução em contextos operacionais reais?
Os erros podem ser categorizados da seguinte forma:

- Erros provenientes da má elaboração ou má qualidade do diagrama (e.g. linhas descontinuadas, áreas demasiadamente hachuradas, baixa resolução do arquivo, panos de fundo com pouco contraste em relação ao diagrama)
- Erros de identificação de texto: há casos genéricos em que modelos de identificação de texto podem confundir caracteres que são suficientemente parecidos. Um exemplo básico é a diferenciação entre a letra O e o número 0. A depender da fonte utilizada, a distinção fica prejudicada até mesmo para um utilizador humano que não tenha contexto a respeito da forma de nomear as entidades no diagrama. A correção deste problema envolveu a utilização de um arquivo que mapeava os textos existentes nos diagramas e uma série de técnicas para explorar um espaço de strings vizinhos em busca do texto correto.
Além disso, havia problemas de tamanho da fonte em instalações mais complexas com valores de fonte abaixo de 8pt. Tamanhos pequenos prejudicam bastante a identificação do texto e nos obrigou a desenvolver técnicas para aprimorar a sua precisão que funcionaram muito bem, mas exigiram muito tempo de desenvolvimento.
- Erros de identificação de componentes: em geral, o componente que apresentou maior complexidade para identificação foi a chave seccionadora, em função da alta variabilidade de padrões deste tipo de componente (foram identificados pelo menos 18 formas diferentes de representação para a chave seccionadora).

Embora consideremos a existência de erros, parte do objetivo do trabalho era demonstrar que estes erros ocorreram com baixíssima frequência. Acreditamos que, sim, ainda é necessária uma revisão humana para aferir o resultado final, porém nossos esforços seguiram na direção de demonstrar a alta precisão da solução.

Título - Uso de Infraestrutura 5G e Edge Computing para Implementação de IA na Prevenção de Falhas em Redes de Distribuição de Energia
Entidade(s) - Instituto Federal do Ceará,NUCLEO DE ESTUDOS E PESQUISAS DO NORTE E NORDESTE,CELESC DISTRIBUICAO SA
Autor(es) - Antonio Wendell de Oliveira Rodrigues,Rogério Guerra Diógenes Filho,André Luiz Carneiro de Araújo,Fabricio Evangelista de Souza,Guilherme Saidler
Resumo
Este trabalho apresenta uma iniciativa pioneira da CELESC, desenvolvida em parceria com a Nokia, voltada para a modernização das redes de distribuição de energia por meio da implementação de uma infraestrutura baseada em 5G NSA (Non-Standalone) e computação em borda (edge computing). A arquitetura adotada, com suporte à plataforma NDAC (Nokia Data Center Automation), permite o monitoramento em tempo real de ativos críticos, como transformadores e bancos de baterias, utilizando sensores inteligentes, câmeras termográficas e algoritmos de inteligência artificial (IA). A combinação entre alta velocidade de comunicação, baixa latência e processamento local possibilita a detecção precoce de anomalias operacionais, reduzindo o risco de falhas graves, como superaquecimento e incêndios. A rede 5G privada emprega enlaces de fibra óptica e rádio, conectando subestações e centros de controle a dispositivos de borda com capacidade de análise em tempo real. A utilização de IA para análise de dados sensoriais e imagens térmicas permite a geração de alertas automáticos e acionamento de ações preventivas, contribuindo para a redução de custos operacionais e aumento da segurança. Durante os testes, observou-se um potencial de redução de 30% nas falhas inesperadas em bancos de baterias. A solução se destaca ainda pela escalabilidade, possibilitando a instalação de milhares de sensores sem comprometer a qualidade da comunicação. Este projeto demonstra o potencial transformador da convergência entre redes 5G, edge computing e IA para o setor elétrico, estabelecendo um novo paradigma para a operação segura e eficiente de sistemas de distribuição de energia.
Perguntas e Respostas

"Esse desempenho superou em mais de 50% a velocidade de resposta dos sistemas de monitoramento baseados em redes legadas, que dependiam de comunicação centralizada com servidores remotos.". Como chegaram no valor de 50%? Como foi realizada esta validação?

O valor de “mais de 50%” de ganho na velocidade de resposta foi obtido a partir de testes de laboratório controlados que compararam a latência de comunicação entre a solução baseada em 5G privado e infraestruturas legadas como 3G público e comunicação satelital. Utilizando pacotes simulados de dados sensoriais, mediu-se o tempo médio de ida e volta (RTT) em cada cenário. A solução com 5G apresentou latência média de 18 ms, enquanto as redes legadas registraram 39 ms (3G) e 54 ms (satelital). O ganho percentual foi calculado comparando os valores, resultando em uma redução de aproximadamente 53,85% em relação ao 3G e 66,66% frente ao satélite, validando tecnicamente a afirmação de ganho superior a 50% no tempo de resposta.

"Os testes conduzidos em campo com a nova infraestrutura 5G e os sistemas de monitoramento inteligente da CELESC demonstraram ganhos significativos

na detecção e prevenção de falhas em ativos críticos, com destaque para os bancos de baterias utilizados em subestações."
Quais foram os ganhos significativos e qual método usaram pra chegar nesse resutado?
Os “ganhos significativos na detecção e prevenção de falhas” referidos no artigo dizem respeito à melhora na capacidade de comunicação de dados entre os sensores instalados em ativos críticos (como bancos de baterias) e os sistemas de supervisão, com foco no tempo de resposta e estabilidade da rede. Esses ganhos foram obtidos por meio de testes laboratoriais realizados com infraestrutura de 5G privado em comparação com redes legadas (3G público e satélite). O método utilizado consistiu na simulação de fluxos de dados sensoriais representativos de eventos anômalos (como aumento de temperatura geral ou individual referenciado por bateria) enviados a partir de um protótipo embarcado (ARGOS v1). Os testes registraram os tempos de envio e recebimento de pacotes entre os dispositivos e os servidores de supervisão em diferentes cenários de rede. Com a infraestrutura 5G, observou-se uma redução significativa na latência e na variabilidade do tempo de comunicação, o que, indiretamente, reduz o tempo de percepção e reação às anomalias. Embora os testes não tenham executado uma lógica de tomada de decisão operacional (como acionamento de alarmes ou shutdown), os resultados de comunicação comprovam que a arquitetura proposta viabiliza futuras aplicações preditivas mais rápidas e confiáveis.

O artigo diz tratar também da implementação de IA na Prevenção de Falhas em Redes de Distribuição de Energia. Como foi feita a parte relacionada a IA?
A implementação de Inteligência Artificial no projeto teve como foco viabilizar a inferência local em dispositivos de borda com alto throughput, utilizando TPUs e GPUs embarcadas (SBC com hat de IA) para processar modelos previamente treinados. Essa capacidade permitiu a execução de análises iniciais diretamente no ambiente da subestação, com baixa latência e sem depender exclusivamente de conectividade constante. Entretanto, o desenho arquitetural priorizou também a integração com o datacenter corporativo da CELESC, para onde os dados classificados como relevantes (como ocorrências anômalas ou padrões suspeitos) eram encaminhados. Essa separação entre inferência local e análise aprofundada remota assegurou maior eficiência no uso da rede 5G e possibilitou a construção de históricos centralizados, com apoio de recursos computacionais mais robustos, essenciais para a retroalimentação de modelos, refinamento de detecções e correlação com eventos operacionais de larga escala.

"Os testes conduzidos em campo com a nova infraestrutura 5G e os sistemas de monitoramento inteligente da CELESC demonstraram ganhos significativos na detecção e prevenção de falhas em ativos críticos, com destaque para os bancos de baterias utilizados em subestações."
Quais foram os ganhos significativos e qual método usaram pra chegar nesse resutado?

Título - Análisis comparativo del comportamiento de las funciones de misión crítica diferencial de línea y tele protección usando tecnologías de comunicación SDH vs MPLS-TP

Entidade(s) - Hitachi Energy Brasil LTDA
Autor(es) - Hector Hernando Moreno Castelblanco

Resumo

Las telecomunicaciones han sido una parte fundamental para la operación eficiente y segura del sistema de potencia y la tecnología SDH (Synchronous Digital Hierarchy) ha sido la piedra angular para este propósito, dada su alta fiabilidad y baja latencia es la tecnología más usada para el transporte de las funciones de misión crítica como es la protección diferencial de línea y las tele protecciones, sin embargo también presenta limitaciones que se han vuelto más evidentes con el avance de las necesidades de comunicaciones actuales, con todo el proceso de la transición energética y tecnologías de digitalización en el sector eléctrico se han aumentado en forma exponencial el volumen de la transmisión de datos lo que ha llevado a necesidades de manejar mayores anchos de banda de una manera más flexible y eficiente que lo que permite la tecnología SDH.

Como respuesta a estos desafíos surge las necesidades de tener tecnologías como es MPLS-TP (Multiprotocol Label Switching - Transport Profile) que combina las ventajas del enrutamiento estático bidireccional basado en etiquetas de MPLS y las características de transporte de SDH, ofreciendo una plataforma más versátil , eficiente , escalable y flexible y a manteniendo la fiabilidad y baja latencia que requieren las funciones de misión crítica como es la protección diferencial y las tele protecciones, mejorando la eficiencia operativa y preparando a las redes eléctricas para la integración con tecnologías emergentes como la generación distribuida y la digitalización.

Bajo este contexto en conjunto con una de las principales transmisoras de energía de Colombia se implementó en laboratorio una arquitectura hibrida (SDH – MPLS-TP) con el fin de hacer un comparativo del performance de cada una de estas tecnologías en diferentes condiciones y contingencias operativas.

Perguntas e Respostas

Diante dos resultados tecnicamente equivalentes entre SDH e MPLS-TP nas funções de missão crítica, quais seriam as principais vantagens justificáveis para a substituição da base instalada de SDH por MPLS-TP, considerando aspectos operacionais, econômicos e de evolução tecnológica?

Las principales ventajas de la tecnología MPLS_TP vs SDH son tener un manejo más eficiente del ancho de banda, flexibilidad y escalabilidad que permite adaptarse a los nuevos requerimientos del aumento de la demanda de datos especialmente por los temas de transición energética y digitalización. También se garantiza el performance necesario para las funciones de misión crítica como diferencial de línea y teleprotección ante diferentes condiciones operativas y casos de contingencia utilizando la misma infraestructura de red de comunicaciones.

Durante os testes com sincronização via PTP (Power Utility Profile), foi monitorada a estabilidade da referência de tempo em situações de falha ou degradação do enlace? Houve perda de sincronismo em algum dos testes com comutação?

Durante las pruebas de conmutación del canal de comunicaciones en la red de multiplexores por los medios SDH, MPLS_TP no se observó pedida o degradación de la señal de sincronismo, sin embargo cuando se realizaron pruebas de saturación si fue necesario implementar QoS al servicio de sincronismo PTP (power Utility profile) dándole el grado más alto de prioridad para garantizar que no tuviera degradación y ocasionara bloqueos o funcionamiento erróneo, ya que este servicio se vuelve tan critico como la misma funcionalidad de protección por lo que se recomienda incluso la implementación de redundancia.

Considerando o legado instalado de SDH, quais seriam os principais desafios técnicos e operacionais enfrentados durante a migração para MPLS-TP em redes que operam em regime contínuo?

Considero que los principales desafíos es poder realizar una transición transparente y con el menos impacto posible sobre el sistema, por lo que se recomienda poder tener equipos multiplexores híbridos que puedan manejar en forma paralela las dos tecnologías permitiendo hacer una transición más suave y transparente al poder ir migrando en forma escalonada de SHD a MPLS_TP manteniendo los servicios de misión crítica.

Título - Implantação de novo ambiente de Software Defined Datacenter (SDDC) para Sistemas de Tecnologia da Automação da Itaipu Binacional.
Entidade(s) - ITAIPU BINACIONAL
Autor(es) - PEDRO PAULO GOMES FERREIRA GARCIA
Resumo
A ITAIPU Binacional, em seu constante objetivo de melhorar o fornecimento de energia, disponibilidade dos equipamentos e instalações, além de minimizar os custos operacionais, sempre busca aplicar tecnologias que melhor adequem a implantação, atualização e modernização dos sistemas do ambiente de tecnologia da automação (TA) aos seus processos e objetivos corporativos e estratégicos. No que se refere ao modelo de arquitetura e tecnologias para implantação de sistemas e datacenters, observou-se que a utilização dos modelos de hiperconvergência (HCI) e Software Defined Datacenter (SDDC) são efetivamente capazes de entregar ambientes de alta performance, resilientes, com escalabilidade, tolerância a falhas, segurança e de fácil gerenciamento.

Até o ano de 2017 a ITAIPU Binacional implantava sistemas de TA baseados em um modelo de infraestrutura de hardware e software dedicados para suporte de cada um dos seus sistemas [1] . Este modelo provou-se eficiente e adequado às tecnologias, custos e processos passados, contudo, tornou-se obsoleto frente a crescente digitalização e demanda por processamento de dados, gerenciamento, segurança e comunicação em rede, o que culminou na substituição deste modelo pelo modelo hiperconvergente em uma infraestrutura denominada Sistema Integrado de Redes Industriais (SIRI). O projeto de Atualização Tecnológica da ITAIPU Binacional, cujo contrato de execução foi iniciado em 2022, está implantado um novo ambiente SDDC, denominado de Rede de Tecnologia da Automação (RTA), como sendo uma modernização e expansão do SIRI (HCI) [2] . Este trabalho apresenta as tecnologias HCI, SDDC e aborda as estratégias e benefícios obtidos com a utilização delas nos sistemas SIRI e RTA.
Perguntas e Respostas

Como a equipe de ITAIPU está lidando com os desafios de capacitação e mudança cultural das equipes técnicas frente à complexidade e abstração dos ambientes virtualizados e definidos por software, especialmente na migração para o modelo SDDC?
Primeiramente é importante ressaltar que o uso da tecnologia HCI nos últimos anos permitiu um contato e capacitação das equipes da Itaipu com tecnologias e culta semelhantes as do SDDC.

A implantação da tecnologia SDDC está inserida no escopo de entrega da nova Rede de Tecnologia da Automação (RTA), a qual faz parte do Projeto de Atualização Tecnológica da Usina. Como demais entregáveis deste projeto, temos uma série de treinamentos divididos em Treinamentos Pré Inspeção em Fábrica, Treinamentos de conhecimento e Treinamentos On-The-Job, onde, cada um deles, pretende, em momentos específicos da implantação, capacitar as equipes da Itaipu.

O impacto causado pela introdução destas tecnologias e da digitação em si esta provocando grandes mudanças de paradigmas nas equipes técnicas da ITAIPU. No caso do SDDC e da RTA, foi previsto, destro do contrato, o serviço de revisão de governança e processos, objetivando criação e adequação dos processos para suporte as novas tecnologias, bem como um serviço de suporte a operação do novo NOC/SOC, onde o treinamento e adaptação cultural das equipes da Itaipu será acompanhada de profissionais especializados da CONTRATADA.

O modelo SDDC implantado contempla algum mecanismo de orquestração automatizada para provisionamento de recursos críticos, como balanceamento de carga e failover automático?
Sim, o ambiente SDDC esta sendo implantado com recurso de HA (high Avaiability) e balanceamento disponibilizado pela solução vMware vCenter o qual fornece estas funcionalidades de forma automática.

O provisionamento de recursos críticos é entregue através da ferramenta vMware Aria.

A RTA já está em produção com sistemas de missão crítica ou apenas sistemas auxiliares foram migrados até o momento? Existe um plano de homologação técnica para funções mais sensíveis?
A principio a RTA foi desenhada para desempenhar funções do nível 3 / 3,5 do modelo PURDUE, ou seja, estará operando apenas com serviços e sistemas auxiliares. Os sistemas de tempo real como SCADA, SDSC e proteção, neste momento, possuem infraestrutura virtualizada segregada da RTA, sem uso de SDDC ou HCI.

Durante o planejamento da migração para SDDC, quais foram os principais desafios enfrentados no mapeamento dos sistemas legados para ambientes virtualizados? Houve necessidade de reengenharia de aplicações?

Título - Cibersegurança nas mensagens GOOSE: estratégias para mitigação de riscos
Entidade(s) - SCHWEITZER ENGINEERING LABORATORIES COMERCIAL LTDA
Autor(es) - Gabriel Cortes Cassiano Pereira,Wesley Silva Roberto,Vinicius Vasconcellos Ferrari
Resumo
Este artigo apresenta um estudo de estratégias para ampliar a mitigação das vulnerabilidades de mensagens GOOSE em redes de tecnologia da operação (TO). O artigo detalha as vulnerabilidades das mensagens GOOSE e analisa os riscos associados. Ademais, analisa comparativamente o nível de mitigação dos riscos usando tecnologias de redes de TO tradicionais e redes definidas por software (SDN), através de simulações de incidentes e ataques ao GOOSE em ambas as tecnologias.
Perguntas e Respostas

O que motivou a escolha do protocolo GOOSE como foco do estudo em vez de outros protocolos da IEC 61850?
Dada sua difusão dentro dos sistemas de potência e suas aplicações estarem diretamente relacionadas a esquemas de proteção via rede, desta forma qualquer incidente ou ataque que afete a confidencialidade, integridade e a disponibilidade do protocolo implicam em impacto nos esquemas de proteção. Todos os protocolos tem uma superfície de ataque, o GOOSE, dado sua disseminação multicast e mecanismo de transmissão permitem explorar os incidentes e ataques de forma mais abrangente nas diferente tecnologias de rede.

Como o uso de SDN pode ser aplicado em subestações existentes que utilizam infraestrutura tradicional? Há limitações práticas?
O switch SDN é um switch Ethernet, portanto se integra com qualquer outro host ou rede Ethernet. A maioria das aplicações no Brasil somente os switches principais são SDN e estes se conectam aos demais switches RSTP.

Na prática, quais ataques ao GOOSE vocês consideram mais prováveis hoje em subestações reais?
Na avaliação de risco para ambientes operacionais probabilidade é considerada após o impacto. Uma vez categorizados por impacto, usamos probabilidade, frequência e dificuldade para priorizar os riscos. Considerado isso, a probabilidade de um incidente é maior que a de um ataque (ator malicioso). Dentro dos incidentes o mais comum é o Flooding. Ele pode ocorrer, por exemplo, em redes de grande porte com banda mal dimensionada, ou quando ocorre um loop na rede, ou até mesmo quando um IED gera quantidades excessivas de tráfego devido à falhas internas ou má configuração.

Na prática, quais ataques ao GOOSE vocês consideram mais prováveis hoje em subestações reais?

Na prática, quais ataques ao GOOSE vocês consideram mais prováveis hoje em subestações reais?

Na prática, quais ataques ao GOOSE vocês consideram mais prováveis hoje em subestações reais?

Na prática, quais ataques ao GOOSE vocês consideram mais prováveis hoje em subestações reais?

Na prática, quais ataques ao GOOSE vocês consideram mais prováveis hoje em subestações reais?

Na prática, quais ataques ao GOOSE vocês consideram mais prováveis hoje em subestações reais?

Título - Transformação Digital no Centro de Operações da ISA Energia Brasil: Integração de IA e SCADA para eficiência, agilidade e segurança ao consultar Documentos Operativos em Tempo Real
Entidade(s) - CTEEP - Companhia de Transmissão de Energia Elétrica Paulista
Autor(es) - Rene Rodrigues Peric,Hemerson Baldo
Resumo
Com o crescimento da rede de subestações na ISA Energia Brasil, os operadores enfrentam desafios crescentes na gestão das demandas, especialmente durante perturbações no Sistema Elétrico de Potência (SEP). Atualmente, o acesso a documentos operacionais é feito através de um sistema desenvolvido pela ISA Energia Brasil, o SISCONWEB. Porém, a utilização deste sistema, exige que os operadores desviem sua atenção do SCADA, impactando a eficiência operacional. Além disso, não é ágil ou eficiente, considerando documentos com 100, 200, até 300 páginas, pois exige que o Operador faça a leitura do documento para encontrar a informação necessária.

A solução desenvolvida executa a divisão de um documento original em trechos, chamados fragmentos, os quais permitem que o Operador receba o trecho do documento na tela do sistema SCADA no ponto exato para leitura da instrução e execução da manobra de liberação ou normalização.

Este projeto foi marcado pela integração entre SCADA (SAGE) e SISCONWEB da ISA Energia Brasil. A aplicação de IA representa um marco na evolução tecnológica no Centro de Operação, melhorando a eficiência e segurança das operações. A solução desenvolvida possui potencial para ser expandida para outros casos de uso, permitindo que Operadores tenham acesso a uma gama ainda maior de informações de forma rápida e assertiva.

A integração entre SISCONWEB e SCADA (SAGE) trouxe inúmeros benefícios e principalmente agilidade das manobras.
Perguntas e Respostas

Existe algum plano de escalabilidade para que a solução seja adaptada a outras áreas da ISA ou até mesmo a outras empresas do setor?
Não existe plano de escalabilidade para outras empresas do setor. A solução foi preparada para utilização interna, considerando que o SISCON é uma ferramenta da ISA Energia Brasil. Quanto a utilização por outras áreas da ISA, sim, já existe a intensão de outras áreas utilizarem a solução, mas até o momento, está em uso apenas pelo Centro de Operação.

Existe algum plano de pesquisa interna para avaliar a aderencia do operador a esse novo modelo de consulta?
Entendi que esse novo modelo de consulta se refere a própria solução, que já está em produção e em pleno uso dos operadores do Centro de Operação. Não preparamos uma pesquisa interna pois a área de TI e Supervisão, responsáveis por este projeto, trabalham fisicamente lado a lado com o Centro de Operação. Portanto, o feedback sobre a ferramenta é feito constantemente.

Quais foram os maiores desafios na etapa de treinamento do modelo?
Utilizamos bibliotecas Python já treinadas para a língua portuguesa. O desafio foi relacionar a resposta da IA com os bancos de dados de sistemas da ISA, bem como com o sistema SCADA.

Título - Redes MPLS-TP: Resiliência com Hitless Switching para Teleproteção
Entidade(s) - Belden
Autor(es) - GUILHERMME LISBOA,Davy Haegdorens
Resumo
Em um mundo em constante evolução, os Sistemas de Proteção, Automação e Controle (PACs) exigem uma rede de telecomunicações confiável, segura e preparada para o futuro. No contexto das telecomunicações operacionais (TO), é fundamental que as redes segreguem com segurança todos os serviços, interconectando aplicações de missão crítica que garantem o funcionamento adequado da infraestrutura do sistema elétrico. Tecnologias baseadas em multiplexação por divisão de tempo (TDM), como SDH (Hierarquia Digital Síncrona) e PDH (Hierarquia Digital Plesiócrona), ainda são amplamente utilizadas por concessionárias de energia para serviços altamente críticos, como a teleproteção, destacando-se a proteção diferencial de corrente pelo seu desempenho e confiabilidade. No entanto, o mercado para essas tecnologias está em declínio há cerca de duas décadas, com muitos produtos tornando-se obsoletos (End Of Life - EOL), especialmente após a escassez de chipsets em 2018. Portanto, é necessário explorar novas tecnologias baseadas em pacotes como sucessoras das redes OT do setor de Geração, Transmissão e Distribuição de energia.
O Multiprotocol Label Switching – Transport Profile (MPLS-TP) é uma norma de rede especificamente definida para telecomunicações operacionais. A estrutura do MPLS-TP, conforme definida na RFC 5921 [1], determina o uso de funções de Operação, Administração e Manutenção (OAM) in-band , caminhos bidirecionais co-roteados, e o uso de Sistema de Gerenciamento de Rede (NMS), além da funcionalidade central do MPLS de encaminhamento baseado em rótulos por meio de caminhos comutados por rótulo (LSP) e emulação de pseudowires ponto a ponto (PWE3). Assim, a solução de rede MPLS-TP permite que o operador, tal como no SDH, tenha controle total sobre a rede, possibilitando a segregação segura e o

transporte de todas as aplicações conectadas. O CIGRE, confirmou que o MPLS-TP é o sucessor ideal para o SDH em seu livro “ Utility Communication Networks and Services ”, publicado em 2016 [2].

Um abrangente projeto de prova de conceito (PoC) foi realizado, abrangendo as aplicações mais críticas de uma rede de concessionária de energia, demonstrando que o MPLS-TP é uma solução de rede segura e resiliente que atende a todos os principais requisitos do setor elétrico. O estudo contemplou todos os aspectos de uma rede moderna de Transmissão e Distribuição, como resiliência em testes de Taxa de Erro de Bits (Bit Error Rate – BER), proteção de tráfego, atrasos unidirecionais e diferenciais, sincronização de rede, otimização de largura de banda e resiliência aprimorada.

Este artigo demonstra que o MPLS-TP é a tecnologia baseada em pacotes mais adequada para uma rede ampla para concessionárias de energia. Mostra que a solução garante a entrega não apenas dos serviços mais críticos, mas de todos os serviços da rede. Além disso, elimina qualquer impacto de falhas de rede sobre os serviços críticos, graças ao recurso 1+1 Hitless Switching com opção 4:1, garantindo zero perda de pacotes na rede – elemento essencial para redes de missão crítica.

Em conclusão, comprova-se que uma solução de rede baseada em pacotes MPLS-TP de ponta a ponta oferece segurança e longevidade ao setor elétrico. Trata-se da solução de rede mais confiável, flexível e preparada para o futuro.

Perguntas e Respostas

Durante os testes houve alguma análise de falhas residuais, como perda de sincronismo ou ainda impacto de fato na proteção, como a diferencial muito citada no documento?

As aplicações foram sincronizadas por meio de adaptive clocking sobre o próprio caminho de dados, portanto, qualquer impacto nos dados levaria, de forma inerente, a problemas de sincronização.

A sincronização foi monitorada em todas as aplicações ao longo dos testes. Perda de sincronismo foi observada no teste de BER para a proteção MPLS-TP 1:1, tanto no relé de proteção quanto no testador de referência C37.94 e no X.21.

Por outro lado, o Hitless Switching não apresentou nenhuma perda de dados nem perda de sincronismo em nenhuma das aplicações, em nenhum dos cenários validados.

A interoperabilidade do MPLS-TP com diferentes fabricantes e equipamentos legados foi testada na PoC? Como garantir que a solução seja plenamente funcional em ambientes WAN híbridos, comuns no setor elétrico?

O MPLS-TP utilizado nesta PoC é interoperável com enlaces legados E1/T1, SDH e SONET. Dito isso, o Hitless Switching é uma funcionalidade exclusiva deste fabricante específico. No MPLS-TP e em outras variantes, há pouquíssimos registros de aplicação nesse contexto, especialmente para 87L, onde as concessionárias tendem a implantar equipamentos do mesmo fabricante ao longo das linhas de transmissão.

A PoC foi realizada aonde? Ela cobre cenários de falha e BER com enlaces únicos. A tecnologia foi testada em topologias em anel ou malha com

múltiplos pontos de falha potenciais? Quais os impactos esperados em termos de recuperação e estabilidade?
Os testes foram realizados no FAT do escritório da Belden em Olen.
Todos os serviços foram configurados estaticamente em topologias virtuais sobre a topologia física de rede com MPLS-TP, proporcionando ao operador controle total sobre todo o tráfego na rede. A teleproteção rodando em C37.94 e X.21 exige uma topologia ponto a ponto, que é criada virtualmente sobre qualquer camada física subjacente. Portanto, a complexidade da rede física não representa um desafio graças à configuração estática no MPLS-TP; na verdade, torna-se um benefício para a redundância do serviço. Quanto maior a rede, mais opções existem para configurar caminhos redundantes. Esta configuração nos limitou ao Hitless Switching 1+1, mas se houver mais caminhos alternativos disponíveis, é possível até mesmo configurar Hitless Switching 4:1 de ponta a ponta.

Título - Utilização prática de sensoreamento de efeitos não-lineares em fibras ópticas: Estudo de Caso das aplicações em suporte à vigilância patrimonial, operação de equipamentos elétricos, monitoramento de redes locais e remotas e outras aplicações em subestações.
Entidade(s) - NETCON CONSULTORIAE ENGENHARIA LTDA,NETCON LTDA,Instituto Scinet
Autor(es) - Cristiano Henrique Ferraz,DANIEL MAGALHAES CRUZ TAVARES DE PADUA,EWERTON DE OLIVEIRA FIGUEIROA
Resumo
A reflectometria óptica, utilizada há mais de cinquenta anos, baseia-se na emissão de pulsos ópticos por meio de um OTDR (Optical Time Domain Reflectometer) e na análise do retroespalhamento causado pela dispersão de Rayleigh ao longo de fibras ópticas. Essa técnica permite identificar e localizar falhas, medir a atenuação do sinal e monitorar a integridade da fibra. Nos últimos anos, surgiram avanços significativos com o uso de pulsos de alta potência para explorar efeitos ópticos não lineares nas fibras, como os provocados por variações térmicas, vibrações e pressão mecânica. Esses efeitos, inicialmente estudados com fibras especiais em laboratórios desde os anos 1990, passaram a ser analisados em fibras padrão de telecomunicações, ampliando seu uso prático. As técnicas baseadas na análise espectral de Brillouin e Raman possibilitam que fibras ópticas funcionem como sensores distribuídos, monitorando temperatura, pressão e vibrações ao longo de grandes distâncias. Essas tecnologias oferecem vantagens como baixo custo, leveza e reutilização da infraestrutura de fibras já instalada, especialmente em ambientes como subestações e usinas de energia. Este artigo avalia a aplicação dessas tecnologias no setor elétrico, com ênfase em necessidades que vão além da comunicação tradicional. São discutidos casos de uso para segurança patrimonial, monitoramento remoto e supervisão de condições ambientais em áreas isoladas, com o uso de cabos dielétricos e OPGW. O estudo também aborda o posicionamento e dimensionamento dos sensores e demais componentes do sistema. As análises espectrais de Brillouin e Raman são destacadas como as únicas técnicas capazes de fornecer medições ópticas distribuídas com precisão. Suas frequências ressonantes variam de forma linear com a temperatura e o alongamento da fibra, facilitando o monitoramento eficiente em tempo real. Neste trabalho, serão demonstradas e avaliadas aplicações não apenas da medição da

perda de potência óptica para sinais de comunicação, mas também aplicações da nova tecnologia para medir, localizar e interpretar outros parâmetros tais como temperatura e vibração em atividades operacionais de subestações e usinas elétricas, bem como cobertura de perímetro. Uma análise comparativa com soluções que usam câmeras e radares para cobertura de perímetro também é realizada.
Perguntas e Respostas

Além da implementação, foram realizados testes controlados da solução? Em caso afirmativo, qual foi a taxa de falsos positivos observada no estudo de caso?"
Não temos dados sobre a ocorrência de falsos positivos. Há um processo de calibração no início que permite aprender e reduzir os alarmes causados por eventos inerentes ao sistema.

No comparativo com câmeras e radares, a ausência de imagens na solução de fibra é apontada como limitação. Há alguma solução híbrida integrada sendo considerada que combine fiber sensing com recursos visuais?
Sim, a visualização imediata de imagens em tempo real é um dos pontos em que câmeras e radares apresentam vantagem.
Entretanto, é possível criar integrações para constituir sistemas híbridos, onde o fiber sensing atua como sistema primário de detecção com cobertura contínua e de longo alcance, enquanto as câmeras são acionadas somente quando o sistema identifica uma anomalia. Essa abordagem reduz significativamente custos operacionais, já que não exige cobertura total por câmeras, mas garante resposta visual imediata quando necessário.
Neste caso, a solução representada pelo DAS gera alarmes em tempo real. A mensagem encaminhada ao Centro de Controle é muito simples, tal como um XML, em presença de um alarme ocorrido em tempo real. A mensagem XML enviada contém as coordenadas do evento e sua identificação. Essa mensagem é exportada e integrada a outros sistemas, o que inclui os sistemas de CFTV No caso, a câmera de CFTV mais próxima do evento detectado pelo DAS é apontada imediatamente para o local do evento.

Quais intervenções são necessárias para a implantação do sistema de sensoriamento em linhas de transmissão já existentes? E quais seriam os principais ganhos operacionais e estratégicos nesse cenário?

A implantação em linhas já existentes é minimamente invasiva, pois reaproveita a infraestrutura óptica disponível, como cabos OPGW. As intervenções necessárias concentram-se em instalação do FTH-DAS com conexão ao equipamento das fibras já implantadas e integração com sistemas de supervisão e controle.
Nas linhas de transmissão, o sistema DAS precisa conectar-se às interfaces ópticas onde terminam as fibras. Em se tratando (primordialmente) de fibras aéreas, o primeiro objeto da monitoração é a tensão mecânica das linhas. Esta pode ser uma função dos testes após a instalação para detectar se o instalador tensionou o cabo além do limite. Também se detecta a degradação do cabo ao longo do tempo, o que é particularmente relevante em linhas aéreas (devido ao “galope” dos cabos OPGW ou por outras ações dos ventos) ou mesmo em cabos instalados ao longo de pontes e túneis, sujeitos a vibrações e cargas mecânicas. Possivelmente, testes de aceitação pontuais podem precisar somente do ONA1000.

Ao identificar as vulnerabilidades, o cliente pode direcionar a manutenção preventiva antes de que a linha se interrompa (por vento, relâmpagos, deformação do solo, gelo, queimadas etc.).

Título - Estudo comparativo de novas tecnologias de comunicação sem fio para empresas do setor elétrico. Análise técnica e econômica sobre aplicações do WiFi6, LTE e 5G para a atual demanda de serviços.
Entidade(s) - NETCON LTDA,Instituto Scinet,NETCON CONSULTORIAE ENGENHARIA LTDA
Autor(es) - EWERTON DE OLIVEIRA FIGUEIROA,Cristiano Henrique Ferraz,Felipe Leitão Valois,Nadja Juliana da Silva Lima
Resumo
Redes sem fio podem ser uma solução para as necessidades de comunicação de utilities , especialmente com a chegada de redes elétricas inteligentes, que impõem requisitos de mobilidade, capilaridade, capacidade, processamento distribuído (e Edge Clouds) baixa latência, segurança cibernética, suporte a equipes móveis e a vários tipos de terminais de IoT, além de cobertura e alcance (distâncias) diversos. Há vários casos de aplicação, cada qual com necessidades e em ambientes distintos. Distribuidoras de energia necessitam comunicação com dispositivos e equipes externos em grande quantidade e com cobertura em áreas públicas. Geradoras e transmissoras (ou armazenadoras) de energia elétrica requerem uma cobertura mais concentrada. No caso destas, a necessidade envolve atendimento em áreas delimitadas e próximas às subestações ou em clusters com perímetros e área de cobertura restrita e funções e necessidades bem definidas, particularmente segurança, apoio operacional e automação das subestações e parques geradores. Neste estudo, foram consideradas as necessidades atuais e futuras de empresas encarregadas da produção e transmissão de energia elétrica para determinação dos casos de aplicação, das necessidades e as características de comunicação. A partir desses estudos, os autores apresentam as opções técnicas e as vantagens e desvantagens respectivas das diversas opções (WiFi6, PLTE e 5G), com o fim de comparar classificar as soluções factíveis segundo os critérios escolhidos.
Perguntas e Respostas

Na comparação apresentada entre as tecnologias de comunicação, foi considerada a IEC 61850 utilizando exclusivamente fibra óptica na comparação. A norma IEC 61850 poderis operar sobre diversas tecnologias como WiFi, LTE e 5G? Essa limitação na análise não compromete a avaliação da tabela, especialmente na coluna de considerações técnicas e de aplicabilidade?
Na verdade, não, pois atualmente a opção ainda é a de IEC 61858 sobre fibras ópticas.

A norma IEC 61850 está sendo ampliada e adaptada para suportar comunicação sem fios em subestações, apesar dos desafios inerentes a ambientes eletromagnéticos adversos e à confiabilidade em tempo real. As soluções sem fios, muitas vezes aproveitando tecnologias industriais sem fios como Zigbee ou redes LTE-A e 5G, NB-IoT e outras mais amplas, visam a reduzir os custos de

cabeamento, aumentar a flexibilidade e permitir novas aplicações, como as de automação de distribuição. Embora a norma utilize principalmente Ethernet cabeada (especialmente com fibras ópticas) para maior imunidade a ruídos e interferências, e para possuir proteção inerente a tentativas de burlar a segurança cibernética, a sua extensão para o ambiente sem fios envolve a integração com redes de área de campo (FANs) sem fios confiáveis e redundantes e a garantia de uma comunicação segura e de baixa latência para atender aos requisitos de missão crítica.

Sem dúvida as redes de área de campo (FANs) sem fios podem ampliar os recursos da norma IEC 61850 para aplicações principalmente na distribuição para aplicações avançadas, como localização de falhas e proteção. Como exemplos de usos atuais de soluções sem fio, citamos:

Automação da distribuição:

Suporte a aplicações como proteção contra queda de condutores e localização de falhas, estendendo a norma IEC 61850 à rede de distribuição.

Monitoração remota: conexão de dispositivos de campo sem fios ao centro de controle.

Virtualização: utilização da virtualização para implementar e configurar relés e dispositivos virtuais através de uma rede sem fios.

Quanto á adequação e preocupações de projeto, podemos citar:

Automação da distribuição:

Quais métricas de desempenho foram efetivamente utilizadas nas comparações reqalizadas (por exemplo, latência, jitter, throughput real)? Há dados quantitativos que demonstrem o atendimento aos requisitos de aplicaçõe citadas como CFTV, IIoT ou teleproteção?
Várias métricas foram – e continuam sendo – utilizadas. Como a diversidade de ambientes e aplicações é muito vasta, os parâmetros avaliados são aqueles que efetivamente impactam cada aplicação. Quando se elaboram os projetos de cobertura wireless, tomam-se em conta as aplicações típicas em cada ambiente para definir os limites a serem atendidos. Em cada projeto, as redes sem fio são dimensionadas para atender às s normas e aos procedimentos de rede segundo as necessidades mais críticas das aplicações.

Quanto aos dados disponíveis foram realizadas medições de todos os fatores críticos, como os mencionados e mais outros, como segurança cibernética, disponibilidade, taxa de erros, necessidade de redundância da rede, imunidade a radiações eletromagnéticas, segurança cibernética e outras.

Exemplos das medições que são feitas:

Latência e confiabilidade

Mensagens críticas como GOOSE exigem latência determinística extremamente

baixa, algo que as redes sem fio tradicionais têm dificuldade em garantir.

Mitigação: o 5G com recursos URLLC foi projetado para resolver isso. Os investigadores também estão a desenvolver métodos de agregação de pacotes para reduzir a perda de pacotes em canais sem fios.

Segurança

As subestações digitais são suscetíveis a ameaças cibernéticas, e a comunicação sem fio adiciona outro vetor de ataque potencial.

Mitigação: é necessária uma adesão mais rigorosa às normas de cibersegurança, como a IEC 62351, segmentação de rede e protocolos seguros de transferência de ficheiros.

Interferência eletromagnética (EMI)

As subestações são ambientes eletromagneticamente adversos, que podem interferir nos sinais radioelétricos.

Mitigação: A utilização de equipamentos sem fio de nível industrial, como roteadores 5G externos, com blindagem e localização adequadas ajudam a manter a integridade do sinal.

Lacunas de normalização

A norma IEC 61850 atual não cobre totalmente todos os aspectos dos sistemas de comunicação sem fio, exigindo soluções adicionais e o desenvolvimento de normas.

Mitigação: acompanhar ativamente a emissão de novas normas e ajudar a adaptar os procedimentos de rede para incluir redes operativas sem fio, particularmente no pátio de subestações e usinas geradoras.

Este é um trabalho em andamento, e é dinâmico para cobrir novas aplicações e novos equipamentos para cada projeto. Não cabe no escopo deste IT incluir dados resultantes das medições e testes feitos; somente as principais conclusões fazem parte deste Informe Técnico

Foram realizados testes e simulações com cenários com interferência eletromagnética intensa, como aqueles encontrados em subestações de alta tensão? Como foi validada a robustez da comunicação nesses ambientes hostis?

Na verdade, não foram realizados testes completos, pois atualmente a principal opção ainda é a de aplicar a norma IEC 61858 sobre fibras ópticas. Esses testes em redes sem fio estão programados para serem efetuados simulando ambientes com EMI elevada e suas formas, e medições dos efeitos digitais (latência, confiabilidade, erros, erros impulsivos e outros) para os vários cenários de EMI, tanto com a medição de campos e interferência eletromagnética quanto com a localização de interferências nos ambientes reais.

As medições para a certificação de soluções sem fio (e, claro, também com fio) são feitas mediante ensaios em laboratório e ambientes simulados, sempre aderindo às normas existentes. Entretanto, tanto nesses ambientes quanto posteriormente, no campo, em operação real, adotam-se técnicas de medição que incluem inteligência artificial para caracterizar os parâmetros que balizam a operação normal (análise de comportamento). Esse balizamento serve tanto para detectar falhas imediatas e ataques cibernéticos quanto para detectar diferenças no padrão de usos que servem como subsídio para possíveis soluções tempestivas para as tendências de variação de comportamento ao longo do tempo. Este processo utiliza o conceito de NPMD (Network Performance, Monitoring and Diagnostics) e BA (Behavior Analysis) com auxílio de inteligência artificial de propósito específico.

Título - Realidade Virtual e Gestão de Ativos, suportadas por modelagem granular aderente a Sistemas HVDC
Entidade(s) - Universidade Federal de Uberlândia,CENTRAIS ELETRICAS DO NORTE DO BRASIL S/A
Autor(es) - ALEXANDRE CARDOSO,Bruno Guilherme Resende Vaz de Melo,GERSON FLAVIO MENDES MENDES DE LIMA,Joao Batista Soares Feitosa,Gabriel Sousa Ferreira,Antonio Eduard Pereira da Silva
Resumo
Este artigo apresenta o desenvolvimento de um sistema de Realidade Virtual (RV) para a gestão do sistema HVDC Eletrobras Eletronorte (HVDC), utilizando modelagem geométrica granular e conceitos de Gêmeos Digitais. A solução busca aprimorar o monitoramento, manutenção e operação de componentes da sala de válvulas, por meio da combinação de RV e Gêmeos Digitais, com uso de ambientes virtuais fiéis às plantas, para facilitar o diagnóstico, a avaliação de falhas e medidas preventivas. Suportados por modelagem geométrica granular, que possibilita a criação de representações tridimensionais detalhadas dos componentes da planta, como transformadores e conversores, permitem-se análises individualizadas nos ambientes virtuais. Com possibilidade de constituição de Gêmeos Digitais, uma vez que recebe atualizações em tempo real sobre o ciclo de vida dos equipamentos, com acesso a dados dos sistemas SAP e SAGE, poderá ser utilizada para a análise preditiva, baseada em dados históricos e em tempo real, identificar padrões de desgaste e antecipar necessidades de intervenção, reduzindo custos e tempo de inatividade, enquanto a visualização em RV amplia a compreensão dos operadores sobre as condições da planta, melhorando a tomada de decisão e a resiliência da infraestrutura. Além disso, o sistema de RV oferece um ambiente de treinamento eficaz para operadores e engenheiros, aprimorando habilidades em simulações realistas e reduzindo riscos associados ao treinamento físico. Essa solução representa um avanço significativo na transformação digital do setor elétrico, promovendo maior eficiência operacional, segurança e integração entre monitoramento, manutenção e operação.
Perguntas e Respostas

O artigo descreve a colaboração dos engenheiros com o sistema. Qual foi a maior dificuldade na utilização da plataforma?

O artigo descreve a colaboração dos engenheiros com o sistema. Qual foi a maior dificuldade na utilização da plataforma?
Como toda solução de Realidade Virtual, há necessidade de computadores com placas gráficas específicas, além da necessidade de acesso às bases de dados da Concessionária.

Existe alguma pesquisa de aderencia da ferramenta? Ou uma pesquisa de mapemento de aceitação do operador?

Sim... ao longo do projeto, diversas iniciativas de validação da ferramenta, junto aos usuários finais, foram efetivadas.

O sistema pode ser adaptado a outros contextos além de HVDC, como subestações convencionais?
Sim... de fato, a estratégia aplica-se, de forma escalável, a outras plantas. Há exigência, para tal, do processo de modelagem paramétrica, insumos de CAD (entre outros) e acesso à bases de dados.

Título - Experiência da EVOLTZ no desenvolvimento de ferramenta para monitoramento e aumento da resiliência de Linhas de transmissão através de IoT
Entidade(s) - Concert Technologies S.A,Evoltz Participações S.A.
Autor(es) - Edson Nunes,Gabriela Prado Da Silva,JULIA DE OLIVEIRA BOTELHO,Keverson de Almeida Carvalho
Resumo
O presente artigo descreve o desenvolvimento de um protótipo de monitoramento remoto para torres de transmissão de energia elétrica, com foco na mitigação e no registro adequado de eventos críticos, como quedas de torres. A infraestrutura proposta integra sensores, câmeras, módulos de comunicação e algoritmos de inteligência artificial embarcados, operando de forma autônoma e contínua. A solução foi desenvolvida para mitigar os desafios operacionais enfrentados por transmissoras, como a ausência de dados históricos que contribuam para evidenciar a ocorrência de eventos extremos e que subsidiem ações de manutenção preventiva. O sistema utiliza comunicação via rede celular ou óptica, com protocolos seguros e integração com centros de operação. A primeira fase do projeto foi implantada na NBTE, com cinco protótipos instalados em torres localizadas no estado do Mato Grosso, validando as funcionalidades de comunicação, alimentação e detecção de intrusão. Apesar de limitações iniciais no modelo de visão computacional, posteriormente corrigidas, o sistema demonstrou potencial para ampliar a segurança, rastreabilidade e eficiência na operação de ativos de transmissão.
Perguntas e Respostas

Existe algum panorama para a implementação de sensores que consigam avaliar a degradação das torres?
A avaliação direta da degradação estrutural não é o foco principal do projeto em curso. O objetivo atual é detectar em tempo real eventos externos críticos, como vandalismo, queimadas, colisões e intempéries severas, que possam levar à queda imediata das torres. Ainda assim, a implementação de sensores voltados para

monitorar processos de degradação é viável (embora ainda não exista) e pode ser considerada em fases futuras do projeto. Alguns tipos de sensores e técnicas recomendadas para captura de estados de dano/degradação incluem:

Acelerômetros / sensores de vibração (MEMS): monitoram mudanças em respostas dinâmicas naturais (frequências próprias, amortecimento) que indicam perda de rigidez ou danos em elementos estruturais.

Sensores de inclinação / deslocamento angular (inclinômetros de alta precisão): detectam mudanças permanentes de geometria (inclinações) que sinalizam avanço de assentamentos ou empenamentos.

Extensômetros: medem esforços locais em estais, pernas e fundações.

Sensores de emissão acústica / ultrassom: detectam fissuras e trincas ativas e monitoram propagação de falhas em materiais metálicos.

Sensores de corrosão e monitoramento eletroquímico: para estruturas metálicas, medir taxa de corrosão é crítico.

Medição geotécnica nas fundações (inclinômetros de base, piezômetros): rastreiam mudanças no suporte da torre.

Monitoramento por imagem avançado (termografia, LIDAR, fotogrametria por drone): inspeciona perda de seção, empenamentos, falhas em isoladores e ancoragens.

Nesse sentido, a arquitetura de comunicação e a capacidade de processamento de borda não apenas já contempla os sensores de deslocamento angular, vibração e estações meteorológicas como parte do escopo, mas também permite a integração dos demais sensores mencionados sem mudança radical de infraestrutura.

O uso de IA foi implementado para identificação de imagens. Existe um panorama do uso de IA para prevenção de degradação da estrutura ?
O uso da inteligência artificial no projeto atual está voltado principalmente à segurança física das torres e à prevenção de eventos súbitos de queda, não ao acompanhamento da degradação progressiva. Ainda assim, a arquitetura foi concebida com flexibilidade para evoluir em fases posteriores.

Técnicas como anomaly detection em séries temporais, modelos preditivos de manutenção (estimativa de vida útil remanescente) e gêmeos digitais integrados a machine learning podem antecipar falhas e apoiar estratégias de manutenção preditiva. O protótipo já aplica visão computacional para detecção de pessoas e veículos no entorno, comprovando a viabilidade de embarcar algoritmos em campo. Essa base pode futuramente ser expandida para análise de dados estruturais, desde que sensores adicionais de degradação sejam integrados.

Existe um panorama de cruzamento de dados com relatórios de inspeção para mapear quais os fatores que promovem maior degradação das torres?
Atualmente, o sistema prioriza a detecção de ameaças externas e o registro preciso de eventos críticos de queda. Nesse sentido, embora o potencial de cruzamento de

dados para fins de manutenção preventiva e análise de degradação seja reconhecido, deve ser entendido como uma vertente futura de evolução tecnológica do protótipo.

Apesar disso, o cruzamento de dados de sensores, variáveis climáticas e imagens com relatórios de inspeção de campo é tecnicamente viável e representa um passo importante para identificar os fatores que mais contribuem para a degradação estrutural das torres. Técnicas de integração de dados (OCR, padronização de relatórios), análise estatística e aprendizado de máquina podem mapear correlações entre condições ambientais, esforços estruturais e ocorrência de danos. O protótipo já coleta dados que podem ser correlacionados com inspeções manuais, criando a base para esse tipo de análise.

Título - Aplicação de Técnicas de Inteligência Artificial na Estratégia Adaptativa como ferramenta para superar desafios na Proteção do Sistema Elétrico de Potência
Entidade(s) - GRID SOLUTIONS TRANSMISSAO DE ENERGIA LTDA,GENERAL ELECTRIC DO BRASIL LTDA
Autor(es) - Annelise Anderson Bittencourt,Rafael Cesar Jabor Fagundes Nogueira
Resumo
O trabalho técnico apresenta uma visão geral da utilização das técnicas de Inteligência Artificial nas estratégias adaptativas implementadas na proteção de Sistemas Elétricos de Potência. A geração atual de dispositivos eletrônicos inteligentes (IED – Intelligent Electronic Device) combinada com a interoperabilidade alcançada com a implementação das definições da norma IEC 61850 estão construindo a infraestrutura para a jornada da transformação digital, desta forma proporcionando a disseminação do uso de técnicas de inteligência artificial como estratégias adaptativas. Devido às diferentes características de cada técnica de IA, o presente trabalho apresenta os estudos em técnicas que estão sendo aplicadas em proteção adaptativa e nas que ainda não estão difundidas neste tipo de aplicação. O estudo teve ênfase nas seguintes técnicas: Sistemas Multiagentes, Redes Neurais, Sistemas Especialistas e Lógica Fuzzy e Machine Learning (ML). O objetivo do informe técnico é demostrar que com a aplicação dessas técnicas percebe-se uma melhoria no sistema de proteção, pois, alguns problemas antes sem solução são agora solucionados e antigas filosofias tornaram-se mais sofisticadas.
Perguntas e Respostas

Diante das particularidades do setor elétrico brasileiro — como a diversidade do parque gerador e a complexidade do sistema interligado nacional —, quais os principais desafios os autores enxergam para a implementação em larga escala das técnicas de IA em sistemas de proteção adaptativa? E como esses desafios poderiam ser superados nos próximos anos?
Com certeza as particularidades citadas são alguns dos desafios que a implementação em larga escala das técnicas de IA em sistemas de proteção adaptativa. O SIN é altamente complexo e integrado, ou seja, gera um grande volume de dados que envolvem proteção, controle e supervisão. Desta forma a implementação das técnicas de IA exigem e exigirão soluções que possam lidar com a vasta quantidade de dados e interconexões. A superação desse desafio envolve o desenvolvimento de algoritmos de IA mais robustos e escaláveis, capazes

de processar e analisar esses grandes volumes de dados em tempo real. Com relação a diversidade do parque gerador, visualizamos que é o ponto onde as técnicas de IA adaptativa entra com as suas vantagens, sendo que de acordo com essas características é fortemente determinante que os sistemas de proteção sejam adaptáveis a diferentes condições e características operacionais. Para a superação desse desafio, as técnicas de aprendizado de máquina podem ser treinadas para reconhecer padrões específicos de cada tipo de geração e ajustar as proteções conforme necessário. Considerando as redes neurais no âmbito de inteligência artificial (ou aprendizado de máquinas), as redes supervisionadas (onde se conhece as saídas durante o processo de treinamento), poderão contribuir de modo significativo na previsão / determinação das correntes de contribuição de curto-circuito e localização de faltas, por exemplo. Como a inserção das fontes não-convencionais de energia (solar, eólica e baterias), também chamadas de fontes interfaceadas via conversores, tem-se os sistemas conhecidos como Grid-Following e, atualmente, os chamados Grid-Forming. Há uma grande dificuldade para os algoritmos atuais dos relés de proteção disponíveis no mercado para o tratamento "temporal", uma vez que o tratamento "espacial" - via o uso da transformada de Fourier, não é mais suficiente, para alguns casos. Como exemplo, a grande maioria dos inversores não injetam sequência negativa e alguns injetam sequência negativa (a depender das exigências dos procedimentos de rede ao redor do mundo), portanto, o uso somente da transformada de Fourier fica comprometido, além disso, há problemas de tratamento de componentes interharmônicas e subharmônicas. Um exemplo: como a maioria dos relés de proteção utilizam janelas deslizantes entre 1 ciclo e 3 ciclos, a determinação de componentes subharmônicas, como 30 Hz por exemplo, exigiria uma janela de meio-ciclo, e assim por diante. Tais componentes subharmônicam podem, então, causarem vazamento espectral durante o processo de digitalização entre a passagem do domínio do tempo para a frequência e depois, novamente, para o domínio do tempo. Portanto, havendo a possibilidade de classificação e determinação de determinados fenômenos apontam o uso de IA ser muito promissor no curto-prazo, uma vez que os IEDs de proteção elétrica disponíveis no mercado ainda não estão preparados para trabalharem como outras técnicas de filtragem e processamento digital, como a transformada de Wavelet, por exemplo, a qual poderia trazer resolução espacial e temporal.

A terceira pergunta (entre as três) já enfatiza um dos principais desafios que os autores identificaram, cibersegurança, ou seja, confiabilidade e segurança dos dados. Garantir a confiabilidade e a segurança dos dados utilizados pelos sistemas de IA é crucial. A implementação de medidas rigorosas de segurança cibernética e protocolos de verificação de dados pode ajudar a mitigar riscos associados a falhas ou ataques. Assim como todas as inovações tecnológicas implementadas no setor elétrico outros dois desafios que a adoção de técnica de IA em proteções adaptativas deve enfrentar são as barreiras regulatórias e capacitação/treinamento de profissionais. A colaboração com órgãos reguladores para desenvolver normas e diretrizes que facilitem a integração de tecnologias de IA pode ajudar a superar a resistência e obstáculos. Com relação a capacitação, é necessário investir em programas de treinamento e educação contínua, para garantir que a força de trabalho esteja preparada para utilizar essas tecnologias de maneira eficaz. Para que todos esses desafios e obstáculos possam ser superados nos próximos anos, é essencial promover a pesquisa e o desenvolvimento de tecnologias em IA específicas para o setor elétrico, incentivar parcerias entre empresas, universidades e centros de pesquisa, e investir em infraestrutura tecnológica que suporte a

implementação dessas soluções.
Como conclusão, a criação de um ambiente regulatório favorável e o fortalecimento da segurança cibernética são fundamentais para que a IA possa ser integrada de forma segura e eficiente nos sistemas de proteção adaptativa.

Considerando o cenário atual dos sistemas de proteção em operação nas subestações, muitas ainda com um extenso legado amplo de equipamentos não modernizados, quais das técnicas apresentadas ou autores entendem que estão mais maduras para serem implementadas, sendo viáveis operacionalmente em um cenário tecnológico muitas vezes heterogêneo?
É importante conduzir avaliações detalhadas das condições atuais dos sistemas e estabelecer planos de integração que levem em conta a compatibilidade com equipamentos legados. O autores entendem que a viabilidade operacional de implementação de técnicas de IA deve levar em consideração a maturidade das tecnologias disponíveis e a capacidade de integração com sistemas heterogêneos. Os sistemas baseados em lógica fuzzy é especialmente útil em cenários onde a precisão e a clareza dos dados podem ser comprometidas devido à diversidade de equipamentos. Ela permite que decisões sejam tomadas com base em informações imprecisas ou incompletas, o que é ideal para sistemas heterogêneos. A técnica baseada em Redes Neurais são amplamente utilizadas por sua capacidade de aprender e se adaptar a diferentes padrões de operação. Elas podem ser implementadas gradualmente, começando com funções específicas de monitoramento e diagnóstico, permitindo que se integrem com sistemas existentes sem a necessidade imediata de substituir equipamentos legados. Algoritmos de Aprendizado de Máquina podem ser usados para análise de dados históricos e em tempo real, ajudando na identificação de padrões de falhas e na otimização dos sistemas de proteção. Esses algoritmos podem ser implementados em camadas superiores de gerenciamento de dados, sem exigir mudanças significativas na infraestrutura física já existente. Outro ponto que não está diretamente ligado aos sistemas de proteção e sim de monitoramento, são sistemas que utilizam IA para prever falhas ou necessidades de manutenção antes que ocorram, estas implementações são altamente valiosas em ambientes com equipamentos legados. Eles podem ajudar a prolongar a vida útil de equipamentos existentes e melhorar a confiabilidade operacional.

Sistemas baseados em inteligência artificial, como toda ampliação de uso tecnológico, também trazem preocupações em relação à cibersegurança, especialmente quando inseridos em funções críticas como proteção. Como os autores avaliam esse risco e como poderiam ser mitigados para garantir a segurança desses sistemas inteligentes aplicados à proteção elétrica?
Os sistemas baseados em inteligência artificial (IA) inseridos em sistemas de infraestruturas/funções críticas, como proteção elétrica, realmente trazem preocupações significativas em relação à cibersegurança. Os autores concordam que este seria um assunto para um novo estudo e apresentação de artigo relacionado ao tema, entendendo que a avaliação de risco e mitigação de riscos de cibersegurança são essenciais para a aplicação de técnicas de IA. Com relação a avaliação dos riscos os autores entendem que os sistemas de IA podem ser suscetíveis a ataques cibernéticos, incluindo manipulação de dados de treinamento ou alterações maliciosas nos algoritmos de decisão. A superfície de ataques

cibernéticos também aumenta com a interconectividade e complexidade dos sistemas de proteção baseados em técnicas de IA adaptativas e praticamente na mesma proporção a dependência de dados está na mesma curva crescente, desta forma, a segurança dos dados, tanto em termos de integridade quanto de confidencialidade, é crítica, pois esses dados são fundamentais para o funcionamento correto dos sistemas de IA, tornando a segurança uma prioridade. Entendemos que para mitigar esses riscos várias ações devem ser tomadas e mencionamos aqui apenas algumas destas, como: implementação de protocolos de segurança rigorosos como: criptografia de dados e autenticação multifatorial; implementação de sistemas de detecção de intrusão para identificar padrões de ataques; realizar avaliações de segurança regulares e auditorias para identificar e corrigir vulnerabilidades potenciais; trabalhar em colaboração com órgãos reguladores para desenvolver normas e diretrizes que garantam a segurança dos sistemas; e novamente capacitar profissionais em práticas de cibersegurança, garantindo que estejam preparados para lidar com possíveis ameaças e vulnerabilidades. Essas medidas de mitigação não são aplicáveis somente para sistema que possuem aplicação de IA, sendo que os sistema OT (Operational Technology) no sistema elétrico já se encontram em muitos casos vulneráveis a estes ataques mesmo sem a aplicação de técnicas de IA.

Título - Uso de Modelos não supervisionados para redução de falsos positivos em modelos de predição de falhas e de digital Twins em Hidrogeradores
Entidade(s) - RADIX ENGENHARIA E DESENVOLVIMENTO DE SOFTWARE S/A
Autor(es) - HUGO DINIZ REBELO,Arnaldo Mendes Pires Junior,Patrícia de Castro Wang,Mauricio Silva de Magalhães,Leonardo Tavares Vianna,KLEYTON PONTES COTTA,Hugo Reiser Vieira Portuita,Tassio Simioni
Resumo
Este estudo propõe o desenvolvimento de modelos de detecção de anomalias para unidades geradoras de usinas hidrelétricas, visando aprimorar a gestão de ativos por meio da implementação de técnicas de manutenção preditiva. A abordagem utiliza técnicas de aprendizado não supervisionado para identificar padrões anômalos, a partir da análise integrada de dados de diversos sensores. Os experimentos demonstraram que o modelo híbrido desenvolvido apresentou desempenho superior comparado a outras técnicas do estado da arte utilizadas, sendo subsequentemente aplicado no treinamento de modelos para detecção de falhas em hidrogeradores.
Perguntas e Respostas

Como o uso de modelos não supervisionados ajuda a reduzir a quantidade de falsos positivos nos sistemas de predição de falhas em hidrogeradores?

O uso de modelos não supervisionados pode ser explorado de diferentes maneiras para reduzir falsos positivos em sistemas de predição de falhas em hidrogeradores.

Uma primeira abordagem consiste em treinar um modelo não supervisionado com os mesmos dados que serão utilizados no modelo supervisionado. O modelo não supervisionado identifica agrupamentos dos dados ou sinaliza quando uma observação não pertence a nenhum grupo (anomalia). Essa informação é então incorporada ao modelo supervisionado, enriquecendo-o com a noção de correlação

e comportamento esperado das variáveis. Assim, o modelo supervisionado passa a considerar mais uma dimensão de contexto, o que reduz a chance de interpretações equivocadas e, consequentemente, de falsos positivos.

Outra abordagem possível é utilizar o modelo não supervisionado como um filtro prévio. Nesse caso, o modelo é treinado apenas com dados considerados normais. Se um novo dado for classificado como anômalo, ele não é repassado ao modelo supervisionado. Dessa forma, evita-se que ruídos ou falhas de aquisição de dados sejam interpretados como falhas reais, prevenindo falsos alarmes e aumentando a confiabilidade do sistema de predição.

Durante o desenvolvimento do modelo, foi destacado o uso de sensores de temperatura do trocador de calor como fonte dos dados. O autor identifica limitações na aplicação dessa metodologia em se tratando da expansão de seu uso para outros tipos de sensores ou outros equipamentos além dos hidrogeradores? Isso exigiria alguma adaptação significativa nos modelos ou na metodologia?
Não seria necessário alterar a metodologia em si. No entanto, para expandir a aplicação a outros tipos de sensores ou equipamentos além dos hidrogeradores, seria preciso realizar um estudo mais aprofundado para avaliar se as mesmas técnicas continuam adequadas. Isso poderia exigir ajustes nos hiperparâmetros e, sobretudo, novas estratégias de pré-processamento adaptadas às características específicas dos dados.

No caso dos sensores de temperatura do trocador de calor, por exemplo, o artigo destacou a importância do pré-processamento, que incluiu a decomposição sazonal por médias móveis e a normalização por quantis, garantindo a remoção de variações periódicas previsíveis e a preservação dos padrões operacionais relevantes. Para outros tipos de sensores ou equipamentos, seria necessário desenvolver abordagens equivalentes, capazes de realçar anomalias sem mascarar comportamentos normais.

No entendimento do autor, quais são os principais benefícios que o uso de inteligência artificial, como foi aplicado nesse trabalho, pode trazer para a operação e manutenção de usinas hidrelétricas além do que foi apresentado?
No meu entendimento, a principal contribuição desse trabalho vai além do uso do aprendizado não supervisionado "apenas" como apoio a modelos supervisionados. Sua aplicação possibilita explorar de maneira mais ampla as correlações entre as diversas variáveis monitoradas pelos sistemas de sensoriamento.

Tradicionalmente, sistemas de supervisão e controle (SCADA) emitem alarmes a partir de limiares fixos definidos para variáveis individuais. Embora prática, essa abordagem é limitada, pois ignora as interações entre diferentes parâmetros.

Com essas técnicas de agrupamento, torna-se possível identificar quando um dado não se enquadra em nenhum grupo esperado. Isso abre caminho para alarmes mais inteligentes e análises mais profundas das correlações entre variáveis, permitindo compreender de forma mais robusta o comportamento multivariado em ambientes complexos, como o de um hidrogerador.

No entendimento do autor, quais são os principais benefícios que o uso de inteligência artificial, como foi aplicado nesse trabalho, pode trazer para a operação e manutenção de usinas hidrelétricas além do que foi apresentado?

Título - ApplicationDrivenLearning.jl: Uma Biblioteca de Alto Desempenho para Treinamento de Modelos Preditivos no Contexto de Tomada de Decisão
Entidade(s) - FACULDADES CATOLICAS,PSR Soluções e Consultoria em Energia Ltda
Autor(es) - Giovanni Almeida Argento De Amorim,Joaquim Masset Lacombe Dias Garcia,Alexandre Street de Aguiar
Resumo
O framework Application-Driven Learning (em português, aprendizado dirigido pela aplicação) propõe uma abordagem de malha fechada que integra diretamente o treinamento de modelos preditivos com processos de tomada de decisão, otimizando os modelos especificamente para o contexto da aplicação. O setor elétrico utiliza, nas suas diversas atividades, sistemas de tomada de decisão baseados em previsões. Assim, apresentamos o ApplicationDrivenLearning.jl, uma biblioteca de código aberto desenvolvida em Julia que permite a representação flexível de processos do tipo "prever-planejar-avaliar" com suporte ao treinamento eficiente desses modelos. Neste artigo aplicamos o método ao problema de despacho econômico, que pode ser executado pelo operador a cada hora ou 15 minutos para programar a operação ótima das centrais de geração com alta acurácia e segurança. O pacote combina usabilidade, flexibilidade e precisão dos ecossistemas de otimização e aprendizado de máquina da linguagem Julia para representar, de forma integrada, modelos de decisão e previsão. O ApplicationDrivenLearning.jl é capaz de representar modelos com diferentes funções de custo e restrições, permitindo ao usuário modelar de forma precisa os processos de planejamento e avaliação bem como utilizar modelos preditivos univariados e multivariados – com ou sem variáveis exógenas. O treinamento pode ser realizado a partir de uma formulação exata de otimização binível ou uma abordagem heurística utilizando métodos de otimização com Nelder-Mead ou gradiente descendente, uma contribuição secundária deste trabalho. A interface fornecida é flexível, permitindo que usuários interessados implementem quaisquer modelos preditivos ou métodos de otimização desejados. O pacote reduz drasticamente as barreiras de acesso a essa nova tecnologia combinando facilidade de uso e métodos de solução de alta performance.
Perguntas e Respostas

O pacote apresentado propõe uma abordagem de malha fechada que integra previsão e decisão. Como você enxerga a adoção dessa abordagem em ambientes regulatórios?
A abordagem de malha fechada viabiliza que modelos preditivos sejam treinados e aplicados para processos de tomada de decisão como alternativa à abordagem de malha aberta, que em geral aplica modificações heurísticas, baseadas em intuição e pouco documentadas para gerar previsões mais aderentes a realidade das decisões a serem tomadas. O método também é alternativa a outros métodos de otimização estocástica, que em geral dependem de técnicas de geração de cenários baseada em dados históricos. Dessa forma, a nossa abordagem apresenta uma clara

vantagem na aplicabilidade e regulação, uma vez que 1) estabelece de forma precisa e com forte base teórica um método para gerar previsões adequadas à tomada de decisão, 2) elimina a dependência de métodos de geração de cenários e 3) permite a padronização do processo de tomada de decisão a partir de um modelo preditivo treinado.

Pensando em aplicações reais no setor elétrico, quais seriam, na sua opinião, os maiores desafios — técnicos ou institucionais — para a adoção do ApplicationDrivenLearning.jl
O principal desafio técnico seria o treinamento de um modelo preditivo adequado em casos de otimização inteira, dado que este caso é bastante comum em aplicações reais no setor elétrico e os métodos de treinamento apresentam limitações para esse tipo de variável. Possível agravante de complexidade nesse caso seria se o modelo treinado possuir muitos parâmetros, pois isso representa mais uma dificuldade para o processo de treinamento.
Institucionalmente, será desafiador 1) implementar processos que utilizem as previsões dadas pelo modelo treinado, uma vez que a previsão apresentará vieses e poderá fugir significativamente do padrão esperado para um modelo preditivo (sendo justamente esse o comportamento esperado) e 2) evitar as modificações humanas heurísticas que são tão comumente aplicadas nesse tipo de processo.

Na visão dos autores, que outros problemas operacionais ou de planejamento no setor elétrico poderiam se beneficiar diretamente dessa abordagem de aprendizado orientado pela aplicação?
Institucionalmente, o principal desafio é a mudança de paradigma necessária para aceitar previsões que são intencionalmente viesadas para otimizar a decisão final, em vez de apenas minimizar o erro estatístico. Este conceito contra-intuitivo pode gerar desconfiança e levar a intervenções manuais que anulam os benefícios do método. A solução passa pela disseminação do conhecimento e pela adoção de uma abordagem dual durante a transição: utilizar o modelo ADL para a tomada de decisão, enquanto um modelo tradicional de baixo erro serve para avaliação e benchmarking. Isso ajuda a construir confiança ao demonstrar quantitativamente que a previsão com "viés inteligente" resulta em uma operação com menor custo e maior segurança.

Na visão dos autores, que outros problemas operacionais ou de planejamento no setor elétrico poderiam se beneficiar diretamente dessa abordagem de aprendizado orientado pela aplicação?

Título - Uso de Inteligência Articial (IA) para Identificação dos Tempos Envolvidos nas Manobras de Disjuntores a SF6 da Subestação de Tijuco Preto
Entidade(s) - UNIVERSIDADE FEDERAL DE ITAJUBA,Universidade Federal de Itajuba,CENTRAIS ELETRICAS BRASILEIRAS SA ELETROBRAS,Centrais Elétricas Brasileiras - Eletrobras
Autor(es) - AURELIO LUIZ MAGALHAES COELHO,Philippe Augusto Varme Dias Liz,Giovani Bernardes Vitor,Ricardo Tozzi de Lima,Ana Cristina de Freitas Marotti,Clayton Duarte Pessoa,Hamilton Batista de Oliveira
Resumo

Um dos principais problemas relacionados aos disjuntores que operam com bancos de capacitores está relacionado à manobra de fechamento que pode gerar elevados transitórios. Isto pode causar danos e desgaste prematuro aos disjuntores e aos equipamentos da rede a eles conectados. Este trabalho apresenta uma abordagem baseada em processamento de sinais e Inteligência Artificial (IA) para identificar os instantes de entrada do resistor de pré-inserção e do contato principal durante a operação de um disjuntor de alta tensão a SF6. Para isso, os sinais de corrente de um disjuntor de 345 kV da Subestação de Tijuco Preto são utilizados como entradas dos modelos baseados em IA considerando os ruídos e interferências comuns neste tipo de ambiente. A modelagem proposta considera as etapas de pré-processamento do sinal com técnicas de filtros de sinais para reduzir ruídos e destacar características relevantes para extração de características, a geração do conjunto de dados para treinamento, e quatro modelos de aprendizado de máquina para avaliação, todos treinados para identificar automaticamente os pontos críticos do sinal e, por fim, a identificação dos melhores momentos para comutação controlada dos disjuntores. Os resultados demonstraram que o melhor modelo alcançou 96% de acurácia e indicam que as técnicas apresentadas são robustas para uso em ambientes reais, permitindo prever falhas com maior confiabilidade, otimizar a manutenção e reduzir custos operacionais. Assim, o trabalho contribui diretamente para a melhoria do sincronismo de fechamento em disjuntores de alta tensão e a mitigação de transientes críticos no sistema elétrico.

Perguntas e Respostas

Mesmo com acurácia e precisão próximas de 96% para os modelos AdaBoost e MLP, como poderiam ser mitigados erros residuais na identificação do contato principal durante uma manobra real? Há algum tipo de validação ou alarme previsto para casos de classificação incorreta?

Com relação aos erros residuais, os mesmos podem ser mitigados incorporando sinais adicionais ao modelo, ao invés de somente a corrente na fase do disjuntor. Por exemplo, a tensão na fase.

Com relação a validação através de alarmes para casos de classificação incorreta, é possível, mas ainda não foi implementado.

Durante a construção do modelo, foram destacados desafios relacionados a ruídos e interferências no ambiente real da subestação, que dificultam a identificação dos eventos no sinal. Na sua visão, quão generalizável é essa solução para outros disjuntores, subestações ou até para outros tipos de manobras? O modelo precisaria ser reconfigurado para cada cenário ou há possibilidade de uma aplicação mais ampla?

Na nossa visão, o modelo foi treinado para disjuntores SF6 de alta cadência com resistor de pré-inserção que manobram bancos de capacitores. Portanto, trata-se de uma solução específica para tal arranjo. É possível realizar uma generalização para outros disjuntores, subestações ou até para outros tipos de manobras, desde que se tenha os dados destes para realização adequada do treinamento do modelo.

O trabalho apresentou uma abordagem baseada na análise dos sinais de corrente, especialmente para identificar os instantes de pré-inserção e de fechamento do contato principal. Considerando que atualmente essa análise é

feita de forma manual por especialistas, como você avalia o impacto da automação desse processo na rotina das equipes de operação e manutenção? Os autores consideram que a análise humana ainda deve ser preservada, sendo apoiada pela IA, ou a IA já poderia assumir esse papel de forma autônoma?
Na nossa visão, o modelo apresentado serve como uma ferramenta complementar para auxiliar os operadores e mantenedores nas tomadas de decisão no processo de manutenção preditiva de disjuntores, sem substituir as atividades de campo necessárias.

Título - Aplicação de Inteligência Artificial para Detecção de Intrusões e Anomalias em Tempo Real em Sistemas de Controle Industrial
Entidade(s) - TI Safe Segurança Cibernética Industrial LTDA
Autor(es) - Marcelo Ayres Branquinho
Resumo
A crescente digitalização e interconexão de sistemas industriais trouxe desafios significativos para a segurança cibernética, especialmente no setor de energia. Com a integração de dispositivos IoT e automação, infraestruturas críticas tornaram-se alvos de ataques sofisticados, como ransomware e APTs (Ameaças Persistentes Avançadas) . A necessidade de resposta rápida e eficiente a incidentes exige soluções avançadas baseadas em Inteligência Artificial (IA) , combinando monitoramento contínuo e automação para fortalecer a defesa cibernética.
Este informe técnico investiga a aplicação da IA no aprimoramento da resposta a incidentes em Security Operations Centers (SOCs) , destacando o impacto do uso da Inteligência Artificial na redução do tempo médio de resposta (MTTR) e na otimização da gestão de incidentes de segurança.
Perguntas e Respostas

Qual é a principal limitação atual da plataforma Safer no que diz respeito à escalabilidade para empresas menores do setor elétrico, que possuem menos recursos tecnológicos e humanos? Seria aplicável caso não exista um SIEN implantado, por exemplo?

A principal limitação da plataforma Safer para empresas menores do setor elétrico é a dependência de fontes estruturadas de dados de segurança, como logs consolidados por SIEMs. Sem um SIEM implantado, a capacidade do Safer de aplicar inteligência artificial para correlação, enriquecimento e automatização da resposta a incidentes fica comprometida. No entanto, é possível adaptar a solução para operar em ambientes com menor maturidade tecnológica, desde que exista ao menos uma geração mínima de logs por firewalls ou EDRs, permitindo uso parcial das funcionalidades do Safer, com foco em apoio à triagem, capacitação e resposta assistida por IA.

Considerando o risco de ataques coordenados e a criticidade do setor elétrico, como a plataforma Safer poderia contribuir no caso de ameaças tipo zero-day, ainda não possuem assinaturas conhecidas nos bancos de dados disponíveis?

A plataforma Safer contribui significativamente na detecção de ameaças do tipo zero-day ao utilizar técnicas de aprendizado de máquina e análise comportamental para identificar padrões anômalos de atividade, mesmo quando não há assinaturas conhecidas. Diferente dos sistemas tradicionais baseados exclusivamente em assinaturas, o Safer correlaciona eventos com base em comportamento histórico, variações de tráfego, contexto operacional e dados externos como OSINT e reputação de IPs e domínios. Assim, mesmo que uma ameaça não esteja registrada em fontes como VirusTotal ou XForce, desvios anômalos podem ser detectados e categorizados como suspeitos, acionando investigações antecipadas e resposta coordenada. Essa abordagem é particularmente valiosa no setor elétrico, onde a detecção proativa é vital para evitar impactos em cascata.

Como é garantida a segurança e a privacidade dos dados processados na nuvem, especialmente em relação à dependência de serviços externos como a OpenAI? Existem estratégias de mitigação para riscos de vazamento de dados ou compliance regulatório?
A segurança e a privacidade dos dados processados pelo Safer são garantidas por uma arquitetura híbrida, onde a maior parte do processamento ocorre localmente em um servidor instalado na DMZ do cliente, e apenas tarefas específicas são encaminhadas à nuvem. Para essas tarefas, utiliza-se uma instância dedicada da OpenAI, com conexões seguras e políticas rígidas de isolamento e confidencialidade. Dados sensíveis permanecem on-premises, e o processamento em nuvem é limitado a informações despersonalizadas ou previamente tratadas, garantindo conformidade com normas como a RO-CB.BR.01 e a IEC 62443. Como estratégia de mitigação, o Safer pode ser configurado para operar em modo totalmente local (air-gapped), quando exigido por políticas de segurança ou compliance regulatório, assegurando controle total sobre os dados críticos.

Título - ChatDGA - Uma ferramenta contextual para auxílio no aprendizado técnico e análise dos resultados do ensaio DGA
Entidade(s) - Phasor,Genesis Pesquisa e Desenvolvimento LTDA
Autor(es) - Daniel Carrijo Polonio Araujo,Gabriel de Souza Pereira Gomes,Victor Rios Belarmino,Rafael Prux Fehlberg,IONY PATRIOTA DE SIQUEIRA
Resumo
A cromatografia gasosa (CG) é uma das principais ferramentas de manutenção preditiva para transformadores de potência, permitindo a detecção antecipada de falhas internas. No entanto, a interpretação dos dados de CG requer conhecimento técnico especializado e análise normativa. Este artigo apresenta o desenvolvimento de um agente inteligente baseado em modelos de linguagem de grande escala (LLMs), especificamente o LLAMA V3.2 1B, treinado por meio de fine-tuning com dados históricos de CG, normas técnicas (IEC 60599 e IEEE C57.104) e literatura especializada. O modelo resultante é capaz de interpretar automaticamente os resultados de CG, identificar prováveis falhas, sugerir ações corretivas e redigir relatórios técnicos de forma padronizada. Testes realizados com mais de 12 laudos demonstraram 87% de acurácia nos diagnósticos e 81% de conformidade normativa. O agente não visa substituir o especialista, mas atuar como ferramenta de apoio à decisão, viabilizando análises em larga escala e aumento da eficiência operacional. Os resultados indicam o potencial da inteligência artificial na modernização da

manutenção de transformadores, abrindo caminho para sua integração em sistemas supervisórios e aplicações industriais em larga escala.

Perguntas e Respostas

Qual foi a maior dificuldade em padronizar os dados de laudos técnicos, normas e entre outros dados de pré-processamento ?

A principal dificuldade esteve na heterogeneidade das fontes de dados e na ausência de um formato normativo unificado entre os diferentes tipos de documentos:

- Laudos técnicos: variavam amplamente em estrutura (tabelas, texto corrido, PDFs escaneados) e terminologia — mesmo dentro da mesma concessionária, havia divergências na nomenclatura de gases e unidades (ppm vs %).
- Normas técnicas (IEC 60599, IEEE C57.104): apresentavam estruturas descritivas e linguísticas distintas, exigindo extração semântica e mapeamento manual para converter trechos textuais em regras operacionais parametrizáveis (ex.: faixas de concentração, relações entre gases, limites de severidade).
- Dados históricos: a curadoria precisou lidar com ruídos, lacunas temporais e resultados inconsistentes (ex.: duplicidades ou medições com erro de calibração).
- O processo de anotação supervisionada exigiu a criação de um vocabulário técnico controlado e uma taxonomia unificada de falhas (PD, arco, sobreaquecimento, envelhecimento, normalidade) para permitir que o modelo aprendesse padrões de forma coerente.

Realmente o principal desafio foi transformar um conjunto semiestruturado, normativo e textual em um dataset coerente, numérico e linguístico, apto ao fine-tuning de um modelo de linguagem.

Para integração desse sistema com sistemas supervisórios, esse modelo de coleta de dados deverá passar por alguma revisão ou é possível coletar os dados a partir de um banco de dados do SAGE, por exemplo?

A integração é tecnicamente viável, mas requer ajustes de estrutura e semântica nos dados de entrada:

- O modelo atual foi treinado para receber entradas tabulares ou textuais estruturadas, simulando o formato de laudos técnicos.
- Sistemas supervisórios como o SAGE (Sistema Aberto de Gerenciamento de Energia) armazenam dados de sensores, alarmes e eventos em bancos relacionais ou SCADA historians, onde as amostras de cromatografia podem estar em diferentes granularidades e formatos.
- Para integração direta, seria necessário um módulo de pré-processamento automatizado, responsável por:
-- Converter as medições brutas de gases (H2, CH4, C2H4, etc.) em um formato compatível com os prompts do modelo.
-- Incluir metadados contextuais (equipamento, data, última intervenção, local da amostragem).
-- Aplicar filtros de consistência e detecção de outliers.
-- O modelo não precisaria ser re-treinado, apenas adaptado no front-end de ingestão de dados, de modo que as entradas do SAGE (ou de outro supervisório)

sejam transformadas em prompts equivalentes aos usados nos testes.

Portanto, não há necessidade de reformular o modelo, apenas revisar a camada de integração e coleta, garantindo compatibilidade semântica e temporal com o banco de dados do SCADA/SAGE.

Existe algum motivo especifico para a escolha do LHAMA 3.2 1B?
A escolha do LLAMA 3.2 1B foi fundamentada em três critérios principais:

- Equilíbrio entre desempenho e custo computacional: O modelo possui cerca de 1 bilhão de parâmetros, oferecendo boa capacidade contextual sem exigir infraestrutura massiva (pode operar em GPU única A100). Isso o torna viável para aplicações industriais e embarcadas, diferentemente de versões maiores (7B, 13B ou 70B) que demandariam clusters de GPU e inviabilizariam o uso em campo.
- Arquitetura aberta e adaptável: Por ser open source (Meta AI) e compatível com bibliotecas como Hugging Face Transformers, PEFT e LoRA, o LLAMA 3.2 1B facilita o fine-tuning eficiente com parameter-efficient methods, reduzindo tempo de treinamento e consumo de memória. A estrutura Transformer decoder-only é ideal para tarefas de geração técnica contextual, como interpretação de laudos e elaboração de relatórios.
- Aderência ao domínio técnico especializado: Testes preliminares mostraram que modelos muito pequenos (= 500 M parâmetros) apresentavam baixa retenção de linguagem normativa, enquanto modelos maiores (> 7B) não agregavam ganhos proporcionais de acurácia para textos curtos e altamente estruturados. O tamanho 1B foi o ponto ótimo entre context length, coerência técnica e eficiência computacional.

A escolha do LLAMA 3.2 1B foi amparada por sua capacidade de aprendizado contextual técnico com custo computacional industrialmente viável e por permitir treinamentos e inferências locais sem depender de serviços de nuvem proprietários.

Título - Avaliação de Inteligência Artificial com Mecanismo de Atenção na Detecção de Ataques de Injeção de Dados Falsos em Sistemas de Potência
Entidade(s) - universidade federal de campina grande,Associacao Tecnico Cientifica Ernesto Luis de O Junior
Autor(es) - Igor Monteiro Abreu dos Santos,George Rossany Soares de Lira,pablo bezerra vilar
Resumo
A modernização dos sistemas elétricos e a transição para redes inteligentes (Smart Grids) trouxeram grandes avanços na gestão de energia, mas também ampliaram a vulnerabilidade a ataques cibernéticos. A digitalização das redes elétricas, embora traga benefícios, expõe os sistemas a ameaças como os ataques de injeção de dados falsos (FDI), que comprometem a precisão das medições e, por conseguinte, a estimativa do estado do sistema. Esses ataques são difíceis de detectar por métodos convencionais, que não identificam desvios causados por ataques coordenados, aumentando o risco de falhas operacionais. Diante desse cenário, este trabalho propõe uma metodologia baseada em autoencoders com mecanismo de atenção para detectar ataques FDI em redes elétricas. A combinação desses dois recursos permite identificar anomalias de forma precisa, destacando variáveis chave

para detectar padrões de ataque. A abordagem foi validada com dados de sistemas IEEE-14 e IEEE-118 barras, incluindo ataques FDI gerados por uma Rede Generativa Adversarial (GAN), permitindo simular cenários mais realistas. Os resultados demonstraram a eficácia do modelo, especialmente no sistema IEEE-14, e sua capacidade de adaptação a ambientes complexos, como no IEEE-118, onde foi crucial distinguir entre falhas operacionais e ataques cibernéticos. O modelo proposto contribui para a segurança das redes elétricas ao melhorar a detecção de ameaças em sistemas de potência.

Perguntas e Respostas

Considerando que ataques de injeção de dados falsos ainda são pouco detectados por métodos tradicionais, como você enxerga a importância de soluções baseadas em inteligência artificial, como a que foi apresentada, para o futuro da segurança nas redes elétricas inteligentes?

A importância de soluções baseadas em inteligência artificial (IA), como o autoencoder com mecanismo de atenção proposto, é fundamental para o futuro da segurança em redes elétricas inteligentes. Os métodos tradicionais de detecção, baseados em regras fixas e modelos matemáticos simplificados, são limitados para identificar ataques coordenados e sutis, como os de injeção de dados falsos (FDI), que podem passar despercebidos por técnicas convencionais de detecção de resíduos.

A IA, especialmente técnicas de deep learning não supervisionadas, permite analisar grandes volumes de dados em tempo real, identificar padrões complexos e adaptar-se a novas ameaças sem depender de dados rotulados. A abordagem proposta, por sua vez, não apenas aumenta a precisão na detecção de anomalias, mas também reduz a dependência de modelos físicos detalhados e de extensos conjuntos de dados rotulados, que são inviáveis em sistemas reais. Além disso, a integração de mecanismos de atenção permite que o modelo priorize variáveis críticas do sistema (como tensão em barras estratégicas), aumentando a sensibilidade a manipulações sutis. Isso torna a detecção mais eficiente e adaptável, essencial para proteger infraestruturas críticas contra ataques cibernéticos cada vez mais sofisticados.

No contexto brasileiro, onde o sistema elétrico é amplamente digitalizado, conectado e dependente de medições remotas, soluções como essa são necessárias para garantir a confiabilidade operacional, a estabilidade do sistema e a segurança energética.

Embora os resultados para o IEEE-118 sejam muito bons, a ocorrência de falsos positivos não é desprezível. Como os autores avaliam que estes resultados podem ser aprimorados?

Os autores reconhecem que, embora o modelo tenha apresentado excelente desempenho no sistema IEEE-118 barras (com 100% de detecção de ataques), a ocorrência de falsos positivos, ou seja, a identificação incorreta de medições normais como anomalias, ainda é um desafio. Atribuímos isso principalmente à complexidade do sistema e à presença dos cenários de falhas no conjunto de dados que podem ser confundidas com ataques e dificultar a detecção. Embora, sabemos que a presença desses cenários torna a detecção mais próxima possível do real. Para aprimorar esses resultados, algumas adaptações nos modelos serão

analisadas futuramente:

Limiares adaptativos: Em vez de usar um limiar fixo (como o 97º percentil), propõe-se o uso de thresholds dinâmicos que se ajustam automaticamente às condições operacionais do sistema, considerando flutuações normais e contextos específicos.

Análise de ataques mais sofisticados: Testar o modelo contra vetores de ataque ainda mais realistas e direcionados, gerados por técnicas avançadas como GANs aprimoradas, para aumentar a eficiência do modelo.

Integração com sistemas de controle: Acoplar o modelo a sistemas de alarme e controle em tempo real, permitindo que os operadores recebam alertas contextuais e priorizados, reduzindo a dependência de limiares estáticos e melhorando a tomada de decisão.

Além disso, os autores planejam validar o modelo em simulação em tempo real e também com dados reais do sistema elétrico brasileiro, o que permitirá ajustes mais finos e uma melhor calibração para ambientes operacionais complexos e heterogêneos.

Embora os resultados para o IEEE-118 sejam muito bons, a ocorrência de falsos positivos não é desprezível. Como os autores avaliam que estes resultados podem ser aprimorados?
Os autores reconhecem que, embora o modelo tenha apresentado excelente desempenho no sistema IEEE-118 barras (com 100% de detecção de ataques), a ocorrência de falsos positivos, ou seja, a identificação incorreta de medições normais como anomalias, ainda é um desafio. Atribuímos isso principalmente à complexidade do sistema e à presença dos cenários de falhas no conjunto de dados que podem ser confundidas com ataques e dificultar a detecção. Embora, sabemos que a presença desses cenários torna a detecção mais próxima possível do real. Para aprimorar esses resultados, algumas adaptações nos modelos serão analisadas futuramente:

Limiares adaptativos: Em vez de usar um limiar fixo (como o 97º percentil), propõe-se o uso de thresholds dinâmicos que se ajustam automaticamente às condições operacionais do sistema, considerando flutuações normais e contextos específicos.

Análise de ataques mais sofisticados: Testar o modelo contra vetores de ataque ainda mais realistas e direcionados, gerados por técnicas avançadas como GANs aprimoradas, para aumentar a eficiência do modelo.

Integração com sistemas de controle: Acoplar o modelo a sistemas de alarme e controle em tempo real, permitindo que os operadores recebam alertas contextuais e priorizados, reduzindo a dependência de limiares estáticos e melhorando a tomada de decisão.

Além disso, os autores planejam validar o modelo em simulação em tempo real e também com dados reais do sistema elétrico brasileiro, o que permitirá ajustes mais finos e uma melhor calibração para ambientes operacionais complexos e

heterogêneos.

Título - Estudos de cibersegurança utilizando plataforma de simulação ciberfísica.
Entidade(s) - OPAL-RT BRASIL TECNOLOGIA LTDA,Universidade Federal do Paraná
Autor(es) - Thais Marzalek Blasi,MARCELA RIBEIRO GONÇALVES DA TRINDADE,Rita de Cássia Kwiek De Pasquale de Souza,Miguel Cervantes Martinez,Mehrdad Kazemtabrizi,Raphael Marzalek Blasi
Resumo
A crescente digitalização das redes elétricas ampliou sua exposição a ameaças cibernéticas, exigindo abordagens que integrem as dimensões física e de comunicação como um Sistema Ciberfísico (CPS). Este trabalho apresenta uma plataforma avançada de co-simulação CPS em tempo real, combinando ferramentas da OPAL-RT, para modelagem elétrica, EXataCPS para emulação da comunicação, com o objetivo de avaliar a resiliência cibernética de redes elétricas. Três estudos de caso foram desenvolvidos. O primeiro simula PMUs comunicando-se com o centro de controle via protocolo C3.118, permitindo a análise de ataques de negação de serviço e manipulação de pacotes. O segundo avalia uma microrrede com troca de mensagens IEC61850 GOOSE entre os REDs e o controlador, observando os impactos de ataques na operação da rede. Já o terceiro caso envolve a GHOST microgrid, com co-simulação ciberfísica e controle implementado em um IED real (SEL 3360), onde se aplicaram ataques como atrasos e alteração de pacotes, avaliando a resposta do controlador e os efeitos sobre tensão e frequência. A plataforma permite emular cenários complexos sem riscos operacionais, sendo útil para desenvolvimento de contramedidas e avaliação da resiliência de sistemas elétricos diante de ameaças cibernéticas. Destaca-se sua capacidade de integrar dinâmicas de controle, comunicação e equipamentos reais.
Perguntas e Respostas

Diante da crescente adoção de tecnologias baseadas em inteligência artificial, existe alguma perspectiva de integração da plataforma com técnicas de IA para detecção e resposta autônoma a ameaças durante as simulações?

Sim, é possível integrar técnicas de IA via Python para comunicar com as variáveis da simulação em tempo real. Dessa forma, é possível aplicar ataques cibernéticos à rede de comunicação, ver o impacto na operação e treinar IAs para detecção desse comportamento e suporte à tomada de decisão para esses eventos.

O ensaio foca bastante em ataques pontuais (como man-in-the-middle ou atrasos de comando), mas ataques avançados persistentes (APTs) são mais próximos da realidade de ameaças direcionadas a infraestruturas críticas. Os autores entendem que a plataforma de co-simulação poderia ser adaptada para lidar com ataques persistentes, que combinam diferentes vetores e ocorrem em múltiplas camadas ao longo do tempo?

Nesse momento a plataforma permite a realização de ataques sistematizados por meio de rotinas para aplicação de ataques, que permitem a realização de ataques

sequenciais em diferentes camadas e com durações previamente especificadas nas configurações dos ataques.

A segurança cibernética vem ganhando cada vez mais visibilidade na realidade do setor elétrico, mas ainda encontra dificuldades para se estabelecer, frente à prevalência da disponibilidade que difere a operação. Na visão dos autores, como a implementação de ambientes de simulação ciberfísica pode ser usada de forma rotineira no apoio à análise de riscos cibernéticos?
O uso da plataforma CPS permite que o operador defina estratégias e esteja preparado para identificar quando se trata de uma anomalia na rede ou quando essa é decorrente de um ataque cibernético. Considerando a digitalização das redes elétricas e consequentemente o aumento da vulnerabilidade dessas a ataques cibernéticos, a plataforma CPS permite também uma réplica da estrutura que se tem em campo, permitindo avaliar o comportamento da rede elétrica e de comunicações, em termos de sua confiabilidade e segurança.

Título - Aplicação de um Modelo de Análise de Ferramentas de Segurança Cibernética no Projeto de Atualização da Subestação da Margem Direita da ITAIPU Binacional
Entidade(s) - ITAIPU,ITAIPU BINACIONAL,ITAIPU Binacional
Autor(es) - ALDO INSFRAN,Marcos Fonseca Mendes,Emilio Arteta
Resumo
Este artigo apresenta um modelo de análise utilizado para a segmentação lógica e identificação de ferramentas de segurança cibernética para a Subestação Margem Direita (SEMD) no âmbito do Projeto de Atualização Tecnológica (PAT) da ITAIPU Binacional. Esse modelo segue a norma IEC 62443 e é baseado em um estudo de análise de risco para a subestação. Além disso, a arquitetura segura para o sistema elétrico é observada na norma IEC 62351, com a identificação de controles de segurança. O trabalho apresenta um desenvolvimento de referência no qual são identificados os componentes típicos da subestação, cenários de risco associados, níveis de risco diferenciados e níveis de segurança máximos, toleráveis e requeridos. Neste processo foram identificados e analisados oito zonas, quatro subzonas e cinco conduítes. Nove controles ou requisitos de sistema foram considerados para uma zona de referência, que determinaram cinco ferramentas e oito critérios. Esses resultados orientam a definição do escopo de fornecimento de equipamentos e serviços de segurança cibernética no PAT da SEMD. O método abordado no trabalho apresenta vantagens com relação aos métodos convencionais, com relação à documentação, escalabilidade e melhoria contínua.
Perguntas e Respostas

No estudo de caso apresentado, como a metodologia baseada na norma IEC 62443 facilitou a elaboração das especificações técnicas para os sistemas de segurança cibernética? Quais foram os ganhos concretos da abordagem normativa adotada?
A norma IEC 62443 serviu como espinha dorsal para converter a análise de riscos em requisitos técnicos objetivos, padronizados e alinhados a boas práticas internacionais. O principal ganho foi a clareza, a rastreabilidade e o foco no risco, resultando em especificações mais robustas e amplamente aceitas.
Essa metodologia supera a abordagem tradicional, ao transformar a seleção de

ferramentas de segurança, de um processo ad hoc, em uma decisão técnica estruturada, proporcional ao risco e em conformidade com padrões internacionais.

Como a segmentação em zonas e conduítes contribuiu, na prática, para a definição das ferramentas de segurança mais adequadas?
A segmentação da arquitetura da subestação em zonas e conduítes forneceu uma estrutura orientada a risco que guiou definição das ferramentas de segurança cibernética.
Agrupando ativos com criticidade semelhantes em zonas e mapear as interconexões por meio de conduítes, foi possível atribuir níveis de segurança-alvo (SL-T) e, a partir deles, determinar a classe adequada de controles para cada zona e conduíte (Z&C). Por exemplo, Z&Cs com SL-T mais elevados justificaram a implementação de controles como firewalls industriais com inspeção profunda de pacotes, gateways seguros, sondas IDS/IPS ou diodos de dados. No entanto Z&Cs menos críticos puderam ser protegidos com mecanismos mais simples, como ACLs ou segmentação VLAN.

O estudo considerou o cenário de uma implementação "green-field". Como os autores veem a possibilidade de adoção dos conceitos apresentados em uma subestação existente, com um legado de equipamentos heterogêneo e em diferentes estágios evolutivos em operação?
O modelo proposto baseado em risco também pode ser aplicado em subestações legadas desde que de forma incremental. A segmentação em zonas e conduítes funciona como diagnóstico inicial, permitindo mapear vulnerabilidades e definir níveis de segurança-alvo (SL-T) compatíveis com restrições do legado. Onde não é viável substituir equipamentos, podem ser aplicados controles compensatórios como firewalls industriais, diodos de dados, jump servers, segmentação lógica via VLANs, proxies de protocolo e monitoramento passivo (IDS/NSM). Essa abordagem progressiva garante mitigação de riscos em cada Z&C, favorece a padronização dos controles de segurança e prepara a arquitetura existente para evoluções futuras alinhadas as normas IEC 62351 e IEC 61850.

Título - Repositório de incidentes de segurança cibernética para investigação de ameaças no setor elétrico
Entidade(s) - Universidade Federal de Santa Maria
Autor(es) - Luiz Fernando Freitas-Gutierres,Arthur Johann Rohrig,Richard Siqueira da Rosa,João Henrique Barreto Correa ,Will Thomas
Resumo
Este trabalho apresenta o Cyber Incident Tracker for Electric Power Systems (CITEPS), um repositório de acesso aberto voltado à catalogação de incidentes de segurança cibernética no setor elétrico. O repositório reúne 49 incidentes identificados por meio de inteligência de fontes abertas, com foco em eventos que afetam ativos de tecnologias operacionais e sistemas de controle industrial. No CITEPS, as ocorrências são organizadas conforme atributos como instituição afetada, ator de ameaça, severidade do incidente, arsenal cibernético mobilizado e táticas empregadas pelos atores maliciosos. Os resultados evidenciam o predomínio de ataques de ransomware em diferentes contextos. O CITEPS contribui para o fortalecimento da inteligência de ameaças cibernéticas, oferecendo subsídios para o

desenvolvimento de estratégias defensivas, avaliações de risco e simulações de adversários voltadas ao setor elétrico.

Perguntas e Respostas

O trabalho apresentou o CITEPS como uma ferramenta aberta e colaborativa. Como você enxerga a participação de agentes do setor elétrico nesse processo de alimentação e uso do repositório? Como superar as barreiras institucionais que possam existir?

O autor acredita que o CITEPS poderia ser integrado a programas de treinamento ou simulações de cibersegurança no setor elétrico? Que tipo de uso prático poderia ser feito com a ferramenta no dia a dia das empresas do setor?

Sim, o CITEPS apresenta potencial de integração a programas de treinamento e simulações de cibersegurança no setor elétrico. Um de seus objetivos é oferecer uma base sistematizada de inteligência, capaz de subsidiar a modelagem de cenários realistas de ataque e defesa. Estão previstos, até o final do ciclo de inteligência, roteiros de wargames a serem incorporados ao CITEPS.

Como os autores enxergam a participação de agentes do setor elétrico no processo de alimentação e uso do repositório? Como superar as barreiras institucionais e eventuais resistências que possam existir?

Neste ciclo de inteligência, o CITEPS concentrou-se na análise e coleta de conhecimento sobre incidentes cibernéticos a partir de informações disponíveis em domínio público e obtidas por meio de open-source intelligence (OSINT). No próximo ciclo, as investigações avançarão para ambientes da Deep e Dark Webs. Nesses casos, está previsto o estabelecimento de contato direto com as organizações do setor elétrico antes da divulgação de qualquer ocorrência no CITEPS. Em outro viés, o CITEPS também pode servir como modelo para o intercâmbio de informações sobre incidentes em canal privado entre as empresas, uma vez que a cibersegurança constitui um desafio coletivo.

A análise de dados do CITEPS evidencia padrões de atuação dos atores de ameaça, com o uso recorrente de phishing, mídias removíveis e exploração de acessos remotos. Dessa forma, como os autores avaliam a efetividade das atuais estratégias adotadas no setor? Quais os principais pontos de atenção?

Os autores reconhecem que há um esforço significativo do setor como um todo na adoção de boas práticas de segurança cibernética. Algumas organizações já demonstram maturidade elevada, com centros de operações de segurança ativos e uso de inteligência de ameaças cibernéticas para aprimorar suas estratégias de defesa. Entretanto, ambientes de TO-ICS ainda enfrentam desafios relevantes, como a presença de tecnologias legadas, a aplicação tardia ou inexistente de correções de segurança (patching), além da existência de organizações que carecem até mesmo de princípios básicos de cibersegurança. Como evidenciado no trabalho, apenas 25% das empresas investem em iniciativas de capacitação em cibersegurança voltadas a seus recursos humanos (dados de 2024), ao passo que phishing e spearphishing permanecem entre os principais vetores de ataque.

Título - Solução de segurança de rede em um Sistema Especial de Proteção de grande porte: SEP das Interligações Norte-Nordeste-Sudeste
Entidade(s) - Operador Nacional do Sistema Elétrico,Autarquia Federal,Ysmart Engenharia Capacitacao e Tecnologia LTDA,SCHWEITZER ENGINEERING LABORATORIES COMERCIAL LTDA
Autor(es) - Igor de Siqueira Cardoso,Yona Lopes,Natalia Castro Fernandes,Helio do Nascimento Cunha Neto,Marcos Vinicius Guimaraes Cabral,Felipe Serazzi Melchert,Ricardo Abboud,Fábio Bruns Ribeiro
Resumo
A crescente digitalização das subestações e a interligação em larga escala de sistemas de potência têm elevado a importância da aplicação de requisitos de segurança cibernética em infraestruturas críticas. Nesse contexto, este trabalho apresenta uma contribuição técnica inédita por meio da realização de testes práticos em um modelo representativo do Sistema Especial de Proteção das interligações Norte-Nordeste-Sudeste do SIN, avaliando sua segurança frente a diferentes tipos de ataques cibernéticos. A rede do SEP, baseada em mensagens GOOSE (IEC 61850) em uma grande infraestrutura Ethernet, foi representada em uma plataforma de testes e submetida à simulação de ataques de personificação, replicação de mensagens, negação de serviço (DoS) e escaneamento de rede. A importância do estudo reside na avaliação prática do comportamento de IED durante condições adversas de ataques cibernéticos, considerando a aplicação de switches com diferentes granularidades de regras de comutação. Os resultados mostram que, mesmo com o uso de mensagens autenticadas, a ausência de filtragem adequada pode comprometer a integridade das lógicas de atuação do SEP. Por outro lado, a aplicação combinada de filtros por porta de entrada, endereço MAC de destino e tipo de protocolo, além de uma topologia adequada, mostrou-se eficaz na mitigação de ameaças. Esta prova de conceito valida os requisitos técnicos de segurança de rede do SEP e contribui para o aprimoramento de projetos similares, além de subsidiar políticas de comissionamento e monitoramento em subestações digitais, com foco em segurança desde a concepção.
Perguntas e Respostas

Tendo em vista que o SEP deve responder em menos de 150 ms, qual o impacto, mesmo mínimo, da aplicação de regras mais granulares nos switches SDN sobre a latência total da mensagem GOOSE? Houve alguma medição ou estimativa prática no ambiente de teste?

Quando há hit em hardware (TCAM) e regras pré-instaladas, o aumento da granularidade não adiciona latência mensurável além do atraso normal de comutação. No caso do SEP houve de fato a medição para validação do atraso, e os resultados foram muito melhores do que o esperado.
Nos testes integrados do SEP, comentados no IT GPC-662, realizou-se um teste para medição do tempo de latência considerando as maiores rotas envolvidas em uma atuação de lógica do SEP (comunicação entre as subestações Serra da Mesa (GO), Colinas (TO), Bacabeira(MA) e Xingu(PA) e o processamento dos respectivos IED). Neste teste, o resultado obtido para a rede do SEP foi inferior a 50 ms.

Considerando que os ataques de personificação foram parcialmente bem-sucedidos mesmo com o uso de mensagens GOOSE autenticadas, quais os

limites da eficácia da autenticação atual adotada? Há intenção de incorporar autenticação baseada em criptografia ou verificação de integridade no payload para mitigar esse tipo de vulnerabilidade?

A GOOSE (IEC 61850-8) por padrão não inclui autenticação/criptografia, portanto a pergunta não se aplica. A proteção criptográfica e a assinatura são tratadas na família IEC 62351 (notadamente a parte 6), porém a disponibilidade em IEDs comerciais e a interoperabilidade multivendedor ainda são limitadas.
Criptografia ponta a ponta em tráfego GOOSE/SV pode introduzir aumento de latência e impacto no determinismo. Dessa forma, precisa ser avaliada cuidadosamente.

Sobre integridade, os procedimentos de rede do ONS (2.11) já demandam verificações de integridade das mensagens. Tais verificações podem ser implementadas por monitores de rede sem alterar o comportamento dos IEDs, e são obrigatórias para subestações digitais atuais.

Salienta-se que, mesmo para que esses ataques tenham sucesso parcial, é necessário que o atacante tenha conhecimento do projeto para conseguir comprometer um switch e obedeça condições específicas, como a do fluxo correto de mensagens no SEP, e o atendimento a determinadas condições da mensagem que são checadas pelos equipamentos de proteção. Por questões de segurança, essas condições não foram tratadas no informe técnico.

Considerando que o SEP N-NE-SE envolve múltiplos agentes operando de forma autônoma, como poderia ser garantida, na prática, a coerência e a sincronização na aplicação das regras de filtragem nos switches SDN entre diferentes empresas, especialmente diante de atualizações ou mudanças operacionais?
As regras de filtragem não precisam de sincronização temporal entre os switches SDN dos agentes. O que é exigido dos agentes é coerência de política: como as regras são pró-ativas, elas não dependem de um protocolo de distribuição em tempo real, bastando que todos apliquem o mesmo padrão de configuração.
No SEP N-NE-SE, o Documento de Requisitos Mínimos de Redes, de observância obrigatória pelos agentes, definiu essa baseline, o que assegurou a padronização, mesmo em ambientes multi-organização, com sucesso.

Título - Cibersegurança para Hidrelétricas: Desafios e Soluções Atuais, Envolvendo Estudos de Caso
Entidade(s) - Voith Hydro Ltda.,Voith Hydro Ltda,Siemens Infraestrutura e Indústria LTDA
Autor(es) - Daniel Diniz Furriel,Samuel Tung,André Alves Cunha,Fernando Pimentel Anes,Vitor Eduardo Lace Maganha
Resumo
A crescente digitalização das usinas hidrelétricas (UHEs) tem ampliado significativamente a superfície de ataque dessas infraestruturas críticas, exigindo a adoção de estratégias robustas de cibersegurança. Este artigo apresenta os principais desafios enfrentados pelas UHEs nesse cenário, com foco na aplicação prática de normas internacionais como a IEC 62443 e nos requisitos do Operador

Nacional do Sistema Elétrico (ONS).

É apresentado um estudo de caso de uma UHE de grande porte no Brasil que implementou uma arquitetura segmentada de rede, baseada em zonas e condutos, conforme preconizado pela norma IEC 62443. A rede foi estruturada em cinco zonas distintas — processo, controle, DMZ industrial, corporativa e externa —, com aplicação de firewalls industriais e políticas de controle de tráfego entre domínios. A segmentação permitiu reduzir a superfície de ataque, aumentar a visibilidade dos fluxos de dados e atender integralmente às exigências regulatórias.

O caso demonstra como a segmentação lógica e física da rede, aliada ao conceito de segurança por design e à estratégia de defesa em profundidade, pode elevar substancialmente o nível de maturidade cibernética de instalações críticas. Conclui-se que arquiteturas bem planejadas, alinhadas às boas práticas internacionais, são fundamentais para garantir a resiliência operacional das UHEs frente às ameaças cibernéticas crescentes.

Perguntas e Respostas

Os autores afirmam que "investir em soluções seguras deixou de ser apenas uma boa prática, tornando-se uma necessidade estratégica." Considerando a complexidade dos sistemas legados em Usina e Subestações, quais estratégias específicas de mitigação vocês consideram mais importantes para mitigar riscos à segurança dos ativos sem comprometer a disponibilidade operacional?

As estratégias para mitigar os riscos de sistemas legados passam por estratégias de segurança por Design. É necessário isolar esse sistema legado, aplicando estratégias de hardening e controle de acesso entre outras, além de utilizar ferramentas como IDS, que realizam a detecção ativa de intrusões.

Como os autores analisam os principais desafios para implementar medidas eficazes de segurança cibernética em sistemas SCADA de Usinas e subestações? A dificuldade de gerir uma série de ferramentas de segurança, que requerem profissionais qualificados para lidar com essa complexidade, é também uma desafio a se considerar?

As dificuldades de implementar medidas eficazes para cibersegurança no ambiente das usinas hidrelétricas passam pela mudança de mentalidade gerada pela integração do mundo de TI com o mundo de OT. Hoje com a convergência dos dois mundos são necessários novos investimentos em cibersegurança no âmbito da automação tradicional que não existiam antes, além de profissionais qualificados para atuar nesse novo ambiente. Além disso, esse profissionais necessitarão cada vez mais se manter atualizados para acompanhar o ritmo da evolução da tecnologia destinada a proteger as usinas hidrelétricas de malfeitores.

O estudo enfatiza o conceito de segurança por design. Na visão dos autores, quais as maiores dificuldades da adoção desse conceito como prática pelos diversos entes que compõem o setor elétrico brasileiro?

Em nossa visão, os principais entraves para essa aplicação são a falta de conhecimento no tema, a crença de que as hidroelétricas encontram-se isoladas e não são alvos de ciber-ataques, o custo de modernização para incluir os conceitos envolvidos e a falta de incentivos para que os agentes façam este investimento.

Título - Sistema de Visão Computacional Tridimensional Baseado em IA para Prevenção de Acidentes em Manutenção de Redes de Transmissão e Distribuição de Energia
Entidade(s) - Kasco Pesquisa e Desenvolvimento,COMPANHIA PAULISTA DE FORÇA E LUZ,CPFL SERVIÇOS, EQUIPAMENTOS, INDUSTRIA E COMERCIA S/A
Autor(es) - FRANCISCO FAMBRINI,Diogo Gara Caetano,Roberto Fonseca Bertolla Junior,Lise R R Navarrete,Amanda Lopes Fernandes,Frederico Prestupa Neto
Resumo
Neste artigo, os autores apresentam o "Projeto Comportamento Seguro", desenvolvido pela Kasco P&D em parceria com CPFL e ANEEL. Este projeto visa prevenir acidentes causados por falhas humanas e pela ausência de Equipamentos de Proteção Individual (EPIs) adequados. Utilizando inteligência artificial (IA), ele assegura a execução precisa de manutenções corretivas e preventivas em sistemas de transmissão e distribuição de energia elétrica. O foco está no desenvolvimento de sistemas portáteis de monitoramento por imagens, empregando câmeras estereoscópicas e computadores embarcados. Esses dispositivos foram projetados para operar em diferentes cenários, como câmeras de campo em tripés, câmeras fixas montadas em tótens, paredes ou tetos, além de instalações em veículos e drones. Os testes ocorreram em parceria com a CPFL, com ótimos resultados.
Perguntas e Respostas

A limitação de detecção de 9 pessoas é devido ao algoritimo ou ao processamento de hardware?

A limitação de detecção de 9 pessoas é devido ao algoritimo ou ao processamento de hardware?

A limitação de detecção de 9 pessoas é devido ao algorítimo ou ao processamento de hardware?
A limitação de 9 pessoas é devida ao Algoritmo utilizado. Pode ser ampliado, mas haverá um pouco mais de demora na resposta, quanto maior for o numero de pessoas que se deseja detectar na mesma cena.

Com a integração de redes do tipo LSTM, quais atividades a mais pretende monitorar?
Inicialmente: 1- Sequencia de troca de elo-fusivel, 2-manuntenção corretiva em transformadores, 3-substituição de transformador e 4-Aplicação/troca de conector eletrico do tipo AMPact.

Existem outras aplicações previstas para o sistema dentro da empresa pra além de segurança do trabalho?
Sim. Além de monitorar as condições de segurança do trabalho, é previsto que todas as atividades filmadas sejam analisadas do ponto de vista de otimizar a eficiência dos serviços de reparos na rede de distribuição de energia elétrica, observar através dos filmes as condições de todos os elementos da rede (postes,

transformadores, chaves-faca, etc) e principalmente observa a necessidade ou não de se relaizar podas na árvores em torno da fiação.

Título - Ferramenta baseada em Inteligência Artificial para gestão da manutenção e operação de ativos de telecomunicações. Estudo de Caso de detecção de falhas no processo de Inspeção de Torres de Telecomunicações.
Entidade(s) - NETCON LTDA,Instituto Scinet,NETCON CONSULTORIAE ENGENHARIA LTDA
Autor(es) - EWERTON DE OLIVEIRA FIGUEIROA,Nadja Juliana da Silva Lima,Jose Arthur Domingues Patricio
Resumo
O presente artigo aborda o desafio de otimizar o processo de inspeção de torres de telecomunicações que atualmente realizado de forma manual nas empresas de utilities , envolvendo altos custos operacionais e riscos para os colaboradores. O objetivo principal deste trabalho é apresentar uma solução inovadora que utilize tecnologias emergentes, como drones, Gêmeo Digital e Inteligência Artificial (IA), para transformar esse processo. A proposta inclui o uso de drones para realizar inspeções automatizadas das torres, capturando imagens de alta resolução e metadados de interesse, com o intuito de criar um modelo digital preciso e atualizado de cada ativo. Esse modelo, conhecido como Gêmeo Digital, permitirá uma visualização detalhada e contínua da estrutura das torres, facilitando a detecção de problemas como falhas estruturais, desgaste de componentes, mau posicionamento de equipamentos e coletando dados de interesse regulatório. A IA será empregada para identificar anomalias nas imagens, prevendo necessidades de manutenção de forma preditiva e garantindo maior eficiência no gerenciamento de ativos. A solução também poderá ser integrada aos sistemas corporativos da empresa de utilitie , proporcionando uma gestão centralizada e fluida das infraestruturas de telecomunicação, com monitoramento em tempo real e relatórios automáticos. Com essa inovação, busca-se não apenas aumentar a segurança dos colaboradores, ao reduzir a necessidade de inspeções físicas, mas também reduzir os custos operacionais e otimizar o tempo de resposta a falhas. Em prova de conceito realizada com essa metodologia, conseguimos reduzir em aproximadamente 70% do tempo de pessoas envolvidas na atividade e 30% no custo. Além disso, é uma ferramenta que traz mais confiabilidade ao processo, pois tem dados mais precisos e maior segurança operacional à medida que diminui o risco da escalada na estrutura. A implementação dessa solução representa um avanço significativo na modernização das operações, alinhando-se às tendências globais de digitalização e automação.
Perguntas e Respostas

Esse sistema foi testado em alguma torre em especifico em campo?

Esse sistema foi testado em alguma torre em especifico em campo?
Sim. O sistema foi testado em torres de telecomunicações e recentemente em torres de linhas de transmissão de alta tensão. Os resultados obtidos foram relevantes e satisfatórios, ilustrando que a ferramenta pode se tornar importante ferramenta no ambiente de operação de concessionárias de energia.

Existe alguma proposta futura de sistema de armazenamento histórico para que possa ter um banco de dados de inspeção?
Sim. Todas a inspeções geram relatórios com datas e arquivos da inspeção que podem gerar uma base de dados para comparativos futuros.

Como vocês garantem a precisão dos modelos gerados por fotogrametria em ambientes com baixa luminosidade ou obstruções?
Até agora não nos deparamos com ambientes de baixa luminosidade para a realização dessas inspeções, mas esse problema pode ser resolvido com refletores. Quanto as obstruções pode-se aumentar a sobreposição das imagens: capturar de diferentes ângulos e posições, garantindo que cada ponto seja visto em múltiplas fotos. Além disso o planejamento de voo (em drones): rotas otimizadas para contornar obstáculos e coletar redundância de dados é essencial para garantir boa precisão. Por fim, o uso de alvos de controle terrestre para amarrar o modelo ao sistema de coordenadas e corrigir pequenas deformações é uma alternativa que também pode ser utilizada.

Título - Método DCT-Bootstrap para detecção de falhas em unidades geradoras
Entidade(s) - RADIX ENGENHARIA E DESENVOLVIMENTO DE SOFTWARE S/A
Autor(es) - Matheus Lira Sartor,KLEYTON PONTES COTTA,Arnaldo Mendes Pires Junior,HUGO DINIZ REBELO,Patrícia de Castro Wang,Mauricio Silva de Magalhães,Hugo Reiser Vieira Portuita,Leonardo Tavares Vianna,Tassio Simioni
Resumo
É essencial que se detectem as falhas das turbinas em usinas hidrelétricas, com vista a garantir a continuidade da produção de eletricidade e a reduzir os custos de uma reparação inesperada. O principal desafio reside em identificar as falhas reais sem serem enredados pelas variações nos dados normais do desempenho dos aparelhos, constituindo uma situação de “falsos positivos”. Nesse sentido, é necessário avaliar falsos positivos, sem sacrificar a precisão no cálculo das falhas. A solução da DCT-Bootstrap provou ter um melhor desempenho em comparação com os métodos tradicionais na inspeção de trabalhos científicos com dados reais em usinas hidrelétricas, assim como nas bases de dados de referência de poços de perfuração de petróleo. Uma abordagem eficaz e inovadora na previsão das avarias de máquinas, o que traduz maior segurança e fiabilidade na sua operação.
Perguntas e Respostas

Como o modelo DCT-Bootstrap lida com mudanças operacionais nas usinas, como variações de carga e ruídos?
Ao avaliar os dados através dos componentes da transformada de cosseno, o ruído pode ser filtrado, para fins experimentais, foram consideradas unidades geradoras em pleno funcionamento.

Há alguma estratégia para adaptar o intervalo de confiança sem re-treinar o modelo?
Ao saber os intervalos e o alpha atuais, é possível recalibrar o modelo para diferentes alphas ou ajustar manualmente os thresholds

Qual foi o critério para a escolha desse modelo?

Uma melhor representação de balanço entre sensibilidade e especificidade para o sistema em operação.

Título - Estruturação de Telecom e SPCS para atendimento do projeto SEP N-NE-SE
Entidade(s) - Argo Energia,ARGO TRANSMISSAO DE ENERGIA SA
Autor(es) - Celso Moreira de Lima Junior,Alexandre Gerber Choupina Latorre,ALAN HENRIQUE RIBEIRO DOS SANTOS
Resumo
Foram previstos até o ano de 2024 reforços significativos no sistema de transmissão em corrente alternada das interligações Norte – Nordeste – Sudeste. Estes reforços foram destinados a viabilizar o escoamento da geração da energia das regiões Norte e Nordeste. Por conta destes reforços, tornou-se necessário uma reavaliação do Sistema Especial de Proteção original implantado na Interligação N-SE. O novo SEP tem como objetivo monitorar linhas de transmissão da interligação N-SE e tomar ações de run-up ou run-back nos bipolos de corrente contínua associados à SE Xingu e/ou realizar corte de unidades geradoras nas UHE Tucuruí, Serra da Mesa, Estreito, Lajeado e Peixe Angical. A ARGO implantou com sucesso o sistema de WAN (Telecom) necessário para funcionamento do projeto SEP N-NE-SE, atendendo aos requisitos técnicos do projeto e entregando as informações dentro do túnel MPLS-TP de uma extremidade até a outra com latência máxima de 0,013ms. Além da infraestrutura de telecomunicações, o projeto contemplou a implementação de um sistema de monitoramento em nível de rede local (LAN), destinado a garantir a aquisição e a integração de sinais críticos para o funcionamento do SEP. Todas as integrações necessárias de telecom e SPCS foram realizadas com êxito nas subestações de Bacabeira, Tianguá II, Parnaíba III e Acaraú III, garantindo um alto nível de confiabilidade na supervisão e no controle das interligações elétricas.
Este trabalho descreve as ações que foram executadas pela ARGO Energia em 2023 e 2024 para atender as recomendações técnicas de telecom denominado como “escopo de WAN” e ações de SPCS denominado como “escopo de LAN”.
Perguntas e Respostas

De que forma o monitoramento via Zabbix e SAGE contribuiu para a confiabilidade do SEP?
O monitoramento via Zabbix (SNMP) permitiu que todos os agentes acompanhassem em tempo real os ativos de telecomunicação e proteção envolvidos no SEP, além do monitoramento centralizado realizado pela Taesa na subestação de Colinas. Assim, cada agente passou a ter visibilidade direta sobre a operação de sua respectiva infraestrutura, fortalecendo a supervisão distribuída.

Já o monitoramento via SAGE possibilitou a análise detalhada de parâmetros específicos dos IEDs, como a qualidade das mensagens GOOSE nas rotas A (principal) e B (alternada), viabilizando a supervisão em tempo real pelos Centros de Operação (COS) e pelo ONS.

Foi desenvolvida uma tela dedicada ao SEP, permitindo a visualização consolidada de alarmes, dados críticos e eventos, o que garantiu detecção ágil de anomalias e, consequentemente, maior confiabilidade operacional.

Como foi validado o tempo de salto no cenário 1?
No Cenário 1, o objetivo foi avaliar o tempo de envio de pacotes exclusivamente na infraestrutura de transporte MPLS-TP, sem envolver a camada LAN (Switches SDN, IEDs e Master).

O ensaio foi conduzido no laboratório da PADTEC (Campinas), simulando o maior enlace do projeto através de bobinas ópticas, atenuadores em bancada e sistemas de amplificação óptica. A medição entre Multiplexador 1 e Multiplexador 2 resultou em um tempo médio aproximado de 2,2 ns, atendendo plenamente aos requisitos de latência estabelecidos para o projeto.

E para o cenário 2 esse teste foi feito com qual metodologia e qual margem de confiabilidade? O teste foi repetido quantas vezes?
No Cenário 2, diferentemente do Cenário 1, foi avaliada a infraestrutura completa, incluindo o transporte via túnel MPLS-TP e a camada LAN do projeto (Switches SDN, IEDs e Master).

A metodologia foi a mesma utilizada no laboratório da PADTEC: bobinas ópticas para simulação da distância do maior enlace, atenuadores em bancada, sistemas de amplificação óptica e inclusão dos elementos LAN no circuito de testes. O resultado obtido foi um tempo médio de 26 ms, valor significativamente inferior ao limite máximo estabelecido pelo ONS (63 ms).

Esse desempenho confirmou a conformidade do sistema dentro da margem de confiabilidade definida. O teste foi repetido continuamente durante uma hora, assegurando consistência estatística nos resultados.

Título - Orquestrador multimodelos para manutenção preditiva em usinas hidrelétricas.
Entidade(s) - RADIX ENGENHARIA E DESENVOLVIMENTO DE SOFTWARE S/A
Autor(es) - Leonardo Tavares Vianna,HUGO DINIZ REBELO,Patrícia de Castro Wang,Mauricio Silva de Magalhães,Arnaldo Mendes Pires Junior,KLEYTON PONTES COTTA,Hugo Reiser Vieira Portuita,Tassio Simioni
Resumo
A gestão de ativos em usinas hidrelétricas impõe desafios relevantes, exigindo estratégias que garantam a confiabilidade e disponibilidade das unidades geradoras (UGs), além de prolongar a vida útil dos equipamentos. Falhas nesses ativos impactam diretamente a geração de energia e a estabilidade do sistema elétrico, tornando essencial a adoção de tecnologias que aumentem a eficiência operacional e reduzam manutenções corretivas.
Ferramentas de Asset Performance Management (APM) têm ganhado destaque por viabilizarem uma abordagem preditiva na manutenção. No entanto, o rápido avanço tecnológico pode gerar a obsolescência de modelos e algoritmos de inteligência artificial, além de ampliar a variedade de soluções e arquiteturas disponíveis, o que dificulta a escolha das tecnologias mais adequadas, principalmente para empresas que não têm a tecnologia como atividade-fim.
Diante desse cenário, este trabalho propôs o desenvolvimento de uma ferramenta, intitulada APM 4.0, que combina inteligência artificial com o conceito de orquestração de modelos. Essa abordagem permite coordenar diversos algoritmos e

selecionar automaticamente o de melhor desempenho.
A ferramenta foi testada em condições reais nas usinas hidrelétricas de Campos Novos e Barra Grande, verificando a sua aplicabilidade. O foco da aplicação foi no monitoramento da saúde dos ativos, detecção de falhas e identificação de desvios operacionais, buscando uma solução flexível e alinhada às demandas de um setor cada vez mais orientado por dados.

Perguntas e Respostas

Existe alguma forma do APM 4.0 se integrar a outros sistemas SCADAs?
Sim. O APM 4.0 foi projetado para ser integrado ao sistema supervisório das usinas, operando na rede operacional. Dessa forma, ele consegue adquirir em tempo real as variáveis monitoradas nas UGs, garantindo compatibilidade com os ambientes cibernéticos regulados pelo ONS. É possível realizar a integração com diferentes sistemas SCADA, mas deve-se avaliar o SCADA em questão e a arquitetura tecnológica da empresa/ativo, sendo necessário analisar cada caso individualmente para garantir a viabilidade e a segurança da integração.

Qual foi o critério usado para escolher os algoritmos de machine learning em cada modelo?
O critério foi a adequação ao tipo de problema, aliado às métricas de avaliação específicas de cada abordagem. Nos modelos de desvio operacional, foram aplicadas técnicas adequadas a séries temporais (ex.: RNN, ARIMAX), avaliadas principalmente pelo RMSE (Root Mean Square Error). Para o índice de saúde (Digital Twin), utilizaram-se algoritmos de regressão, validados também por métricas de erro como o RMSE, para medir a proximidade entre os valores previstos e os reais. Na carta de performance da turbina, foram testados algoritmos de regressão e classificação (Random Forest, Gradient Boosting, LSTM, XGBoost), escolhendo-se os melhores de acordo com métricas de eficiência e de classificação. Já nos modelos de detecção de falhas, seis algoritmos distintos (SVM, LOF, RPCA, MWRPCA, LSTM-VAE e DCT-Bootstrap) foram comparados utilizando F1 Score Macro e Weighted, métricas adequadas para cenários com classes desbalanceadas. O orquestrador multimodelo então selecionava automaticamente o modelo mais eficaz para cada situação.

Qual foi o principal benefício observado nas usinas após a aplicação do APM 4.0?
O APM 4.0 está em operação há aproximadamente um ano e meio, sendo acompanhado pelas equipes de manutenção das usinas. O principal benefício percebido é a maior confiabilidade na tomada de decisão, apoiada pela disponibilização de mais informações relevantes sobre os ativos. Esse ganho qualitativo tem refletido positivamente nos indicadores de manutenção e operação, como redução de paradas não programadas e melhor planejamento das intervenções.

Título - Desafio da manutenção da disponibilidade do sistema de telecomunicações durante a crise Enchentes RS
Entidade(s) - COMPANHIA ESTADUAL DE TRANSMISSÃO DE ENERGIA ELÉTRICA
Autor(es) - Igor Freitas Fagundes,André Luis Silveira Fraga,Felipe Tatsch

Resumo
Durante o desastre das enchentes no Rio Grande do Sul a resiliência e robustez do sistema de telecomunicações da CPFL Transmissão foi colocada a prova, com múltiplas interrupções de rotas ópticas e canais de comunicação, subestações operando com contingência de serviços auxiliares e em alguns casos com salas de comando parcialmente submersas. As infraestruturas de operadoras de telecomunicações no estado também tiveram restrições severas, afetadas pela indisponibilidade de energia elétrica em áreas alagadas e rompimentos de fibras ópticas instaladas em pontes nas travessias dos principais rios. Em um cenário de mobilidade restrita, a manutenção da disponibilidade dos sistemas de telecomunicações era determinante para garantir a operação com segurança do sistema elétrico.

A operação e manutenção do sistema de telecomunicações da CPFL Transmissão é realizada por equipes próprias, o que permitiu a rápida definição das estratégias e acionamento dos planos de contingência. No período mais crítico, das cinco principais rotas de comunicação que interligam o interior do estado ao centro de operação, três apresentavam restrições operativas de forma simultânea. As ações iniciais de contingência foram realizadas de forma remota, com a parametrização e ativação lógica de rotas de comunicação interligando os sistemas sul e noroeste, viabilizando o reestabelecimento de rotas alternativas para regiões que operavam em condição de falha dupla. A existência de interligações físicas nas subestações e a disponibilidade de infraestrutura das empresas parceiras acelerou a implementação das contingências, reduzindo as atividades em campo necessárias para implementar as soluções. O sistema da região da serra foi o menos impactado, também sendo utilizado como ponto de interligação entre os subsistemas.

Com a rápida evolução dos níveis das águas na região metropolitana de Porto Alegre, foi colocado em ação o plano de contingência para deslocamento parcial dos servidores SAGE de Canoas para Gravataí. A arquitetura de comunicação dos servidores SAGE instalados em ambiente de rede operativa (TO) em configuração hot-stantby (1+1) permitiu agilidade na transferência, com as atividades de desativação e ativação, incluindo as adequações de infraestrutura realizadas em 12 horas. A utilização de protocolo de comunicação IEC104 combinada aos protocolos de roteamento dinâmico da rede de transporte adicionaram segurança para a execução da migração. O trabalho apresenta uma linha do tempo com as principais estratégias e ações adotadas para garantir a teleassistência das subestações.

Perguntas e Respostas

Quais aprendizados vocês consideram mais valiosos após essa experiência, e o que acreditam que poderia ter sido feito de forma diferente para mitigar os impactos?

Entre os principais aprendizados destaco.

- Comunicação eficaz, a troca clara e constante de informações entre equipes técnicas, gestão e operação foi determinante para reduzir incertezas e acelerar decisões.
- Importância de planos de contingência, a experiência reforçou a necessidade de revisar e testar periodicamente os planos de contingência.

Poderíamos fazer de forma diferente simulações mais frequentes de cenários críticos.

Quais foram os principais critérios considerados para decidir a realocação dos servidores SAGE?

Entre os principais critérios destaco:
- A rápida elevação dos níveis das águas nos dois centros e as condições favoráveis de acesso na subestação de Gravataí.
- A infraestrutura de telecomunicações disponível na subestação.
- A arquitetura de hardware redundante implementada no sistema SAGE.

Houve alguma lição aprendida que pode ser incorporada ao planejamento futuro de desastres?
Reforço da importância capacitação das equipes em gestão de crises, com treinamentos regulares para melhorar a tomada de decisão sob pressão.
Simulações mais frequentes de cenários críticos, contudo não com as proporções do evento vivenciado.

4.0 – Constatações