Proteção, Medição, Controle e Automação em Sistemas de Potência

19 a 22 de outubro de 2025

RELATÓRIO ESPECIAL PRÉVIO

Pablo Humeres Flores
Pablo Humeres Flores,Denise Borges de Oliveira,Julio Cesar Marques de Lima

1.0 CONSIDERAÇÕES GERAIS

Para a 28ª edição do SNPTEE foram estabelecidos pelo Comitê Técnico 11 Temas Preferenciais para os trabalhos aprovados para apresentação na sala GPC (Grupo de Proteção, Controle Local, Medição e Automação). 04 Temas Preferenciais não tiveram ITs aprovados. Efetivamente os 37 ITs apresentados nessa edição foram classificados em 07 temas preferenciais, conforme abaixo:

TEMA PREFERENCIAL	No. DE ITS
Tema 1 - Sistemas locais de proteção, automação, controle e medição, incluindo elos CC a dois e multi-terminais:	06
Tema 2 - Proteção Sistêmica	02

Tema 3 - Esquemas especiais de proteção

03

Tema 4 – Aplicações da Norma IEC 618560

16

Tema 5 – Sistemas de Medição Sincrofasorial

01

Tema 6 – Perturbações no Sistema Elétrico

03

Tema 8 - Fontes de energia Distribuída – Impactos na Automação e Proteção

02

Tema 11 – Desafios no Treinamento e Capacitação

03

TOTAL DE ITs SALA GPC

36

Analisando os ITs apresentados x Temas Preferencias vale destacar:

O Tema Preferencial 4 referente aos aspectos de implantação da Norma IEC 61850 seguem representando um grande percentual dos trabalhos aprovados refletindo o estágio atual do desenvolvimento dessa tecnologia nas empresas do setor elétrico, principalmente devido aos projetos de implantação da automação do barramento de processo e os recentes requisitos aprovados para os Procedimentos de Rede do ONS referentes ao monitoramento da rede de proteção e automação nas subestações digitais;

Tem crescido o número de ITs aprovados para o Tema Preferencial 8 referente aos impactos nos sistemas de proteção e automação referentes às fontes de geração distribuída, de modo especial o impacto das fontes de geração baseadas em IBRs;

Nota-se uma redução preocupante no número de ITs propostos para o Tema Preferencial 6 - Perturbações no Sistema Elétrico, que pode estar ligada à redução da execução sistemática dessa atividade nas empresas do setor elétrico.

Apesar dos esforços da coordenação do CE B5, ainda não apresentaram resultados as ações para inserir no evento ITs referentes aos temas de proteção e automação da Distribuição – MT (Tema Preferencial 7). Nenhum IT foi aprovado para esse tema nesta edição do SNPTEE.

2.0 - Classificação dos Informes Técnicos

Para a 28ª edição do SNPTEE foram estabelecidos pelo Comitê Técnico 11 Temas Preferenciais para os trabalhos aprovados para apresentação na sala GPC (Grupo de Proteção, Controle Local, Medição e Automação). 04 Temas Preferenciais não tiveram ITs aprovados. Efetivamente os 37 ITs apresentados nessa edição foram classificados em 07 temas preferenciais, conforme abaixo:

TEMA PREFERENCIAL

No. DE ITS

Tema 1 - Sistemas locais de proteção, automação, controle e medição, incluindo elos CC a dois e multi-terminais:

06

Tema 2 - Proteção Sistêmica

02

Tema 3 - Esquemas especiais de proteção

03

Tema 4 – Aplicações da Norma IEC 618560

16

Tema 5 – Sistemas de Medição Sincrofasorial

01

Tema 6 – Perturbações no Sistema Elétrico

03

Tema 8 - Fontes de energia Distribuída – Impactos na Automação e Proteção

02

Tema 11 – Desafios no Treinamento e Capacitação

03

TOTAL DE ITs SALA GPC

36

Analisando os ITs apresentados x Temas Preferencias vale destacar:

O Tema Preferencial 4 referente aos aspectos de implantação da Norma IEC 61850 seguem representando um grande percentual dos trabalhos aprovados refletindo o estágio atual do desenvolvimento dessa tecnologia nas empresas do setor elétrico, principalmente devido aos projetos de implantação da automação do barramento de processo e os recentes requisitos aprovados para os Procedimentos de Rede do ONS referentes ao monitoramento da rede de proteção e automação nas subestações digitais;

Tem crescido o número de ITs aprovados para o Tema Preferencial 8 referente aos impactos nos sistemas de proteção e automação referentes às fontes de geração distribuída, de modo especial o impacto das fontes de geração baseadas em IBRs;

Nota-se uma redução preocupante no número de ITs propostos para o Tema Preferencial 6 - Perturbações no Sistema Elétrico, que pode estar ligada à redução da execução sistemática dessa atividade nas empresas do setor elétrico.

Apesar dos esforços da coordenação do CE B5, ainda não apresentaram resultados as ações para inserir no evento ITs referentes aos temas de proteção e automação da Distribuição – MT (Tema Preferencial 7). Nenhum IT foi aprovado para esse tema nesta edição do SNPTEE.

2.1 - Sistemas locais de proteção, automação, controle e medição, incluindo elos CC a dois e multiterminais - 6
2.2 - Proteção sistêmica - 2
2.3 - Esquemas especiais de proteção - 3
2.4 - Aplicações da norma IEC 61850 - 15
2.5 - Sistemas de Medição Sincrofasorial - 1
2.6 - Perturbações no sistema elétrico - 3
2.7 - Fontes de energia distribuída (geração eólica, geração solar, sistemas de armazenamento de energia, etc) e seus impactos na automação e proteção: - 2

2.8 - Desafios no treinamento e capacitação dos profissionais e gestores da área de proteção, controle medição e automação - 3
2.9 - Resumo Transferido - 1

- Digital Twin : A Revolução na Manutenção da Proteção do Sistema Elétrico

- Projeto Athena: Laboratório de Automação de Subestações para o Grid 4.0 na escola SENAI
- Modernização de Currículo de Engenharia Elétrica – Estudo de Caso da Universidade Federal Fluminense
- Método de Desenvolvimento e Métricas de Avaliação de treinamentos para profissionais e estudantes das áreas de proteção, controle e automação com enfoque em Subestações Digitais com implementação de barramento de processo

- Os Impactos de Inversores Grid-Forming em Proteções de Linhas de Interconexão de Fontes Renováveis
- Análise de Desempenho da Proteção de Distância com Supervisão Weak-Infeed para Linhas de Interconexão de Fontes Interfaceadas por Inversores

- Impacto da penetração de fontes de energias renováveis com inversores no SIN
- Avaliação de Algoritmo de Seleção de Fases Baseado em Componentes Pseudo-Incrementais Frente a Cenários Complexos de Falta em Sistemas de Transmissão Reais
- Experiência da CEMIG GT na Análise de Perturbações utilizando o SIPROTEC DigitalTwin

- Experiência prática de implementação de PMU com utilização do protocolo PTP para sincronização de tempo.

- Ensaios em Virtual Protection, Automation and Control Systems (vPACS)
- Análise de desempenho da primeira subestação digital do Grupo CPFL
- Recomendações para a Implementação do Barramento de Processos em Subestações Digitais à Luz do WG B5.69
- Proteção Diferencial de Linhas com IEDs Virtuais em Subestações IEC 61850: Implementação e Avaliação
- Ferramenta Automática para Modelagem de Hardware de IEDs e MUs dentro de uma Plataforma de Engenharia
- Confiabilidade em subestações digitais com monitoramento eficaz de redes IEC 61850
- Análise Comparativa entre Transformadores para Instrumentos Ópticos e Convencionais em Subestações Digitais: Desafios e Perspectivas
- Monitoramento de Barramento de Processo em Subestações Digitais: Plano de Inspeção e Testes com Múltiplos Fabricantes
- Implementação e Validação de Monitoramento de Rede para Barramento de Processo na Subestação Cerro Chato: Desafios da implementação em Anel HSR
- Diretrizes para Interpretação e Uso de Informações de Monitoramento em Subestações Digitais: Análise Eficiente do Barramento de Processos
- Desempenho da Proteção Diferencial de Linha em Subestações Digitais: Análise do Impacto do Barramento de Processo e Sincronismo de Tempo
- Monitoramento da Integridade das Mensagens no Barramento de Processo: Um Estudo de Caso em uma Rede Multi-Fabricante

- Aplicação de Processo de Engenharia Top-Down em Sistemas de Proteção, Controle e Supervisão de Subestações Digitais
- Monitoramento de sistemas de automação na norma IEC 61850: Riscos, oportunidades e recomendações
- Avaliação de Desempenho de Teleproteção via R-GOOSE sobre MPLS-TP: Estudo de Caso e Resultados

- ENSAIOS, SIMULAÇÕES E MODELAGEM DO SISTEMA DE POTÊNCIA NO SIMULADOR EM TEMPO REAL (RTDS) PARA MODERNIZAÇÃO DAS PROTEÇÕES DE LINHAS, BARRAS, GERADORES E TRANSFORMADORES DA USINA DE ITAIPU
- Implantação e testes do maior Sistema Especial de Proteção do SIN: SEP das Interligações Norte-Nordeste-Sudeste
- Virtualização e Centralização da Proteção e Controle: Transição do Gerenciamento de Dispositivos para a Gestão de Aplicações

- SIPS – um recurso para minimizar/controlar as consequências de perturbações de grande porte
- AVALIAÇÃO DAS FUNÇÕES DE OSCILAÇÃO DE POTÊNCIA DO SISTEMA ACRE-RONDÔNIA ATRAVÉS DE TESTE NO SIMULADOR DIGITAL EM TEMPO REAL EM MALHA FECHADA COM OS IED DE PROTEÇÃO

- BENCHMARK DE CASOS COMTRADE PARA ANÁLISE DO DESEMPENHO DE PROTEÇÕES DE GERADORES SÍNCRONOS DURANTE GRANDES PERTURBAÇÕES
- Estimativa de frequência elétrica instantânea de simulações e registros de perturbações envolvendo a usina hidrelétrica de Itaipu empregando geometria diferencial
- Resultados Prático na Proteção de Reatores de Núcleo de ar para Faltas entre Espiras por Elemento de Impedância
- Desempeño de relés distancia en redes con presencia de dispositivos M-SSSC
- Testes de injeção de secundário em Merging Unit considerando o uso da tecnologia Low Power instrument Transformers
- Análise comparativa entre proteção de barras digital convencional e por barramento de processos

3.0 - Relatório sobre os Informes Técnicos

Título - BENCHMARK DE CASOS COMTRADE PARA ANÁLISE DO DESEMPENHO DE PROTEÇÕES DE GERADORES SÍNCRONOS DURANTE GRANDES PERTURBAÇÕES
Entidade(s) - ITAIPU BINACIONAL,GENERAL ELECTRIC DO BRASIL LTDA,RIO PARANÁ ENERGIA S.A.,ENGIE BRASIL ENERGIA S.A
Autor(es) - Jonas Pesente,Rafael Cesar Jabor Fagundes Nogueira,Lucas Fernando Vitti,Felipe Eduardo Stein Cardoso
Resumo
Este informe relata o desenvolvimento de um conjunto de registros oscilográficos de referência (benchmark) para realização de ensaios de proteções de geradores

síncronos em bancada, elaborados pelo grupo de trabalho de levantamento das melhores práticas de ensaios de proteção de geradores síncronos do CIGRE-BR (B5/GT-04). O intuito deste conjunto de registros é complementar os ensaios funcionais existentes com testes que permitam identificar e antever atuações indesejadas durante eventos no sistema elétrico ou que atualmente não estão cobertos pelas funções existentes. O risco de tais atuações indesejadas é embasada no histórico existente na bibliografia, ocorridas especialmente como resposta da proteção dos geradores à grandes blecautes. As oscilografias foram criadas considerando uma representação realista de sistemas elétricos hidrotérmicos-renováveis, incorporando as variações de frequência e tensão decorrentes das perturbações simuladas. No artigo são descritos os casos de maior relevância e apresentadas diretrizes para aplicação. O banco completo pode ser descarregado no link ao lado.

Perguntas e Respostas

1- Este banco de dados já está disponível para uso ?

2 - Estas oscilografias podem ser utilizadas para uma avaliação preliminar , mas , por exemplo, no caso de avaliação de proteções em condições sistÊmicas adversas , os autores recomendam testes mais específicos , como por exemplo, em RTDS?

Recomendamos. O banco de oscilografias permite realizar uma avaliação do comportamento da proteção em condições não típicas dos ensaios convencionais, ampliando, portanto, as avaliações usualmente realizadas. Isto é verdade também para proteções sistêmicas, porém nestes caso, a simulação em malha fechada permite incorporar outros fenômenos, proteções e esquemas do sistema que possam ter interação com a proteção reagindo à sua atuação, sendo portanto, um ensaio mais completo que a injeção de arquivos COMTRADE.

3- Na base de dados estarão detalhadas as funções que são esperadas atuar para cada evento?

A modelagem adotada esta dentro de uma prática internacional ou alguma referência de norma internacional, ou é uma abordagem inedita?

A abordagem, incluindo a modelagem, é inédita, no melhor do nosso conhecimento, considerando sua abrangência, extensão dos modelos e número de oscilografias. Não obstante, nossa proposta está em consonância com normas existentes, como a IEEE Std C37.233™-2009 (IEEE Guide for Power System Protection Testing) e IEEE Std C37.102™-1995 (IEEE Guide for AC Generator Protection).

1 - Os autores comentam a recomendação do IEEE quanto à adoção de ajustes para a proteção ANSI 40 para identificação de fechamento do disjuntor fora de sincornismo. É possível alterar os tradicionais ajustes dessa função de proteção para atender a essa condição sem perda de seletividade para a perda de excitação?

Não. Embora mencionado na bibliografia especializada, nossas simulações mostraram que a trajetória de impedância aparente terminal no caso de fechamento fora de sincronismo se dá prioritariamente no semiplano RX correspondente à

reatância positiva, onde não é permitido ajuste da função 40. Embora tenha ocorrido trânsito no semiplano negativo imaginário da impedância, este foi excessivamente rápido (da ordem de 4ms no caso mais lento), podendo expor à unidade à desligamentos desnecessários ajustar a função 40 com uma zona instantânea.

1 - Os autores comentam a recomendação do IEEE quanto à adoção de ajustes para a proteção ANSI 40 para identificação de fechamento do disjuntor fora de sincornismo. É possível alterar os tradicionais ajustes dessa função de proteção para atender a essa condição sem perda de seletividade para a perda de excitação?

Título - Estimativa de frequência elétrica instantânea de simulações e registros de perturbações envolvendo a usina hidrelétrica de Itaipu empregando geometria diferencial
Entidade(s) - ITAIPU BINACIONAL, Universidade Tecnológica Federal do Paraná (UTFPR) Campus Medianeira
Autor(es) - Jonas Pesente,Diogo Marujo
Resumo
Este trabalho trata de um estudo de aplicação de geometria diferencial no cômputo da frequência elétrica de sistemas de potência. Neste arcabouço, as grandezas elétricas são descritas como grandezas espaciais sobre o referencial de Frenet, o que fornece aparato conceitual sobre as limitações dos métodos existentes. Em decorrência da simplicidade da sua aplicação, a geometria diferencial apresenta desempenho numérico-computacional muito superior aos métodos tradicionalmente empregados, sendo, portanto, interessante a aplicações embarcadas, com aquelas de proteções de sistemas elétricos. Neste trabalho são descritos os fundamentos matemáticos do método e os resultados obtidos de um conjunto de experimentos computacionais empregando simulações realistas e registros de perturbações reais, mostrando sua viabilidade e a qualidade das soluções.
Perguntas e Respostas

1- Os autores chegaram a aplicar os dados obtidos por este método em modelos de IEDs para verificar seu desempenho?
Implementamos o método de estimação de frequência elétrica por geometria diferencial em ATP e aplicamos no controle de oscilações eletromecânicas, já que a medida de frequência é modo de falha na ação do PSS. Estamos em processo de aplicá-la também aos modelos de proteção em EMT da nossa biblioteca.

2- Com relação À sensibilidade a ruídos e distorções nos sinais medidos, o metodo fica muito dependente da filtragem . Os autores já tem resultados relacionados a estes filtros a serem aplicados?.
Temos. Fizemos uma ampla análise do impacto de ruídos e harmônicos ao método de estimação da frequência elétrica pela geometria diferencial. Foram testados os filtros típicos de aplicação industrial, dentre eles o Filtro de Kalman, o Filtro de Savitzky-Golay, o Filtro Gaussiano, e o Filtro de Butterworth. Os resultados obtidos demonstram que o emprego dos filtros é suficiente para garantir ao método uma precisão superior à 1% para uma banda de filtragem também típica.

A modelagem adotada esta dentro de uma prática internacional ou alguma referência de norma internacional, ou é uma abordagem inedita?

Qual seria uma evolução da modelagem proposta para sua aplicação em IEDs?

O esquema de proteção prtoposto prevê uma unidade de ajuste (Zona 1) que deve ter seu pick-up ajustado acima do pior caso de saturação do TC, do inrush do reator e do desequilíbrio do reator. É possível encontrar essa solução ótima através do estudo em escritório ou somente após testes de campo?

Considerando as limitações do método informadas nas conclusões do trabalho, como os autores vislumbram a possibilidade de aplicação do mesmo em equipamntos comerciais de proteção?
Vislumbramos. Estamos fazendo experimentos de aplicação no software de análise de perturbações do Parque Tecnológico Itaipu, com apoio da equipe do parque, e em seguida devemos fazer também experimentos no registrador de perturbações desenvolvido e distribuído pelo parque tecnológico.

Considerando as limitações do método informadas nas conclusões do trabalho, como os autores vislumbram a possibilidade de aplicação do mesmo em equipamntos comerciais de proteção?

Considerando as limitações do método informadas nas conclusões do trabalho, como os autores vislumbram a possibilidade de aplicação do mesmo em equipamntos comerciais de proteção?

Título - Resultados Prático na Proteção de Reatores de Núcleo de ar para Faltas entre Espiras por Elemento de Impedância
Entidade(s) -
Autor(es) - Camila da Silva Oliveira
Resumo
Até poucos anos atrás, reatores de núcleo a ar eram mais usados em níveis de média tensão, de 34,5kV. Atualmente, com o avanço de algumas tecnologias, estes reatores passaram a ser comercializados também em níveis de alta e extra alta tensão. O desafio deste cenário vem sendo adequar a proteção destes equipamentos, mais especificadamente a proteção para faltas entre espiras. No reator de núcleo de ferro com enrolamento imerso em óleo a detecção deste tipo de falha era feita através do relé de pressão súbita. Este tipo de detecção não é mais possível no reator de núcleo de ar. Outro ponto importante é que as faltas entre espiras são o tipo de falta mais provável de acontecer no reator de núcleo a ar devido as suas características construtivas, que mantém um bom isolamento entre as fases e da fase para o terra.
O artigo propõe uma proteção de reator de núcleo a ar aterrado, tipo que vem

sendo aplicado no Sistema Interligado Nacional (SIN), com base em impedância, capaz de indicar se a falta está no reator ou no sistema. O princípio básico de funcionamento se baseia na análise do diagrama de impedâncias de sequência zero para uma falta entre espiras.

O artigo apresentará um caso de simulação do algoritmo proposto e um caso real. O trabalho conclui que o uso deste elemento de impedância para definir a direcionalidade da falta opera de maneira eficiente e sensível para faltas entre espiras em reatores de núcleo a ar, independentemente do ponto do sistema que o reator esteja conectado.

Perguntas e Respostas

1- Quais os requisitos para aplicação com sucesso desta solução?

Práticas da aplicação desta função tem nos mostrado a necessidade de atenção de alguns pontos:

1) Garantir que o RTC escolhido tenha sensibilidade para as faltas em questão garantindo um processo mínimo de saturação.

2) Garantir que se conheça o desbalanço máximo entre fases do reator para podermos ajustar devidamente o sobrecorrente de alta sensibilidade.

3) Garantir a atuação correta do elemento de impedância para faltas externas que gerem uma queda de tensão considerável a ser medida pelo relé (isenção da grandeza de polarização).

2- A aplicação e ajuste desta função requer estudos mais detalhados para verificação de desempenho . O que a autora recomenda como estudos a serem efetuados para sua correta aplicação?

A aplicação de funções de impedância é bastante confiável para detecção de faltas internas, porém, temos a questão da possível perda da tensão de polarização para algumas situações. Por isso devem ser testadas condições de queda de tensão de polarização e a efetiva atuação ou bloqueio da função. O esquema proposto de impedâncias é imune a estes momentos de queda de tensão de polarização.

Quais os principais desafios esperados na aplicação da proposta apresentada em sistemas em operação

O esquema de proteção proposto prevê uma unidade de ajuste (Zona 1) que deve ter seu pick-up ajustado acima do pior caso de saturação do TC, do inrush do reator e do desequilíbrio do reator. É possível encontrar essa solução ótima através do estudo em escritório ou somente após testes de campo?

Na verdade quando usamos a grandeza de operação como a corrente de neutro estamos imunes a situações de inrush, deixando pelo menos este problema de lado. O desequilíbrio máximo do reator é conhecido e pode ser também vencido. A grande questão que depende de um estudo maior é a saturação dos TCs, onde um estudo prévio já é suficiente através do cálculo do Kinrush proposto no artigo.

Título - Desempeño de relés distancia en redes con presencia de dispositivos M-SSSC

Entidade(s) - Smart Wires Inc.,Smart Wires Inc

Autor(es) - David Urbaez León,Dilan Caro Barranco,Carlos Eduardo Borda Zapata
Resumo
La transición energética hacia fuentes renovables requiere una mayor flexibilidad en las redes de transmisión para gestionar la variabilidad inherente a estas fuentes de generación. Los Compensadores Síncronos Estáticos Serie Modulares (M-SSSC), como parte de las tecnologías FACTS, representan una alternativa eficiente a la construcción de nuevas líneas de transmisión, ofreciendo ventajas en términos de costos, tiempos de implementación e impacto socioambiental. Estos dispositivos permiten controlar el flujo de potencia mediante la inyección de voltaje en cuadratura con la corriente de línea, modificando dinámicamente la impedancia del circuito. Sin embargo, esta característica plantea interrogantes sobre su interacción con los sistemas de protección de distancia, cuya operación se basa en la medición de impedancia durante eventos de cortocircuito. Este articulo evalúa el comportamiento de las protecciones de distancia en redes compensadas con M-SSSC, analizando escenarios de falla mediante simulaciones en entornos fasoriales y de transitorios electromagnéticos (EMT). Se hace enfásis en la funcionalidad de bypass de alta velocidad integrada en estos equipos, diseñada para mitigar posibles interferencias con los esquemas de protección existentes durante condiciones de falla.
Perguntas e Respostas

1- Os testes efetuados contemplaram falha na proteção do M-SSSC? Como foi o desempenho da proteção da linha?
Em caso de ocorrer uma condição de falha no bypass do dispositivo, o M-SSSC entra automaticamente em estado de monitoramento (IDLE), cessando completamente a injeção de tensão. Embora o M-SSSC não ative fisicamente o bypass, ao injetar tensão zero, sua presença torna-se imperceptível para os relés de proteção, pois não é detectada nenhuma contribuição adicional de tensão na rede.

Para validar esse comportamento, foram realizados testes comparativos do desempenho dos sistemas de proteção antes e depois da instalação do M-SSSC. Observou-se que a impedância medida em condições operacionais varia devido à função principal do dispositivo, que é controlar o fluxo de potência em regime permanente. No entanto, durante eventos de curto-circuito, a impedância de falta registrada foi equivalente, tanto com quanto sem a presença do M-SSSC.

Isso indica que, do ponto de vista da proteção de linha, não ocorre alteração na resposta esperada diante de uma falha, de modo que o desempenho da proteção é considerado adequado e consistente com as condições de projeto do sistema.

2 - Tem alguma recomendação para que seja utilizada proteção de distância nas linhas com M-SSSC?

2 - Tem alguma recomendação para que seja utilizada proteção de distância nas linhas com M-SSSC?

1 - Quais os principais desafios enfrentados nos testes?

Qual a eficacia do baypass no M-SSSC quando da deteção de sobrecorrente?
Quando é detectada uma condição de sobrecorrente, o M-SSSC envia um sinal de disparo para os SCR (Silicon-Controlled Rectifier), que são dispositivos de eletrônica de potência com resposta extremamente rápida. Para garantir uma operação confiável, o sistema conta com uma arquitetura redundante composta por dois SCR conectados em paralelo. Essa configuração, na qual os componentes permanecem normalmente fechados, permite que o bypass seja ativado de forma segura mesmo no caso de falha de um dos elementos. Essa estratégia garante que o equipamento entre em estado de bypass em um tempo estimado inferior a 1 milissegundo.
Esse comportamento foi considerado nos modelos EMT (Transitórios Eletromagnéticos) do dispositivo e validado por meio de testes de simulação em tempo real. Nessas simulações, avalia-se o desempenho do equipamento físico diante de condições específicas que ativam o bypass. Os resultados confirmam que os tempos de atuação permanecem abaixo de 1 ms e que a resposta dos sistemas de proteção (relés) não é negativamente impactada pela operação do bypass do M-SSSC.
Além disso, como medida adicional de confiabilidade, o M-SSSC incorpora um sinal de comando de bypass externo ao dispositivo, o que aumenta ainda mais a robustez do sistema de proteção. Em conjunto, essas características tornam o mecanismo de bypass do M-SSSC altamente eficaz para proteger o sistema em eventos de sobrecorrente.

Existem casos relatados de atuações indevidas ou recusas de atuação da proteção de distância devido a falha do by-pass integrado ao circuito de controle do compensador?
Nos estudos realizados até o momento, não foram identificadas condições que causem uma operação incorreta da proteção de distância como consequência de falhas no bypass do M-SSSC. Da mesma forma, nas instalações atualmente em operação em campo, não foram registrados eventos em que a proteção de distância tenha atuado de forma indevida ou tenha falhado em operar devido a um mau funcionamento do bypass.
Além disso, graças às medidas de redundância implementadas no projeto do equipamento, a probabilidade de uma atuação indevida da proteção de distância é consideravelmente reduzida, o que contribui para a confiabilidade geral do sistema.

Título - Testes de injeção de secundário em Merging Unit considerando o uso da tecnologia Low Power instrument Transformers
Entidade(s) - SecuBrasil Equipamentos de Teste e Medição Ltda,Conprove Industria E Comercio De Produtos Eletroeletronicos Ltda
Autor(es) - Paulo Sergio Pereira Junior,Antoni Furlani Rosa,André Luiz Rios,Rodolfo Cabral Bernardino,Gustavo Silva Salge,Cristiano Moreira Martins,Gustavo Espinha Lourenço,Paulo Sergio Pereira
Resumo
Toda a evolução tecnológica nos Sistemas de Proteção, Automação e Controle (PACS) impulsionada pelo advento da norma IEC 61850, culminou no estágio atual onde diversas subestações digitais tem sido implementadas ao redor do mundo.

Nesse sentido, todas as trocas de informações entre IEDs (Intelligent Electronic Devices) de diferentes fabricantes, utilizando os protocolos de comunicação definidos pela IEC 61850, demonstram a importância da interoperabilidade. Além disso, destaca-se a relevância e criticidade dos dados transmitidos na rede do Barramento de Processos, com ênfase particular na sincronização temporal, alcançada por meio do Precision Time Protocol (PTP), recurso indispensável nesse contexto. Nesse cenário, a forma de envio das informações de corrente e tensão é alterada por meio das Sampled Values (SV), cuja implementação pode ser realizada, por exemplo, com o uso de transformadores de instrumento não convencionais (do inglês NCITs – Non-Conventional Instrument Transformers), que possuem saída de baixa tensão, inerentemente mais seguros.

Assim, de forma a contribuir com o avanço e disseminação de sistemas de proteção baseados em IEC 61850, este trabalho tem como objetivo demonstrar a efetividade do uso de Low Power Instrument Transformers (LPITs) e Merging Units (MU).

Diversos testes em malha fechada serão demonstrados, onde foi realizada a injeção de sinais de baixa tensão nas entradas da Merging Unit de forma a simular as saídas de LPIT baseados em bobinas Rogowski e divisor capacitivo. A resposta da Merging Unit foi monitorada através da saída em Sampled Values via conexão em fibra óptica diretamente pela mala de testes. Os resultados dos testes serão discutidos em termos de verificação de linearidade, tempo entre frames SV, integridade das mensagens, perda de amostras ou amostras duplicadas, tempo de digitalização, precisão de amplitude e ângulo e sincronismo temporal.

Perguntas e Respostas

1 - Os autores apresentaram diversos benefícios para o uso de LPOIT. Qual o fator limitante para sua aplicação atualmente?

2 - Com relação ao LPIT, quais são os principais modos de falha deste equipamento e sua estimativa de vida útil?

Quanto aos modos de falha, eles podem ser separados basicamente em dois tipos: as falhas analógicas e falhas digitais.

A falhas digitais são aquelas que podem ocorrer após a digitalização do sinal e consequente envio dos sinais de Sampled Values. Todas as falhas pertinentes a 61850 podem ser aplicadas: perda de mensagens, mensagens duplicadas, tempo anormal entre mensagens, erros de formatação, falha na sincronização, etc.

Quanto as falhas analógicas, a mais relevante seria a falha na conexão (algum cabo rompido ou em curto). Mecanismos de detecção de canal de medição aberto ou em curto circuito devem ser utilizados para gerar alertas sobre essas falhas.

O encapsulamento do LPIT foi projetado e construído de forma análoga a uma partição convencional de resina fundida. Os sensores embutidos são completamente passivos (apenas fio de cobre). O equipamento foi aprovado no teste de envelhecimento artificial com 3 vezes a tensão nominal por >2000 h (equivalente a >50 anos de vida útil na tensão nominal). A PCB da caixa de conexão possui um MTBF calculado a 40°C de 397 anos e um MTBF calculado a 75°C de 86 anos. Sendo que os MTBFs em condições reais são tipicamente ainda maiores do que os calculados. A PCB pode ser substituída sem recalibração. Portanto, esperamos uma vida útil muito longa, similar à de Transformadores de Instrumento convencionais, sem impacto na vida útil geral da GIS.

Os autores poderiam detalhar um pouco mais como é o dispositivo que simula o LPIT? Qual a sua fidelidade com um LPIT de mercado?
O Low Power Adapter (LPA) é um equipamento totalmente analógico e passivo, construído de forma similar ao LPIT original. Usando dos mesmos princípios e componentes elétricos, somente com uma relação de transformação ajustada de forma proporcional a saídas de uma mala de testes. Ou seja, é fiel ao comportamento do LPIT de mercado pois utiliza componentes proporcionais e/ou equivalentes com o mesmo comportamento elétrico (bobina rogowski e divisores capacitivos ou resistivos).

Nos testes houve impacto numa comparação de aplicação convencional e LPIT no desempenho da proteção?
No trabalho apresentado, não foram realizados ensaios de proteção. O foco eram os ensaios com a Merging Unit sendo realizados de duas formas: injetando os sinais secundários de low level diretamente na MU, com uma mala de testes que possua saídas de baixa tensão, ou utilizando o adaptador de low level para malas de testes que não implementam essa tecnologia. Assim, através desses ensaios de malha fechada, utilizando a mala de testes, foram realizados testes de linearidade e erro percentual para as medições de tensão e corrente, de forma trifásica e monofásica. Além desses testes, foi realizado o monitoramento dos frames SV publicados pela MU, assinando-os e processando-os com o intuito de observar se existe alguma falha, do tipo perda de mensagem, mensagens duplicadas ou corrompidas. Foram verificadas questões de sincronização da MU, tempo entre amostras SV e tempo de digitalização da MU. A mala de testes também assinou e processou as mensagens SV também para verificar se os valores de amplitude e ângulo estavam dentro do esperado, realizando análises de oscilografia e fasoriais. A resposta transitória da MU não foi considerada nos ensaios.
Em todos os ensaios realizados, os resultados foram satisfatórios demonstrando que a tecnologia do LPIT é confiável. Isto implica que numa situação de proteção, principalmente naquelas que dependem de amostragem alinhadas no tempo, como esquemas de teleproteção baseados em SV que realizam comparação fasorial ou instantânea (ex: diferencial de linha), não haveria prejuízos no desempenho da proteção com relação à tecnologia baseada em transformadores de instrumento convencionais.

Os autores poderiam detalhar vantagens e desvantagens comparativas de LPITs que utilizam a medição ótica x LPITs que utilizam Bobina de Rogowski?

Título - Análise comparativa entre proteção de barras digital convencional e por barramento de processos
Entidade(s) - TRANSFORMADORES E SERVICOS DE ENERGIA DAS AMERICAS S.A.,Transformadores e Serviços de Energia das Américas
Autor(es) - Renato Augusto Di Loreto,Rafael Matiussi Vaz,Rodrigo Kenzo Kuniyoshi Pacheco
Resumo
Este estudo comparativo busca examinar as soluções sob diferentes perspectivas as quais são determinantes para a concepção de um novo projeto, observando alguns critérios como tempo de resposta da proteção e atuação das saídas digitais,

confiabilidade de cada filosofia e custos com projeto, materiais e implantação de cada solução.

Com base nos critérios apresentados, o artigo apresentará informações baseadas em histórico de execuções anteriores e avaliará pontos de atenção de cada solução para auxiliar na discussão de qual solução é mais adequada para cada caso.

Para exemplificar essas diferenças na prática, serão apresentados dois casos, baseados em situações reais de aplicação de proteção de barras em subestações de transmissão de 500kV no layout de disjuntor e meio, sendo que o primeiro projeto foi desenvolvido para uma a solução convencional e o segundo foi desenvolvido para uma solução digital por process bus, analisando as questões de tempo de resposta, custos e confiabilidade.

Perguntas e Respostas

1- Os autores poderiam elencar que pontos de atenção devem ser destacados no caso de aplicação de proteção de barras num barramento de processo

2- Um ponto importante é a possibilidade de expansão das proteções diferenciais de barra. Os autores podem comentar algo sobre este tema

Na comparação entre o sistema convencional e digital em termos de desempenho e custos faltaram alguns elementos, especialmente a bay-unit de uma subestação convencional. Que impacto teria isso nesta comparação?

Entendemos que a solução baseada em bay units de proteção, seguindo a arquitetura legada, apresenta um custo comparável ao de uma solução digital utilizando merging units. No entanto, é importante destacar que, nas soluções legadas, não era comum a instalação de painéis no pátio. Portanto, a economia com cablagem, um dos principais benefícios da digitalização, não se aplica nesse caso. Além disso, as bay units são dedicadas exclusivamente à proteção, enquanto as merging units, por sua natureza mais versátil, também podem ser utilizadas para funções adicionais, como proteção e controle do bay. Dessa forma, concluímos que uma solução convencional distribuída teria um custo semelhante ao de uma solução digital distribuída, porém sem os ganhos associados à redução de cabos e à simplificação da arquitetura física do sistema.

Considerando que a motivação deste trabalho surgiu a partir de dois casos reais — a implantação da proteção de barras na SE Fortaleza com uma solução convencional concentrada, e a modernização da proteção de barras na SE Ji-Paraná com uma solução digital distribuída utilizando merging units —, optamos por não abordar em detalhes a solução convencional distribuída. Ainda assim, reconhecemos que essa poderia ser uma alternativa adicional a ser considerada, embora seja uma abordagem que tende a ser gradualmente descontinuada.

Numa visão de custos, para as empresas de energia importa não apenas a implantação mas as ampliações futuras, que numa solução convencional é critica. Na opinião dos autores numa solução digital teriamos vantagens neste sentido?

Sim, algumas vantagens e outras desvantagens:

Vantagens:

- Diminuição de interfaces físicas;
- Diminuição da necessidade de desligamentos para sinais que possam ser lidos a partir da rede, sem necessitar desligamento de um bay;
- Dificilmente as atividades enfrentam limitações de espaço nos painéis existentes;

Desvantagens:

- Limitação entre sistemas de agentes diferentes;
- Maior cuidado com a implantação da rede e na configuração de switches e novos equipamentos;

Entendemos que riscos de desligamentos indevidos ou dificuldades de projetos são equivalentes em ambas as soluções.

Numa visão de custos, para as empresas de energia importa não apenas a implantação mas as ampliações futuras, que numa solução convencional é critica. Na opinião dos autores numa solução digital teriamos vantagens neste sentido?

Na comparação entre o sistema convencional e digital em termos de desempenho e custos faltaram alguns elementos, especialmente a bay-unit de uma subestação convencional. Que impacto teria isso nesta comparação?

Considerando as conclusões apresentadas que demonstram maior vantagem em termos de desempenho e custo de implantação da solução convencional em relação à solução por barramento de processo, como os autores vislumbram os futuros projetos de proteção diferencial de barras no ambiente em que as subestações tendem a ser totalmente digitais?

Baseado nas conclusões e no que foi visto nos projetos, se o principal critério de análise forem custos e tempo de atuação da proteção, as soluções digitais atuais não fazem sentido, pois apresentaram custos maiores e tempos de atuação mais elevados.

Caso a subestação já utilize soluções totalmente digitais, entendemos que a proteção de barras deve aproveitar os benefícios proporcionados pelas merging units e pela disponibilidade de sinais na rede, adotando, assim, uma solução completamente digital. Isso é especialmente viável, uma vez que os custos já estarão diluídos na implantação geral.

Título - SIPS – um recurso para minimizar/controlar as consequências de perturbações de grande porte

Entidade(s) - Power Security & Quality LTDA

Autor(es) - Paulo Gomes

Resumo

O crescimento contínuo do grau de penetração de novas gerações com inversores de potência, tem provocado um aumento da complexidade operacional dos sistemas de potência.

Neste contexto, verifica-se um menor número de geradores síncronos em operação, com consequente redução da inércia do sistema, dos níveis de curto-circuito e da controlabilidade dos sistemas. Por outro lado, mudanças climáticas, ataques

cibernéticos e outros fatores têm provocado um aumento das contingências caracterizadas por alto impacto e baixa frequência (High Impact/Low Frequency – HILF contingencies).
Para minimizar as consequências destas perturbações um dos recursos que estão sendo propostos é a utilização dos Special Integrity Protection Systems – SIPS .
Perguntas e Respostas

1- Como é classificado um WAMPAC ? É também classificado como SPIS?

2 - A PPS é a última linha de defesa do sistema , pois serve para promover ilhamentos inclusive para distúrbios não previstos nos estudos. Já os SEP , são definidos para distúrbios bem definidos e caracterizados , apesar de terem o mesmo objetivo. Quando todos estes esquemas são englobados na mesma nomenclatura , estes diferenças podem não ficar claras. Peço o comentários dos autores sobre o tema
A proposta do JWG é classificar os SPIS como uma proteção para os sistemas de potência como um todo, com 2 objetivos distintos:
- Aumentar os limites de transmissão em casos de contingências simples (N-1)
- Evitar/minimizar as consequências de contingências múltiplas (N-K)

Os SIPS se distinguem da proteção convencional cujo objetivo é a proteção de componentes da rede.

Existem casos especiais que um tipo de proteção pode ter a função de proteger o equipamento ou o sistema como um todo. Exemplo: perda de sincronismo de um gerador ou acelerar a separação do sistema em caso de perda de sincronismo. Outro caso: corte de geração para controle de carregamento ou para condições de instabilidade.

Os Planos de Defesa são compostos de várias ações. No caso do ONS e outros Operadores de Sistemas:
- medidas para reduzir o impacto das perturbações
- medidas para evitar/minimizar a propagação das perturbações
- medidas para reduzir o tempo de recomposição

Nos últimos 10 – 15 anos com as mudanças em curso (Transição Energética) e o surgimento das denominadas perturbações do tipo HILF (High Impact Low Frequency) as medidas para redução dos tempos de recomposição têm sido também tratadas com prioritárias. Como exempla pode-se citar as ações implantadas pela PJM (Estados Unidos).

No Brasil, o ONS implantou o seu Plano de Defesa em 2003 e as medidas para redução dos tempos de recomposição foram estabelecidas, com base na experiência acumulada desde o tempo do GCOI. As seguintes medidas constam deste Plano: ilhamento de usinas térmicas com carga local, ilhamento de usinas hidrelétricas de médio porte com carga local e 'House Load Operation 'da usina Nuclear de Angra 2 (Ilhamento da usina com a carga dos serviços auxiliares). Tais medidas evitam o desligamento destas usinas, o que provocariam um tempo apreciável para o retorno das mesmas a operação, o que aumentaria o tempo de

recomposição do sistema.

3 - Qual o objetivo e o estado dos trabalhos do citado (JWG C2/B5.46)?
O JWG C2/B5 tem o seguinte objetivo: “Contribute to increase understanding of SIPS: values, opportunuties, and impact on secure operation of the power system”

- 55 membros
- 15 países
Membros brasileiros: Paulo Gomes / Rafael Fontoura / Jeder Francisco de Oliveira
O trabalho (Brochura Técnica) está sendo elaborado em 12 capítulos:
1- Introdução
2- Revesiting definitions of SIPS in the (N-1) criteria perspective
3- SIPS design -operation and control aspects
4- SIPS design -protection and automation aspects
5- Implementation management
6- Operation management
7- Maintenance, revision & adaptation management
8- International examples and experiences
9- Assessment of SIPS drawbacks and risks
10- Future forecasted needs, and requirements/questions for further research
11- Conclusions
References

A primeira reunião do JWG foi realizada em 29/08/2024, tendo sido até agora realizadas 6 reuniões.

Entregas:
-Artigo revista ELECTRA
-TUTORIAL
- BROCHURA TÉCNICA

Brochura Técnica:
1º draft - setembro/2025
2º draft – janeiro/2026
3º draft – maio/2026
Final draft - janeiro/2027

Como os SIPS estão sendo considerados no contexto da digitalização dos sistemas de proteção e automação?
A digitalização dos sistemas de proteção e automação permite facilitar/melhorar a concepção e a implantação de SIPS, lembrando sempre que os mesmos devem estar sintonizados com a segurança cibernética e que as medições e comandos de acesso devem ser protegidos da ação de hackers e de acesso não autorizados.

Título - AVALIAÇÃO DAS FUNÇÕES DE OSCILAÇÃO DE POTÊNCIA DO SISTEMA ACRE-RONDÔNIA ATRAVÉS DE TESTE NO SIMULADOR DIGITAL EM TEMPO REAL EM MALHA FECHADA COM OS IED DE PROTEÇÃO
Entidade(s) - Operador Nacional do Sistema Elétrico,Jauru Transmissora de Energia S.A.,Siemens Infraestrutura e Indústria LTDA
Autor(es) - Tatiana Maria Tavares de Souza Alves,Denise Borges de Oliveira,Karina Stockler Herszterg,Matheus Sene Paulo ,Alex de Castro,Oscar Antonio Solano Rueda,Claudinei Santana da Rocha,Diego Pontes de Mello
Resumo
Este artigo apresenta a etapa de testes para avaliação e aprimoramento dos novos ajustes e filosofia das funções de disparo por oscilação de potência (68OST) que foram aplicadas no tronco de 230 kV que interliga o subsistema Acre-Rondônia ao SIN – Sistema Interligado Nacional. São apresentadas as etapas de proposição dos ajustes, as metodologias utilizadas nos testes e resultados. Também são apresentadas as dificuldades encontradas e os benefícios agregados na utilização do Simulador Digital em Tempo Real. Nesse sentido, é dado destaque que esse recurso de simulação se torna cada vez mais necessário na busca da segurança de ajustes sistêmicos, visto que o sistema elétrico está cada vez mais complexo e a representação fidedigna dos sistemas de proteção nos estudos elétricos se torna imprescindível.
Perguntas e Respostas

O trabalho cita a importância das simulações em RTDS especialmente em proteções sistêmicas. Que ações os autores entendem que poderia se estabelecer como rotina para antever situações de maior risco?
A experiência desse trabalho, mostrou que o teste RTDS deve ser inserido como rotina para qualquer processo de ajuste de funções de perda de sincronismo para aplicação no SIN, visto que através dele é possível testar o algoritmo real do IED as suas coordenações. Especialmente, considerando que os sistemas estão cada vez mais complexos e os algoritmos tradicionais dessas funções podem ser afetados pela alta penetração de IBRs e elementos baseados em eletrônica de potência.

Considerando as mudanças complexas no sistema de potência os autores entendem que pode haver necessidade de revisitar os ajustes e testes realizados?
Sim, no caso de expansão significativa da rede ou modernização das proteções atuais os ajustes e testes devem ser revisitados.

Foi avaliada a possibilidade de aplicar R-GOOSE na solução?

Foi avaliada a possibilidade de aplicar R-GOOSE na solução?

Considerando os resultados obtidos neste estudo com as simulações em ambiente RTDS, em complemento às simulações de estabilidade eletromecânica, o ONS pretende utilizar essa ferramenta como padrão para

simulações de validação de ajustes de funções de oscilação de potência e de perda de sincronismo?
Sim, sempre que possível essa etapa de estudos no RTDS será utilizada para agregar segurança aos ajustes.

Título - ENSAIOS, SIMULAÇÕES E MODELAGEM DO SISTEMA DE POTÊNCIA NO SIMULADOR EM TEMPO REAL (RTDS) PARA MODERNIZAÇÃO DAS PROTEÇÕES DE LINHAS, BARRAS, GERADORES E TRANSFORMADORES DA USINA DE ITAIPU
Entidade(s) - GENERAL ELECTRIC DO BRASIL LTDA,Fundação Parque Tecnológico Itaipu - Brasil,GRID SOLUTIONS TRANSMISSAO DE ENERGIA LTDA,GENERAL ELECTRIC
Autor(es) - Denys Lellys,Rafael Cesar Jabor Fagundes Nogueira,LEONARDO DE ASSIS NIZER,Paulo Thiago de Godoy,Liz Rosana Alvarez Ferreira,Hector León,Guilherme Justino,Augusto Dias Hubner,Ícaro Bispo de Moura e Rocha
Resumo
O artigo relata a experiência dos ensaios, simulações e modelagem do sistema de potência Brasileiro e Paraguaio no simulador em tempo real (RTDS) para validação de modelo e aferição de ajustes com a finalidade de modernização dos sistemas de proteção de barras, linhas, transformadores e geradores da usina hidrelétrica da ITAIPU binacional, como também garantir o correto funcionamento dos sistemas de proteções propostos sob diferentes condições de falha e carga do sistema. Os ensaios foram executados em malha fechada com o RTDS nas dependências do centro de competência em gestão energética (GE.DT) do laboratório Itaipu Parquetec.
O projeto de modernização dos sistemas de proteção dos sistemas elétricos da UHE Itaipu binacional, contempla a substituição completa de todas as proteções principais e de retaguardas das 10 (dez) unidades geradoras de 50 Hz, 10 (dez) unidades geradoras de 60 Hz, 10 (dez) transformadores elevadores 18 kV/500 kV – 50 Hz, 10 (dez) transformadores elevadores 18 kV/500 kV – 60 Hz, 04 linhas de transmissão 500 kV-50 Hz, 04 linhas de transmissão 500 kV-60 Hz, 04 (quatro) sistemas de barras de 50 Hz e 04 (quatro) sistemas de barras de 60 Hz.
Perguntas e Respostas

1 - Qual a maior dificuldade enfrentada para a realização dos testes ?

2 - Quais as novas inovações nas funções de proteção de geradores testadas no RTDS ? E qual o desempenho obtido para estas funções?
Uma função de proteção de destaque foi a função de perda de excitação (40), implementada como curva "tomate" com várias vantagens em comparação com a tradicional curva MHO.

Entre as principais vantagens desatacamos:

1. Atuação instantanea quando da perda de excitação total;
2. Maior confiabilidade devido a temporização e uttilização dos critérios de rotor e estator.
3. Maior fexibilidade de faixa de ajustes.

Qual a dificuldade enfrentada na modelagem para o RTDS?
A modelagem do equivalente dinamico, ao invés do equivalente de curto circuito, do sistema da ITAIPU, representando todas as unidades geradoras e os controles associados tais como regulador de tensão, regulador de velocidade e o sistema de estabizaçao de potência (PSS), consumiu um tempo consideravél de modelagem e também a falta de modelos na biblioteca do RSCAD, por exemplo transformadores do sistema de excitação com conexão estrela-zig-zap, necessitou novo desevolvimento do modelo. Também a modelagem dos transformadores de corrente, cujos dados preliminares não estavam em acordo com os dados do campo, sendo necessários a realização de trabalho especifico para aferir as curvas de saturação.

O autor destacaria algum teste de proteção de geradores realizado ou a realizar onde se obteve ou se espera obter resultados mais precisos quando comparados com os tradicionais testes ralizados até então?
Testes de proteção de geradores no RTDS são raramentes executado pelos agentes e também pelos fabricantes. Recomenda-se fortemente que em modernizaçóes e retrofit de usinas seja incluido como requisito mandatório aferir o algoritmo do relé digital de proteção e validar a perfomance no RTDS.

Título - Implantação e testes do maior Sistema Especial de Proteção do SIN: SEP das Interligações Norte-Nordeste-Sudeste
Entidade(s) - Operador Nacional do Sistema Elétrico,Autarquia Federal,Ysmart Engenharia Capacitacao e Tecnologia LTDA,Transmissora Aliança de Energia Elétrica S.A,Schweitzer Engineering Laboratories,SCHWEITZER ENGINEERING LABORATORIES COMERCIAL LTDA,GRACA ARANHA SILVANIA TRANSMISSORA DE ENERGIA,BELO MONTE TRANSMISSORA DE ENERGIA SPE,Instituto Militar de Engenharia
Autor(es) - Igor de Siqueira Cardoso,Edson Ferreira de Oliveira,Bruno Pestana Rosa,Yona Lopes,Natalia Castro Fernandes,Helio do Nascimento Cunha Neto,Thales Gabriel Ribeiro Quintino,Ronald Serra Jogaib Cabo,Marcos Vinicius Guimaraes Cabral,Ricardo Abboud,Victor Argemil Teixeira,JEFFERSON MENDES AMANCIO,Marcos Vinícius Pimentel Teixeira
Resumo
A crescente complexidade do Sistema Interligado Nacional do Brasil exige soluções inovadoras para garantir sua operação segura e otimizada. Nesse contexto, o SEP das Interligações Norte-Nordeste-Sudeste foi desenvolvido para atuar de forma rápida e eficiente, prevenindo sobrecargas e perda de sincronismo entre regiões diante de contingências no sistema de transmissão de 500 kV. O SEP N-NE-SE cobre uma área de aproximadamente 750.000 km² e integra ativos de 15 concessionárias, exigindo uma arquitetura de comunicação robusta e segura para a coleta de dados em tempo real e o envio de comandos corretivos. Para isso, foram estabelecidas três redes distintas: a rede do SEP, baseada em mensagens GOOSE (IEC-61850) para sinais de missão crítica; a rede de Monitoramento e a rede de Supervisão, utilizadas para gerenciamento via protocolos MMS (IEC-61850) e SNMP. O sistema apresenta um aspecto inovador ao executar ações adaptativas nos bipolos HVDC, modulando potência de forma dinâmica para restaurar o ponto operativo pré-perturbação. Essa abordagem foi validada por testes em ambiente

RTDS e por ações reais em campo. O artigo discute os desafios e etapas de implementação do SEP, desde testes de aceitação em fábrica até a validação integrada em campo. Os testes demonstraram tempos de atuação de até 40 ms em cenários críticos, confirmando o sucesso da solução adotada, bem como desempenho das ações de controle condizente com os resultados de RTDS. Este SEP entrou em operação definitiva no dia 15 de dezembro de 2024.

Perguntas e Respostas

1 - Qual o maior desafio enfrentado na implantação deste SEP?

2 - Futuras ampliações terão necessidade de testes em RTDS? Existe uma plataforma permanente montada para este tipo de teste?

Os testes em RTDS serão novamente necessários apenas quando houver revisões do SEP que ensejem alterações nas lógicas de controle do sistema HVDC como, por exemplo, alteração das taxas de execução das rampas de run-up ou run-back, ou a necessidade de novos sinais que interajam com o Controle Mestre do sistema HVDC. Uma vez que o RTDS do ONS dispõe de réplicas dos controles desse sistema, é proveitoso realizar testes das lógicas neste ambiente de simulação, para reduzir o tempo de testes em campo, uma vez que estes podem impor restrições ao sistema e custo elevado para a operação. Esta plataforma é permanente.

Para a validação de demais alterações de lógicas nos IED do SEP, por outro lado, poderá ser utilizada a plataforma de testes do SEP. Nesta plataforma, também permanente, podem ser carregadas as configurações de qualquer IED do SEP.

2 - Futuras ampliações terão necessidade de testes em RTDS? Existe uma plataforma permanente montada para este tipo de teste?

3 - Como é feito o monitoramento da rede utilizada no SEP e que requisitos são monitorados?

A troca de sinais entre os IEDs envolveu mensagens GOOSE e SV? Como se garantiu a segurança cibernetica a conectar redes de agentes diferentes?

Foi possível atender as necessidades de missão crítica do SEP exclusivamente com mensagens GOOSE. Esses sinais compreendem sinalizações de estado do equipamento, de atuação de proteção, de atuação de lógicas do SEP, e medições de fluxo de potência ativa. As medições de fluxo de potência também são incluídas nos datasets GOOSE, que são publicadas na rede a cada 10 ms.

A segurança cibernética entre diversos agentes foi garantida através da concepção de uma rede isolada com aspectos de bloqueio para proteger tanto a rede do SEP, quanto a rede do agente com definições claras descritas nos requisitos mínimos de implementação da rede. Foi estabelecida uma rede única do SEP, com uma porta exclusiva e distinta do acesso de gerência, protegida por equipamento de segurança com regras de acesso. Outros exemplos de aspectos de segurança incluem controle do tráfego (nesta rede trafegam apenas mensagens GOOSE). A solução escolhida pelos agentes para esse fim foi a utilização de switches SDN, nos quais foram implementadas regras de filtragem de mensagens GOOSE, bem como outras regras.

Esses equipamentos foram implementados, minimamente, no ponto de chegada ou partida de cada subestação envolvida no SEP, sendo o ponto de interface entre os IED locais e com o equipamento de telecomunicação. Dessa forma, nenhum tráfego que não seja previsto pode sair da subestação, ou mesmo trafegar localmente entre os IED.

A troca de sinais entre os IEDs envolveu mensagens GOOSE e SV? Como se garantiu a segurança cibernetica a conectar redes de agentes diferentes?

Os IEDs instalados nas instalações dos diversos agentes são exclusivos para o SEP?
Sim. Conforme a filosofia atualmente empregada pelo ONS, este SEP se configura como Tipo 1, implicando que possui o maior nível de criticidade, bem como de requisitos de implantação. Entre esses requisitos, considera-se a completa redundância e independência de demais sistemas de proteção e controle dos equipamentos monitorados. Portanto, não é admitida a utilização dos sistemas de proteção existentes para as funções do SEP.

Quais são os requisitos de redundância adotados para o IED Master instalado na SE Colinas?

Título - Virtualização e Centralização da Proteção e Controle: Transição do Gerenciamento de Dispositivos para a Gestão de Aplicações
Entidade(s) - Siemens Ltda
Autor(es) - Guilherme Cristofani De Sanz Pires,Jorge luis Gambini Damasceno
Resumo
A digitalização desbloqueou novas e significativas formas de trazer valor aos consumidores/clientes. A rede de energia elétrica está passando por uma rápida transformação e está em uma trajetória de evolução digital. Com a rápida transformação da rede, os desafios já existentes de gerenciamento de ativos e patches , inventário de ativos, mudanças adaptativas de configurações, expansibilidade e implantação mais rápida são ainda mais amplificados. É extremamente importante adotar novas abordagens tecnológicas que possam potencialmente ajudar a superar ou minimizar os desafios necessários. Existem 3 elementos para abraçar uma nova abordagem: tecnologia, pessoas e processos. A tecnologia não é uma barreira ou impedimento. A tecnologia está presente para apoiar, aprimorar certos aspectos e potencialmente minimizar a complexidade. Pessoas e processos são elementos onde uma nova abordagem tecnológica requer mais adaptações. Este artigo concentra-se em fornecer uma visão sobre a virtualização como uma nova abordagem tecnológica. O artigo fornecerá um contraste entre conceitos convencionais e virtualizados de proteção e controle, juntamente com a necessidade de virtualização. O conceito virtualizado abordará duas tecnologias diferentes: máquinas virtuais e conteinerização. O conceito de virtualização concentra-se em desacoplar aplicações de proteção e automação de dispositivos embarcados para permitir a implantação de aplicações de software em hardware mais poderoso (servidores industriais ou computadores). Discutem-se em detalhes os benefícios da arquitetura de software conteinerizada em comparação

com a arquitetura baseada em máquinas virtuais e, por fim, este artigo apresentará resultados de testes de aplicações de proteção e controle em ambiente virtualizado em comparação com relés de proteção digital embarcados.

Perguntas e Respostas

1 - Um dos pontos a serem explorados dizem respeito a segurança cibernética e manutenção do sistema. Os autores tem alguma colocação sobre estes temas?

2 - Esta arquitetura de software conteinerizada já está aplicada em alguma subestação como piloto?

3 - Como ficam o monitoramento da rede e a redundância dos sistemas de proteção no caso de utilização de arquitetura de software conteinerizada?
Em arquiteturas conteinerizadas, o monitoramento de redes e protocolos de redundância (PRP, HSR) seguem os mesmos princípios descentralizados, com um número bem menor de dispositivos, uma vez que inúmeros relés de proteção serão substituídos por um servidor principal e um redundante. A conteinerização, via orquestração (Kubernetes), otimiza a resiliência dos serviços subjacentes com auto-healing, replicação e escalonamento dinâmico, garantindo a continuidade operacional.

Como sera a integração de diferentes fornecedores na mesma plataforma computacional?
Ao integrar diferentes fornecedores, uma 'abordagem multi-fornecedor' oferece flexibilidade, mas frequentemente leva a desafios como maior esforço de integração, falta de padrões de arquitetura comuns e questões complexas de responsabilidade. Na Siemens, inclinamo-nos para uma abordagem 'específica do fornecedor', que combina nosso hardware, software e ferramentas de engenharia em um ecossistema coeso. Isso nos permite garantir desempenho otimizado, fornecer suporte simplificado e reduzir significativamente o esforço de integração para nossos usuários, entregando uma solução mais confiável e fácil de gerenciar.

Os autores acreditam que a virtualização permitira pensar em processamento em nuvem (especialmente na distribuição)?

Os autores realizaram algum estudo comparativo de custos de implantação da arquitetura centralizada em relação à arquitetura distribuída?
No momento, ainda não foram concluídos estudos comparativos de custos abrangentes e formais que avaliem a implementação de arquiteturas centralizadas versus distribuídas. No entanto, esta é uma etapa crucial em nossa análise contínua. Estamos atualmente focados em projetos-piloto para ambas as abordagens. A ideia é que, ao implementar e testar essas arquiteturas em cenários reais e controlados, possamos coletar dados de custos, esforço de integração, desempenho e manutenção de forma mais precisa e prática. Esses projetos-piloto nos permitirão entender as nuances financeiras e operacionais de cada modelo em nosso contexto específico. Os resultados desses pilotos serão fundamentais para a realização de

um estudo comparativo de custos detalhado no futuro, fornecendo uma base sólida para decisões estratégicas.

Título - Ensaios em Virtual Protection, Automation and Control Systems (vPACS)
Entidade(s) - Conprove Industria E Comercio De Produtos Eletroeletronicos Ltda
Autor(es) - Paulo Sergio Pereira Junior,Rodolfo Cabral Bernardino,Gustavo Espinha Lourenço,Paulo Sergio Pereira,Gustavo Silva Salge,Cristiano Moreira Martins
Resumo
Devido ao crescente número de subestações digitais baseadas na norma IEC 61850 sendo implementadas em todo o mundo, a próxima etapa na evolução dos sistemas de proteção, automação e controle envolve o desacoplamento do software do seu hardware dedicado, virtualizando funcionalidades e, assim, criando uma rede definida por software (software-defined smart grid).

Considerando que o vPACS está na vanguarda do desenvolvimento tecnológico dos SAS (Sistemas de Automação de Subestações), este artigo tem como objetivo explorar os requisitos de teste nesse novo paradigma, comparando os requisitos para testes de IEDs físicos com aqueles para testes de IEDs virtuais (vIEDs). Serão discutidas as semelhanças e diferenças entre essas duas abordagens de teste, bem como sugestões para sua realização. Além disso, os testes no contexto do vPACS será investigado utilizando tanto ferramentas de testes físicas quanto virtuais, comparando as diferenças, vantagens e desvantagens de cada método.

Serão abordadas as diferentes etapas de teste, como testes de comissionamento (FAT – Factory Acceptance Tests e SAT – Site Acceptance Tests) e testes de manutenção, os passos gerais para a realização dos testes (isolamento do DUT – Device Under Test, simulação e captura da resposta), além de questões relacionadas à sincronização de tempo no contexto do vPACS. Também será feita uma comparação entre a aplicação de um arquivo COMTRADE a partir de uma mala de testes física e a aplicação de um arquivo PCAP a partir de uma mala de testes virtual para análise de registros de perturbação.

O artigo inicia com uma análise histórica dos sistemas de proteção, traçando sua evolução desde os primeiros relés implementados com chaveamento eletromecânico até a virtualização. Em seguida, serão abordados alguns conceitos básicos dos mecanismos de virtualização essenciais para a compreensão do vPACS. Os requisitos fundamentais do vPACS, juntamente com seus desafios de implementação, também serão abordados.

Por fim, será explorada a evolução das ferramentas de teste, além da evolução dos IEDs, bem como os métodos de implementação do ambiente de teste em um contexto virtualizado.
Perguntas e Respostas

1- Diversos são os fatores citados desafiadores para utilização de Vpac. Um dos principais diz respeito a interoperabilidade. Pode detalhar mais as dificuldades e necessidades para garantir a interoperabilidade neste caso?

A interoperabilidade no âmbito do vPACS vai além do contexto da comunicação e troca de informações entre IEDs de diferentes fabricantes, verificada quando da implementação de mecanismos e protocolos de comunicação como GOOSE, SV, PTP e MMS. Deve-se verificar a interoperabilidade no âmbito de software e infraestrutura de virtualização, envolvendo aspectos como:

- Requisitos do software desacoplados de requisitos de hardware: os vIEDs devem

ser descritos de forma abstrata do hardware. Isto é, os descritores de hardware e mecanismos de virtualização (hypervisor ou container engine) devem ser tais que não dependam de requisitos específicos do ambiente de execução;
- Interfaces padronizadas (APIs): para assegurar a interoperabilidade no ambiente de execução do vPACS, envolvendo aplicações de diversos fabricantes, é necessário que as APIs utilizadas sejam padronizadas.

2- Poderia elencar de forma resumida os benefícios de uma caixa de teste fisica com relaçao a uma caixa de testes virtual e vice versa?

Na visão dos autores a virtualização facilitara a aplicação de Inteligencia Articial, já que esta depende de uma plataforma computacional tambem?
No vPACS, os dados de corrente, tensão, trip, sincronização temporal, lógicas entre IEDs, redundância, monitoramento e sistema supervisório estarão todos digitalizados e centralizados em um servidor. Tais condições são pré-requisitos fundamentais para alimentar a Inteligência Artificial (IA) e realizar seu treinamento. Assim, fica claro que a virtualização facilitará a aplicação da IA no sistema de proteção das subestações digitais. Além disso, a IA também pode ser implementada na gestão de ativos (asset management).

A formação e o treinamento do pessoal responsável por lidar com os sistemas PCA das subestações neste momento de introdução de novas tecnologias é uma preocupação permanente. Quais são os impactos previstos para as atividades de manutenção e testes de sistemas PAC com a introdução de sistemas vPACS?
Com o desenvolvimento do vPACS, surgem novos desafios concernentes aos ensaios de proteção em comissionamento (TAF - Testes de Aceitação de Fábrica e TAC - Testes de Aceitação de Campo) e em manutenção. Tais desafios estão relacionados aos instrumentos de testes utilizados e à capacitação do pessoal técnico.
As novas ferramentas de testes devem atender aos requisitos do vPACS em termos de implementação de GOOSE, Sampled Values e PTP, de forma a realizarem os ensaios de proteção no ambiente virtualizado com sucesso. Tanto instrumentos de testes físicos quanto virtuais, como aplicativos em um servidor, podem atender às demandas em questão, desde que estejam preparadas para esse contexto, principalmente às exigências de tempo crítico dos SV e GOOSE com informações de trip. Outra questão importante, ainda nesse cenário, é a integração da solução de testes à arquitetura de rede utilizada no vPACS, que deve prever um uso duplicado de largura de banda, por conta dos frames simulados.
Para extrair o máximo potencial das soluções de testes nesse contexto que exige novos métodos de ensaios de proteção, é imprescindível que a equipe técnica esteja capacitada e atualizada nos requisitos da norma IEC 61850. Conceitos básicos de redes de comunicação, orientação a objetos, modelagem de dados, cybersecurity e funcionamento dos mecanismos GOOSE, SV e PTP, são básicos realizar os ensaios de proteção e analisar possíveis falhas.

Título - Análise de desempenho da primeira subestação digital do Grupo CPFL
Entidade(s) - COMPANHIA PAULISTA DE FORÇA E LUZ

Autor(es) - Wagner Seizo Hokama,Letícia Lima Trujillo de Souza
Resumo
Uma subestação digital exige um novo método para a análise do desempenho do seu sistema de supervisão e controle, visto a sua complexidade tecnológica e desafios na arquitetura do sistema de comunicação.
Esse artigo apresenta a experiência da CPFL no acompanhamento do desempenho da subestação digital de Bethânia (primeiro bay – Transformador 1, que depois evoluiu para mais três bays) e Souzas (primeira subestação completa), nas cidades de São Carlos e Campinas, respectivamente, ambas no estado de SP, sendo que o primeiro projeto foi realizado com a solução Siemens e o segundo projeto foi realizado o teste de interoperabilidade entre os equipamentos de quatro fornecedores diferentes.
No caso da SE Bethânia, o sistema já foi apresentado em outros congressos, cabendo nesse artigo uma atualização do seu desempenho após 5 anos de implantação e ampliação para mais três bays.
Já na SE Souzas, a interoperabilidade de IEDs e MUs de diferentes fornecedores em uma mesma rede foi avaliado, assim como as ferramentas de configuração dos fabricantes para a troca de arquivos SCL para o processo de engenharia.
Por fim, é apresentado como o monitoramento das mensagens SV e GOOSE, alertando quando há falhas ou indisponibilidade de alguma funcionalidade, é essencial para o aumento significativo da confiabilidade do sistema.
Perguntas e Respostas

1- As falhas verificadas de GOOSE estavam relacionadas com o IED e não com a rede, pelo exposto no trabalho. O desempenho da rede está sendo monitorado também, ou apenas as mensagens de diagnósticos dos IEDs?
O desempenho da rede foi monitorada durante o TAF e TAC. Também estamos prevendo alguns monitoramentos periódicos, visando identificar alguma alteração ou degradação da rede, mas entendemos que não seja necessário em regime permanente.

2 - A dificuldade de utilização de diversas ferramentas específicas para cada fabricante , e até mesmo na padronização dos arquivos SCD , é uma das maiores dificuldades para implementação , manutenção e monitoramento dos sistemas de proteção numa SE digital . Esta experiência também pode ser verificada pelos autores?

3 - Com a experiencia obtida até o momento nas se digitais, a CPFL tem a intenção de caminhar para uma padronização de projetos? Qual foi o principal desafio encontrado?

1 - A troca de sinais entre os IEDs envolveu mensagens GOOSE e SV? Como se garantiu a segurança cibernetica a conectar redes de agentes diferentes?

Como foi na expansão de novos bays a questão de diferentes versões da Norma IEC 61850 aplicadas em IEDs?
Ainda não passamos por isso, mas pretendemos manter o mesmo padrão inicial.

Que impacto no desempenho tem tido o dominio das equipes de manutenção?

O artigo relata falhas relacionadas ao sistema de automação que foram solucionadas com a substituição do firmware dos equipamentos digitais. Essas falhas eram passíveis de serem identificadas na etapa de comissionamento (TAF/TAC)?
Infelizmente isso não foi identificado em TAF e TAC, pois tratou-se de um defeito intermitente.

O autor poderia detalhar um pouco mais a dificuldade encontrada com a manipulação dos arquivos SSD? Essa dificuldade, à luz da padronização estabelecida pela Norma, era esperada?

Título - Recomendações para a Implementação do Barramento de Processos em Subestações Digitais à Luz do WG B5.69
Entidade(s) - Conprove Industria E Comercio De Produtos Eletroeletronicos Ltda
Autor(es) - Paulo Sergio Pereira Junior,Rodolfo Cabral Bernardino,Gustavo Espinha Lourenço,Paulo Sergio Pereira,Gustavo Silva Salge,Cristiano Moreira Martins
Resumo
Este trabalho realiza uma análise das recomendações do WG (Working Group) B5.69 para a implementação do Barramento de Processos em subestações digitais baseadas na norma IEC 61850, abordando aspectos técnicos, econômicos e operacionais. Desafios serão discutidos, como custos iniciais, estratégias de redes redundantes, sincronização temporal via Precision Time Protocol (PTP), segurança cibernética e a interoperabilidade.
Aspectos importantes também serão abordados, como definição de estratégias de testes na fase de comissionamento, abrangendo tanto os Testes de Aceitação de Fábrica (TAF) quanto os Testes de Aceitação de Campo (TAC), capacitação técnica e gestão de ativos.
Os benefícios da implementação do barramento de processos, incluem redução de custos e maior eficiência operacional, no entanto existem desafios com relação à interoperabilidade e sincronização de tempo quando em condições adversas de rede, tais questões também serão discutidas no artigo.
Perguntas e Respostas

1 - Baseado na experiencia dos autores na utilização de barramento de processos , qual o ponto mais relevante.?
A rede de comunicação é um ativo muito importante da subestação digital, consequentemente é o ponto mais relevante do barramento de processos a ser considerado. Apesar da interoperabilidade ser a grande contribuição da norma IEC 61850, sem uma rede de comunicação sadia, ela não seria possível. Sendo assim, torna-se extremamente importante a adoção de sistemas especializados de diagnóstico e monitoramento, que apontem e registrem eventos de falha na rede.

Na opinião dos autores quais fatores seriam mais decisivos para gerar a escala de aplicação do barramento de processo?

Uma das primeiras barreiras para uma implantação em larga escala do barramento de processos é o receio inerente a uma tecnologia ainda incipiente. A melhor forma de vencer tal barreira é através da adoção de procedimentos e rotinas de testes bem definidos que irão trazer a confiança necessária na nova tecnologia e, consequentemente, contribuir para gerar escala na aplicação do barramento de processos. Outra questão importante, e também atrelada às questões de testes, é o desenvolvimento de políticas específicas para treinamentos e reciclagens periódicas para os colaboradores da área técnica no contexto da norma IEC 61850.

Os autores afirmam no trabalho, a respeito do monitoramento da rede IEC61850, que "Dispositivos especializados são necessários para monitorar todos os aspectos de rede, incluindo aqueles com exigência de tempo crítico". O WG B5.69 em suas conclusões chega a sugerir ou detalhar qual seria o modo mais eficiente e seguro de realizar esse monitoramento?
O WG B5.69, nas suas recomendações para a implementação do barramento de processos em subestações digitais, no capítulo 9, trata da parte de monitoramento tanto das condições dos equipamentos de primário quanto da rede de comunicação no PACS. Inclui alguns Logical Nodes de monitoramento da norma IEC 61850 como LCCH, LTMS, LGOS e LSVS. Já no capítulo 12 (conclusões), cita que o integrador do sistema precisa considerar no projeto os limites da tecnologia de comunicação atual com relação a desafios como taxa de transferência de pacotes, largura de banda e latência, além da sincronização temporal.
No entanto, não descreve detalhadamente ou sugere, indicando qual o modo mais eficiente de se realizar o monitoramento no barramento de processos. Fica a cargo do gestor de ativos, junto com uma equipe técnica especializada, avaliar a importância de se ter um sistema de monitoramento implementado em hardware e software, com a capacidade de monitorar aspectos de tempo crítico de mecanismos como GOOSE e SV. Tais aspectos envolvem transfer time, tempo de digitalização de amostras SV e tempo entre frames.
É importante ressaltar que está em andamento um trabalho conduzido pelo WG B5.86 que vai abordar mais profundamente o monitoramento de redes nas subestações digitais.

Título - Proteção Diferencial de Linhas com IEDs Virtuais em Subestações IEC 61850: Implementação e Avaliação
Entidade(s) - Universidade de São Paulo,Universidade Federal da Bahia
Autor(es) - Alailton Alves,Denis Vinicius Coury,Ricardo Augusto Souza Fernandes,Daniel Barbosa
Resumo
Este informe técnico avalia a aplicação de IEDs virtuais na implementação da proteção diferencial de linhas em subestações digitais, conforme os padrões estabelecidos pela IEC 61850. Diferentemente dos IEDs físicos, que são dispositivos de hardware dedicados com interfaces de entrada/saída e circuitos especializados para o processamento de sinais, os IEDs virtuais são implementados em ambientes computacionais, como máquinas virtuais ou contêineres, executados em servidores centralizados. Essa abordagem permite não apenas a replicação fiel das funções de proteção e controle, mas também a redução significativa dos custos, a simplificação dos procedimentos de manutenção e a facilidade na atualização das funcionalidades, em consonância com as tendências de digitalização e

modernização das subestações. A proposta aborda o desenvolvimento de uma arquitetura de software open source que replica com alta fidelidade as funções dos IEDs convencionais para aplicação em subestações digitais. O estudo investiga a implementação dos algoritmos de proteção diferencial, enfatizando a comunicação sincronizada entre dois dispositivos virtuais e a análise dos tempos de resposta, bem como dos atrasos nos sinais de trip durante a ocorrência de faltas. Ensaios, conduzidos com base em simulações computacionais de uma linha de transmissão, com medições realizadas em ambas as extremidades e a replicação de diversos cenários de falta por meio de um gerador de SV, evidenciaram que a virtualização dos dispositivos apresenta desempenho comparável ao dos IEDs tradicionais, registrando um atraso médio de 1 ciclo e um máximo de 2,6 ciclos, além de proporcionar significativas vantagens em termos de flexibilidade e escalabilidade.

Perguntas e Respostas

1- Alguns tópicos ainda faltam ser explorados para o uso destes IEDs virtuais, tais como segurança cibernética, interoperabilidade e redundância. Os autores poderiam comentar um pouco sobre estes desafios?

O artigo ressalta que, embora os vIEDs apresentem vantagens significativas em termos de flexibilidade, escalabilidade e redução de custos, a adoção dessa tecnologia também traz desafios que precisam ser considerados para garantir a confiabilidade do sistema. Entre eles, destacam-se a segurança cibernética, a interoperabilidade e a redundância.

No que se refere à segurança cibernética, a diferença em relação aos IEDs físicos está no fato de que os dispositivos tradicionais contam com certo grau de isolamento, enquanto os vIEDs dependem fortemente de camadas de software e de redes baseadas em protocolos de TI amplamente utilizados, como TCP/IP. Essa característica amplia a superfície de ataque, exigindo medidas de defesa mais sofisticadas, como segmentação da rede, autenticação forte, monitoramento contínuo de tráfego e sistemas de detecção de intrusão adaptados aos protocolos IEC 61850. Além disso, a centralização de múltiplos vIEDs em um mesmo servidor pode criar pontos únicos de falha que, se comprometidos, afetam simultaneamente diversas funções de proteção.

A interoperabilidade é outro aspecto que precisa ser avaliado. Embora o padrão IEC 61850 ofereça um arcabouço sólido de comunicação, sua aplicação em ambientes virtualizados pode gerar dificuldades adicionais, especialmente quando envolvem soluções de diferentes fabricantes. Problemas relacionados à sincronização temporal, à modelagem de funções e à garantia de latência mínima podem comprometer a operação integrada, em especial em cenários híbridos nos quais IEDs físicos e vIEDs precisam coexistir de forma consistente.

Em relação à redundância, nos sistemas baseados em IEDs físicos ela não é obtida pela simples duplicação de hardware, mas sim pela utilização de proteções de retaguarda. Nesse esquema, determinados dispositivos assumem a função de proteção secundária de outros, de modo que, caso a proteção primária falhe, a retaguarda atua assegurando a continuidade da proteção do sistema. Essa filosofia pode ser aplicada também em ambientes virtualizados, em que a redundância pode ser alcançada pela replicação de instâncias de software em diferentes servidores e pela orquestração dessas funções. Embora essa abordagem seja mais flexível, ela

aumenta a dependência da infraestrutura de TI, das plataformas de virtualização e das redes de comunicação. Protocolos como PRP (Parallel Redundancy Protocol) e HSR (High-availability Seamless Redundancy) ajudam a garantir a continuidade da comunicação, mas permanece o desafio de implementar redundância também no nível do hipervisor e das máquinas virtuais, prevenindo falhas simultâneas que comprometam a operação.

Assim, a adoção dos vIEDs não depende apenas da comprovação de sua viabilidade técnica em termos de desempenho, mas também do avanço em soluções que assegurem níveis adequados de segurança, interoperabilidade e redundância, compatíveis com as exigências dos sistemas elétricos de potência.

2 - Há intenção de testar outras funções de proteção implementadas em IEDs virtuais depois desta experiência?

3 - Quais as recomendações e cuidados no uso das redes para esta aplicação?

Numa aplicação real numa subestação a aquisição de sinais (analogicos, digitais, comandos) ainda utilizaria Merging Units em cada para conversão analógica/digital ou haveria uma possibilidade disto tambem estar virtualizado?
No estado atual da tecnologia, a aquisição de sinais analógicos (corrente e tensão) ainda é feita por Merging Units (MUs) ou por instrument transformers não convencionais, responsáveis por converter sinais analógicos em fluxos digitais de Sampled Values (SV).

Ou seja, mesmo que a lógica de proteção e controle seja virtualizada nos vIEDs, a camada física de medição continua dependendo de hardware instalado em campo, próximo aos equipamentos de potência. Isso se deve à necessidade de interface direta com o sistema elétrico, algo que não pode ser totalmente virtualizado.

A tendência futura, entretanto, é que a virtualização avance até a borda do sistema, mas dificilmente será possível eliminar completamente as MUs, já que elas constituem o elo físico entre o mundo analógico (corrente/tensão nos barramentos) e o ambiente digital. O que pode ocorrer é uma integração mais estreita entre MUs inteligentes e plataformas de virtualização, permitindo que parte de suas funções (como filtragem, compressão ou até processamento prévio de fasores) seja migrada para o ambiente virtualizado.

A aplicação de apenas uma função de proteção num ambiente virtualizado não agrega economicamente muito ganho porque esta se trocando um IED por um computador. Mas a evolução natural do projeto sera poder incluir outras funções?

A aplicação de apenas uma função de proteção num ambiente virtualizado não agrega economicamente muito ganho porque esta se trocando um IED por

um computador. Mas a evolução natural do projeto sera poder incluir outras funções?

Considerando que os vIED são uma promessa de implementação futura, que aspectos relacionados à confiabilidade precisam ser mais investigados e aprofundados no escopo da transição doambiente baseado em hardware para os ambientes virtualizados?

Para que os vIEDs se consolidem como uma alternativa viável em aplicações reais de proteção e controle, é necessário aprofundar os estudos sobre diversos aspectos relacionados à sua confiabilidade. Diferentemente dos IEDs físicos, que contam com hardware dedicado capaz de garantir respostas determinísticas em tempo real, os vIEDs compartilham recursos de servidores com outras máquinas virtuais ou containers. Nesse contexto, torna-se essencial explorar e validar técnicas de alocação de recursos, como o CPU pinning e o Single Root I/O Virtualization (SR-IOV), de modo a assegurar baixa latência e reduzir a variabilidade nas respostas do sistema.

Outro ponto fundamental refere-se à gestão de falhas e à tolerância a erros. A confiabilidade dos vIEDs depende do desenvolvimento de arquiteturas que permitam failover automático, replicação de instâncias e recuperação rápida em caso de falhas de software, do hipervisor ou mesmo do hardware. Isso exige a validação de estratégias de redundância não apenas no nível da rede, com protocolos como PRP e HSR, mas também no nível da própria virtualização, garantindo que eventuais interrupções não comprometam a continuidade das funções de proteção.

A resiliência cibernética também deve ser considerada como parte integrante da confiabilidade. Não basta que os vIEDs atendam aos requisitos elétricos de desempenho; é igualmente necessário que resistam a tentativas de ataque e manipulação maliciosa. Para isso, mecanismos de monitoramento contínuo, segmentação de tráfego e detecção de anomalias precisam ser avaliados em cenários práticos, de forma a verificar sua eficácia em situações reais de risco.

Além disso, durante o período de transição, é esperado que sistemas híbridos, compostos simultaneamente por IEDs físicos e vIEDs, passem a operar em conjunto. Nessa condição, a confiabilidade do sistema dependerá da interoperabilidade e da coordenação entre dispositivos de naturezas distintas, o que reforça a necessidade de validação em ambientes de testes em larga escala.

Por fim, a maturidade das plataformas de virtualização é um fator determinante para o sucesso dessa transição. É imprescindível compreender como diferentes hipervisores, sistemas operacionais em tempo real e soluções de orquestração impactam a estabilidade e a confiabilidade dos vIEDs, já que vulnerabilidades ou falhas nesses componentes podem comprometer simultaneamente diversas funções de proteção.

Título - Ferramenta Automática para Modelagem de Hardware de IEDs e MUs dentro de uma Plataforma de Engenharia

Entidade(s) - ESC - ENGENHARIA DE SISTEMAS DE CONTROLE LTDA,UPE UNIVERSIDADE DE PERNAMBUCO,Sm Smart Energy Solutions LTDA
Autor(es) - Allane Sales de Menezes,Rafael Falcão de Aquino,Saulo Soares Santos,Fillipe Moraes Finco,José Raimundo Lima Júnior,Eduardo Ferreira da Silva
Resumo
A digitalização, automação e integração de sistemas viabilizam a modernização das subestações. Os IEDs e MUs são cruciais na implementação de uma operação inteligente e otimizada. Entretanto, a modelagem do hardware desses dispositivos nos projetos executivos é um processo manual, demorado e propenso a erros. Como alternativa, propõe-se uma ferramenta capaz de gerar um modelo digital completo do hardware do dispositivo a partir do seu identificador universal (código de compra), considerando como base os módulos dos fabricantes previamente registrados no banco de dados da plataforma de engenharia. A ferramenta adapta os módulos dos fabricantes ao IED ou MU especificado pelo usuário, garantindo a definição precisa dos pontos de conexão elétricos dos equipamentos. Os resultados apresentados, utilizando como exemplo um fabricante, constataram uma redução de aproximadamente 90% no tempo de atividade, comparado ao modelo anterior de trabalho.
Perguntas e Respostas

1 - os autores comentam sobre o ganho de tempo quando de utilização desta ferramenta. Voces teriam valores em termos percentuais de quanto seria esta redução no escopo total do projeto?

1 - os autores comentam sobre o ganho de tempo quando de utilização desta ferramenta. Voces teriam valores em termos percentuais de quanto seria esta redução no escopo total do projeto?
Considerando a distribuição típica interna do tempo de desenvolvimento de um projeto funcional – 30% cadastro, 10% unifilares, 30% distribuições de analógicos, 10% interfaces entradas/saídas digitais e 20% interações com existentes – e o fato de que a ferramenta automatiza o processo de cadastramento, reduzindo em aproximadamente 94,6% o tempo originalmente gasto nesta etapa, constatou-se que o tempo total de execução do projeto seja reduzido em cerca de 28,38%.
Em outras palavras, a etapa de cadastro, que antes representava 30% do esforço total, passa a representar aproximadamente 1,62% do tempo de projeto após a automação, impactando de forma significativa a duração global do processo.

O trabalho apresenta a automatização das conexões eletrica e modulos necessarios no projeto do SPSC. Como é definido os sinais que chegarão no dispositivo?
A ferramenta proposta não possui a finalidade de definir os sinais a serem associados ao IED ou MU. Sua função concentra-se na automatização da modelagem do hardware desses dispositivos, a partir do código universal disponibilizado pelo fabricante. A definição dos sinais (entradas e saídas digitais e analógicas, medições e comandos) é realizada durante o desenvolvimento do projeto funcional do Sistema de Proteção, Controle e Supervisão (SPCS), em conformidade com a aplicação específica. Nesse contexto, os requisitos de sinalização e comando variam conforme o tipo de ativo ou instalação a ser protegida

e monitorada, como transformadores, reatores, linhas de transmissão ou bancos de capacitores.

As funções de proteção e controle a serem aplicados não estão no foco do trabalho. Os autores acreditam que seria possivel automatizar isto?

As funções de proteção e controle a serem aplicados não estão no foco do trabalho. Os autores acreditam que seria possivel automatizar isto?

Os autores informam que erros na identificação de pontos de conexão dos equipamentos digitais impactam a montagem elétrica dos painéis, uma das razões da proposta apresentada. Poderiam comentar como é realizado o processo de codificação desses pontos e como é realizada a conferência dessas conexões durante os testes de aceitação dos painéis?
Após a conclusão do projeto funcional, a plataforma de engenharia gera automaticamente uma planilha contendo todos os pontos de conexão, tanto do painel quanto dos IEDs e MUs. Antes do desenvolvimento da ferramenta apresentada neste trabalho, essa planilha era conferida manualmente, e eventuais erros de cadastro só eram identificados após o projetista já ter investido considerável tempo no processo de modelagem manual dos dispositivos. Em alguns casos, tais inconsistências chegavam a impactar a etapa de montagem do painel, sendo detectadas apenas durante os Testes de Aceitação em Fábrica (TAF), quando eram realizadas as verificações das medições dos pontos de fiação.
Com a implementação da nova ferramenta, além da expressiva redução do tempo de cadastramento — e, por consequência, do tempo total de desenvolvimento do projeto executivo —, observou-se um aumento significativo na confiabilidade das planilhas de fiação. Isso se deve à diminuição substancial do índice de erros identificados no processo de conferência manual anteriormente mencionado.

Título - Confiabilidade em subestações digitais com monitoramento eficaz de redes IEC 61850
Entidade(s) - SCHWEITZER ENGINEERING LABORATORIES COMERCIAL LTDA
Autor(es) - Vinicius Vasconcellos Ferrari,Paulo Silva Lima,Gabriel Cortes Cassiano Pereira
Resumo
Com a introdução das subestações digitais no Sistema Interligado Nacional (SIN), foi necessário atualizar os procedimentos e requisitos do ONS para os sistemas de proteção dessas subestações. Novos conceitos, como Merging Units, sensores de baixa potência e barramento de processo, foram integrados aos sistemas de proteção. Isso resultou em várias mudanças nos requisitos existentes e na criação de novos, que estão incluídos na nova revisão do Submódulo 2.11. Um dos novos requisitos é a implementação obrigatória de um sistema de monitoramento das redes usadas para proteção.
Independentemente dos requisitos regulamentares, o monitoramento das redes IEC 61850 é essencial para assegurar a confiabilidade do sistema de proteção e fornecer dados para uma operação mais eficiente. Para isso, existem diferentes abordagens,

como a supervisão baseada na captura de tráfego da rede (sniffer) e o monitoramento baseado em informações disponibilizadas pelos IEDs (Intelligent Electronic Devices).

O presente trabalho foca na metodologia de monitoramento baseada em dispositivos, descrevendo sua concepção, benefícios e desafios. O conceito está fundamentado no fato de que uma parte significativa do processo de comunicação ocorre nos dispositivos finais. Dessa forma, busca-se fornecer uma compreensão mais profunda e fundamentada das razões que justificam a escolha de uma abordagem em detrimento de outras. Para tanto, apresenta-se uma análise sobre os critérios de performance estabelecidos na IEC 61850.

Na sequência, apresenta-se um modelo de sistema de monitoramento desenvolvido com base nas informações dos IEDs, visando atender e superar os requisitos estabelecidos do submódulo. Conclui-se que tal metodologia proporciona a capacidade de supervisão integral a cadeia de comunicação, abrangendo não apenas a rede, mas também, e principalmente, o processamento nas extremidades.

Perguntas e Respostas

1 - Pode -se concluir pelo trabalho que um sistEma de monitoramento hibrido, utilizado as informações dos IEDs e a captura de tráfego (sniffer) seria um método mais completo e necessário para atendimento dos requisitos dos Procedimentos de Rede do ONS?

2 - Com relação ao monitoramento da rede do sistema de proteção , além dos requisitos mínimos exigidos pelos Procedimentos de Rede do ONS , pela experiencia do autor, algum outro requisito de monitoramento poderia ser inserido como obrigatório?

No trabalho esta a tese de que basta o monitoramento com as informações dos IEDs para aplicar um sistema de monitoramento. Mas isto não atenderia aos procedimentos de rede, já que la esta previsto alertar sobre sianis na rede que não estão de acordo com o SCD estabelecido no projeto, incluindo trafegos que não fazem parte de aplicação PAC. Como seria possivel monitorar que na rede estão todos os sinais, e somente os previstos?

Este requisito exige um mecanismo adicional para detecção de mensagens não previstas.

Uma das possibilidades é a utilização de switches SDN-OT, que naturalmente inibem qualquer trafego não previsto na aplicação.

O tráfego não previsto é então redirecionado para uma porta específica dedicada à analise dos pacotes descartados.

Além desse mecanismo na rede SDN, os IED's usados no projeto possuem função de detecção e alarme de pacotes não previstos em sua interface, complementando ainda mais a solução.

Numa solução de aplicação de IEC 61850 a rede e seus dispositivos fazem parte da função de proteção. O monitoramento dos trafegos e desempenhos são importantes, e poderiam ser informados pelos Switches. Atualmente não existe uma boa modelagem na norma sobre isto, e o registro interno de um

switch não tem compromisso com milissegundos e nem com MMS para entregar os dados. Os autores acreditam que uma evolução neste sentido, de requisitos e modelagem poderia contribuir?
Entendemos que as informações fornecidas pelos switches têm caráter meramente complementar, independentemente da modelagem ou do protocolo adotado. A única forma de monitorar integralmente o processo de comunicação é por meio da observação direta no dispositivo final.

A adoção de uma modelagem padronizada para os dados de monitoramento dos IEDs certamente representaria um avanço significativo nesse sentido.

No entanto, a padronização de funções, sejam elas de proteção ou de monitoramento, não está contemplada no escopo da norma IEC 61850. Uma alternativa plausível seria o desenvolvimento de uma documentação complementar, nos moldes do guia 9-2LE, que pudesse orientar e harmonizar essas práticas.

Os autores apontam a "possibilidade de falhas no processo de monitoramento depacotes que podem gerar alarmes falsos generalizados". Esse mesmo tipo de falha não ocorre no processo de monitoramento baseado em IEDs? Por que?
O monitoramento baseado em tráfego possui uma arquitetura centralizada. Isso significa que uma falha nesse sistema pode comprometer a visibilidade de todo o ambiente de comunicação.

Por outro lado, o monitoramento distribuído, realizado diretamente nos IEDs, atribui a cada dispositivo a responsabilidade de supervisionar os dados que recebe e processa. Nesse modelo, eventuais falhas ficam restritas ao IED afetado, preservando a integridade do restante do sistema e facilitando a identificação e contenção de problemas.

Título - Análise Comparativa entre Transformadores para Instrumentos Ópticos e Convencionais em Subestações Digitais: Desafios e Perspectivas
Entidade(s) - UPE UNIVERSIDADE DE PERNAMBUCO
Autor(es) - José Raimundo Lima Júnior
Resumo
Este estudo realiza uma análise entre transformadores de corrente e potencial convencionais e ópticos, com foco na aplicação em subestações digitais. Os LPIT, por utilizarem sensores ópticos em vez de bobinas e núcleos de ferro, eliminam problemas como a saturação magnética e são mais resistentes a interferências eletromagnéticas. Além disso, a conversão direta dos sinais em valores amostrados facilita a integração ao barramento de processo definido pela norma IEC 61850, reduzindo a quantidade de cabeamento e simplificando a infraestrutura. Ainda assim, os custos de aquisição e as adaptações necessárias à infraestrutura atual são barreiras relevantes. Soma-se a isso a resistência de técnicos e engenheiros, muitas vezes motivada pela falta de familiaridade com essas tecnologias. Nesse cenário, projetos-piloto se apresentam como uma ferramenta estratégica para validar os benefícios dos LPIT em condições reais de operação, proporcionando tempo e dados para que os profissionais se adaptem gradualmente. Os recentes ajustes nos Procedimentos de Rede também contribuem para fomentar a adoção, ao

estabelecer novos requisitos para subestações digitais. Conclui-se que, apesar dos desafios técnicos, econômicos e culturais, a substituição dos transformadores convencionais por LPIT representa um caminho promissor. O avanço dessa transição dependerá não só de investimentos financeiros, mas também de políticas públicas, incentivos regulatórios e ações de capacitação que promovam a confiança nas novas tecnologias.

Perguntas e Respostas

2 - O artigo informa que em alguns casos é necessário o uso de sincronismo de temo absoluto. Pode explorar mais este tema?

Não identificamos a indicação do uso de "tempo absoluto" em nosso trabalho. Os LPIT são equipamentos para medição de correntes e tensões utilizando tecnologias de baixa potência, não necessitando de fontes de sincronismo. Por outro lado, em subestações digitais, o sincronismo de tempo é requisito importante e mandatório para o uso de SV, conforme IEC 618450.

Considerando as vantagens de não saturação podemos esperar um melhor desempenho das funções de proteção?

Obrigado pela pergunta. Certamente. Critérios conservadores para a definição de ajustes de proteção que levam em conta a condição de saturação podem ser revisados de forma a otimizar o desempenho das funções de proteção. Um exemplo é a proteção diferencial que é altamente afetada pelo desempenho dos TC.

Na opinião dos autores que desafios existem para aplicação em escala de LPIT?

Que critérios devem ser observados na especificação de um LPIT levando em conta as tecnologia disponíveis?

Os critérios para seleção dos LPIT podem ser os mesmos abordados na seleção de TC/TP convencionais. Porém, é importante ter em conta as diferenças entre as tecnologias de LPIT empregados. A depender do projeto, pode ser necessário o uso de EIT (Eletronic Instrument Transformers) com componentes eletrônicos ativos ao invés de LPIT. Estes devem ser conectados a SAMU externas, por exemplo. Em outros casos, entendendo o LPIT como elemento passivo, este pode ser conectado diretamente ao barramento de processos.

Título - Monitoramento de Barramento de Processo em Subestações Digitais: Plano de Inspeção e Testes com Múltiplos Fabricantes

Entidade(s) - Companhia de Geração e Transmissão de Energia Elétrica do Sul do Brasil - Eletrobras CGT Eletrosul,CENTRAIS ELETRICAS BRASILEIRAS SA ELETROBRAS,Autarquia Federal,Ysmart Engenharia Capacitacao e Tecnologia LTDA

Autor(es) - Mateus Alexandrino,Mateus Cruz Lunardi,Yona Lopes,Matheus Felipe Ayello Leite,Arthur Albuquerque Zopellaro Soares

Resumo

O barramento de processo (Process Bus), normatizado pela IEC 61850, requer monitoramento contínuo para garantir confiabilidade nas cadeias de proteção, pois falhas na comunicação podem comprometer a segurança operacional. O Plano de

Inspeção e Testes (PIT) desenvolvido pela Eletrobras CGT Eletrosul, baseado nas diretrizes do CIGRE Brasil (GT B5-03) foi inicialmente aplicado na subestação Itajaí sem contemplar cenários com múltiplos fabricantes. Para superar essa limitação, estabeleceu-se uma Prova de Conceito (PoC) que avaliou o desempenho do monitoramento em ambientes com um único fornecedor e em configurações heterogêneas, visando aprimorar o PIT. Os resultados demonstraram a complexidade do monitoramento em ambientes heterogêneos e evidenciaram a importância do plano de testes ser aderente também a múltiplos fabricantes. O requisito de integridade do submódulo do ONS foi o mais afetado nos testes. O caráter inédito do estudo reside na avaliação prática desses aspectos em um ambiente real e na consolidação das lições aprendidas em um PIT atualizado. Sendo assim, este trabalho oferece subsídios para futuras implementações em subestações digitais, reforçando a necessidade de padronização entre diferentes fabricantes para ampliar a confiabilidade e a resiliência dos sistemas. As conclusões apresentadas servem como referência para o setor elétrico, demonstrando o valor de protocolos normatizados e métodos híbridos de monitoramento, bem como a possibilidade de reduzir riscos e custos na adoção do barramento de processo em diferentes aplicações.

Perguntas e Respostas

1 - Pelo trabalho apresentado , foram identificados casos em que houve diferenciação nas padronizações dos diagnósticos de perda de integridade das mensagens, em IEDs de fabricantes distintos. Na opinião dos autores é um problema de interpretação da norma ou realmente há brechas na norma que permitam esta diferença ?

Existem as duas situações em momentos distintos. Algumas aplicações de enumerados referentes ao estado do sincronismo apresentam divergências em relação à norma para um dos fabricantes. Em outros, como a indicação de falha do GOOSE para determinado parâmetro, pode haver interpretações diversas sobre quais parâmetros devem ser considerados para evidenciar a falha de recepção da mensagem (tanto que um dos fabricantes deixa para o usuário escolher quais parâmetros serão considerados nesta análise).

2 - Como os autores sugerem melhoria na questão de resposta para determinados tipos de diagnósticos de perda de integridade de mensagens para diferentes fabricantes? Os Procedimentos de Rede podem ajudar na solução destes problemas , indicando uma padronização ou carece de um maior detalhamento na propria norma?

Foi avaliado tambem o aspecto de ter na mesma instalação IEDs com versões diferentes da norma? Isto pode acontecer à medida de ampliações na subestação.

Nesta PoC não foi avaliado este ponto em particular (diferentes versões de norma na mesma instalação). Mas de fato é um ponto relevante que fatalmente irá ocorrer nas instalações e pode ser alvo de trabalho futuro.

Foi avaliado tambem o aspecto de ter na mesma instalação IEDs com versões diferentes da norma? Isto pode acontecer à medida de ampliações na subestação.

Foi avaliado tambem o aspecto de ter na mesma instalação IEDs com versões diferentes da norma? Isto pode acontecer à medida de ampliações na subestação.

Considerando os testes realizados pelos autores, pode-se afirmar que o modo mais eficaz de realizar o monitoramento da rede IEC61850 deve combinar a captura de pacotes e a verificação das assianturas dos IEDs?
Os resultados apresentados indicam que a forma mais eficaz de identificar um maior número de possíveis eventos no SPCS que possam vir a impactar no desempenho dos dispositivos é de fato realizar a verificação dos pontos de sanidade internos disponíveis nos dispositivos e a captura de pacotes nas redes de comunicação.

Título - Implementação e Validação de Monitoramento de Rede para Barramento de Processo na Subestação Cerro Chato: Desafios da implementação em Anel HSR
Entidade(s) - Transmissora Aliança de Energia Elétrica S.A,Siemens Infraestrutura e Indústria LTDA,Ysmart Engenharia Capacitacao e Tecnologia LTDA,Autarquia Federal
Autor(es) - Thalisson Duarte Moreira,Arthur Albuquerque Zopellaro Soares,Yona Lopes,Arthur Augusto Pereira Cruz,Thales Gabriel Ribeiro Quintino,Matheus Felipe Ayello Leite
Resumo
A subestação Cerro Chato, instalação de 230 kV, foi equipada com uma solução de proteção de barramentos híbrida, que combina medições convencionais e comunicações digitais via Sampled Values (SV), conforme a norma IEC 61850. O barramento de processo foi implementado em um anel High-availability Seamless Redundancy (HSR), inicialmente configurado de forma isolada, sem pontos de acesso convencionais. A operação desse sistema evidenciou a necessidade de monitoramento contínuo para garantir sua integridade e desempenho. Esse informe traz os resultados da primeira homologação de um sistema de monitoramento para barramento de processo em anel HSR de uma empresa transmissora, visando a implementação na subestação de Cerro Chato. A implementação desafiadora revela a relevância da experiência prática em soluções de monitoramento para redes configuradas em um anel HSR sem interferir no funcionamento do barramento de processo. O desafio consistiu em proporcionar visibilidade detalhada da rede, preservando simultaneamente a integridade do tráfego de dados e garantindo que o monitoramento da rede em SPCS operasse de maneira eficiente e segura, mesmo em uma configuração de anel HSR. A metodologia inclui dois tipos de avaliação de latência, uma sendo a latência da rede baseada em captura, e a outra sendo a latência entre os IEDs. Os resultados obtidos mostram que o sistema de monitoramento adotado é capaz de capturar e analisar dados de comunicação em tempo real, fornecendo informações detalhadas sobre a integridade das mensagens Generic Object Oriented Substation Event (GOOSE) e SV, além de monitorar requisitos essenciais, como latência e outros parâmetros especificados pelo Operador Nacional do Sistema Elétrico (ONS) se forma muito precisa. Destacam-se a detecção de anomalias e o monitoramento preciso da latência entre os IEDs, o que

facilita uma resposta imediata a problemas que possam comprometer a proteção de barramentos.

Perguntas e Respostas

1- O trabalho pontuou pontos de atenção quando do monitoramento de uma rede HSR. Poderiam afirmar que este tipo de rede impõem maiores desafios para o monitoramento e destacar estes pontos?

Redes HSR de fato impõem maiores desafios para o monitoramento em relação a topologias convencionais. Os principais pontos de atenção são:

- Duplicação de tráfego: cada mensagem é enviada em ambos os sentidos do anel, elevando o volume de dados e a carga nos IEDs, além de precisar de mais atenção sobre os impactos do rompimento do anel quanto a latência, integridade e resiliência, por exemplo.

- Saturação de enlace: o tráfego intensivo pode saturar enlaces ou portas de equipamentos em anéis grandes.

- Latência e jitter: falhas ou rompimentos de enlace podem causar assimetrias de tempo entre mensagens, impactando a proteção. Latências podem variar bastante durante a falha, dependendo do tamanho do anel.

- Escalabilidade: em topologias pequenas o desempenho é satisfatório, mas em anéis maiores cresce o risco de perda de assinaturas devido a carga na rede.

- Intervenção: inserir pontos de captura no anel pode alterar o comportamento da rede, exigindo ferramentas específicas para HSR.

2 - Após os resultados obtidos nos testes de latência , os autores poderiam detalhar os próximos casos

O sistema de monitoramento avalia os trafegos, mas tambem acusa sinais não previstos no SCD?

Sim. Ele acusa mensagens não previstas no SCD e informa através de um status o motivo pelo qual não é prevista.

Os autores poderiam detalhar as diferenças observadas na medição da latência por inferência e por telemetria? Para os objetivos do monitoramento definido nos Procedientos de Rede qual o método mais adequado?

- Inferência (ex.: n-Cap): mede o tempo entre o IED/MU que gerou a mensagem até o ponto de captura. É útil para análises de tráfego, mas não representa a latência entre dois IEDs/MUs.

- Telemetria (ex.: n-Watch): mede a latência diretamente entre os IEDs/MUs,

refletindo a latência fim-a-fim real entre origem e destino.

Para os objetivos de monitoramento definidos nos Procedimentos de Rede, o método mais adequado é o de telemetria, pois garante uma visão fiel do comportamento da rede e da integridade das funções de proteção, enquanto a inferência pode mascarar problemas e gerar falsos positivos como foi visto nos testes.

Título - Diretrizes para Interpretação e Uso de Informações de Monitoramento em Subestações Digitais: Análise Eficiente do Barramento de Processos
Entidade(s) - CTEEP - Companhia de Transmissão de Energia Elétrica Paulista,Autarquia Federal,Ysmart Engenharia Capacitacao e Tecnologia LTDA,GRID SOLUTIONS TRANSMISSAO DE ENERGIA LTDA
Autor(es) - Pedro Minoru Sakaguchi,Matheus Felipe Ayello Leite,Arthur Albuquerque Zopellaro Soares,Yona Lopes,Alex Hideaki Takeda,Rodrigo Reviglio Weishaupt
Resumo
Este informe técnico aborda a análise e proposição de diretrizes para o monitoramento e interpretação dos alarmes em subestações digitais, com foco nos requisitos estabelecidos pelo Procedimento de Rede 2.11 do Operador Nacional do Sistema Elétrico (ONS). Considerando a crescente complexidade das redes de comunicação e a importância da rápida intervenção frente a falhas, o trabalho apresenta uma metodologia para testes realizados em uma topologia baseada na subestação de Lorena da ISA Energia Brasil, utilizando um monitor de rede específico para detectar ausência de mensagens previstas, latência e presença de mensagens não previstas nos barramentos de processo e de estação. Os casos de testes contemplam cenários reais que evidenciam os desafios na identificação e classificação dos alarmes, bem como na padronização dos registros e apresentação das informações para facilitar a tomada de decisão. Os resultados demonstram a eficácia das diretrizes propostas em aumentar a confiabilidade e a eficiência do Sistema de Proteção, Controle e Supervisão (SPCS), contribuindo para a maximização da disponibilidade do fornecimento de energia elétrica. Este trabalho destaca-se pela abordagem inédita e detalhada na interpretação dos alarmes, oferecendo uma referência técnica para aprimoramentos futuros no monitoramento de subestações digitais.
Perguntas e Respostas

1 - Quais os principais desafios enfrentados nos testes?
Os principais desafios enfrentados nos testes estão relacionados à complexidade da rede de comunicação das subestações digitais e à interpretação correta dos alarmes gerados. Dentre os principais podemos citar:
Classificação da severidade dos alarmes, essencial para priorizar ações corretivas.
Montar cenário de testes o mais próximos das condições reais encontradas na subestação.
Incluir diretrizes objetivas e fácil compreensão para o operador.

2 - Dos resultados obtidos os autores vislumbram outros requisitos para monitoramento além dos já definidos no Procedimentos de Rede?

Foi avaliado tambem o aspecto de ter na mesma instalação IEDs com versões diferentes da norma? Isto pode acontecer à medida de ampliações na subestação.
Não foi avaliada essa possibilidade neste escopo, pois o objetivo inicial dos testes foi reduzir a quantidade de variáveis que poderiam dificultar o diagnóstico e a classificação dos resultados de monitoramento. Contudo, em testes anteriores verificou-se que a presença de IEDs com versões diferentes da norma IEC 61850 pode impactar de forma distinta os requisitos estabelecidos pelo ONS. Alguns requisitos são diretamente afetados, enquanto outros permanecem inalterados. Observou-se ainda que o impacto geral é menor do que o esperado inicialmente e bastante semelhante ao efeito provocado por mudanças de firmware, o que reforça a necessidade de cuidados adicionais de validação e de testes do Monitor de Rede.

Com base nos testes realizados, os autores observaram algum requisito para o monitoramento da rede IEC61850 que poderia ser contemplado em uma futura revisão dos requisitos estabelecidos pelo Operador Nacional?
Nos testes realizados, ficou evidente que a perda de conexão com um equipamento também deve ser reportada, uma vez que métodos que não notificam essa condição podem manter status antigos e incorretos. Além disso, acreditamos que a inclusão de relatórios de status, capazes de indicar possíveis causas associadas a cada alarme, representaria um aprimoramento relevante. Outro ponto importante seria tornar obrigatório o envio desses registros de monitoramento ao centro de controle, ampliando a visibilidade e contribuindo para maior eficiência operacional.

Título - Desempenho da Proteção Diferencial de Linha em Subestações Digitais: Análise do Impacto do Barramento de Processo e Sincronismo de Tempo
Entidade(s) - Siemens Ltda,Itaipu Binacional,Siemens Infraestrutura e Indústria LTDA
Autor(es) - Jorge luis Gambini Damasceno,GUSTAVO DAVID MERELES GALEANO,Matheus Hideo Yuzawa
Resumo
À medida que a tecnologia do barramento de processo ganha espaço entre as empresas do setor elétrico, diversas questões têm sido levantadas quanto ao seu impacto nas funções de proteção. Um dos principais aspectos a serem considerados em subestações que utilizam essa tecnologia é o sincronismo dos dispositivos, que deve ser altamente preciso para evitar erros indesejáveis de medição. O sincronismo das amostras pode ter origem local (relativa) ou global (absoluta), como no caso do sinal de tempo proveniente de sistemas GNSS.
Muitos dos novos empreendimentos também incluem a proteção diferencial de linha de transmissão, um sistema que possui seu próprio mecanismo para sincronizar as medições entre os dois terminais da linha. Esse sistema opera de forma independente do sincronismo das amostras no barramento de processo da subestação e, na maioria dos casos, não requer um sincronismo global de alta precisão, utilizando apenas um mecanismo conhecido como “ping-pong”.
O objetivo deste artigo é avaliar o desempenho da proteção diferencial de linha em

conjunto com o barramento de processo e tecnologias modernas de transmissão óptica através de pacotes (MPLS-TP), considerando apenas uma fonte local para o sincronismo preciso das amostras. Dessa forma, busca-se verificar a viabilidade da utilização dessas tecnologias sem a dependência de fontes globais de sincronismo de alta precisão.

Perguntas e Respostas

1 - Quais os requisitos para que o uso de MPLS-TP tenha um comportamento determnístico e não interfira na função de proteção?

2 - O artigo informa que em alguns casos é necessário o uso de sincronismo de temo absoluto. Pode explorar mais este tema?

O sincronismo absoluto embora não necessário para o sincronismo das amostras do barramento de processo, ainda é necessário para funções como PMU e para diferenciais de linha onde o canal de telecomunicações não atender requisitos mínimos de simetria.

Os autores avaliam a aplicação de um relogio local somente na aplicação de proteção diferencial de linha, ou seria para todos os IEDs da subestação?

Se o relogio for local, depende do rollover do cristal do relogio, mas em algum momento o PTP tera a indicação de perda de precisão. Qual sera o efeito no IED?

quando se utiliza uma fonte de referência local, o sinal de Announcement do PTP será publicado com a informação de que a fonte de sincronismo é o oscilador interno (clock class: 248) e que a precisão é desconhecida (clock accuracy: Unknown) isso porque o equipamento que é a fonte do sincronismo não possui uma referência externa. Neste caso não há holdover pois não há sinal de referência externo.

O artigo informa que o custo de implantação do sincronismo relativo é reduzido, quando comparado com o custo de implantação do sincronismo via GPS. A opção pelo sincronismo relativo se justifica mesmo em subestações onde já existe um sincronismo de tempo via GNSS?

Sim, pois mesmo que já exista o GNSS na subestação o Receptor de GNSS e os elementos de rede podem não ser compatíveis com a norma IEEE1588. E mesmo no caso em que sejam compatíveis ainda existe a questão da resiliência. Com o sincronismo local, o barramento de processo não dependerá de um sinal oriundo de um equipamento que está a 20000km de distância da terra.

Título - Monitoramento da Integridade das Mensagens no Barramento de Processo: Um Estudo de Caso em uma Rede Multi-Fabricante

Entidade(s) - Ysmart Engenharia Capacitacao e Tecnologia LTDA,Autarquia Federal,Companhia de Geração e Transmissão de Energia Elétrica do Sul do Brasil - Eletrobras CGT Eletrosul,CENTRAIS ELETRICAS BRASILEIRAS SA ELETROBRAS

Autor(es) - Arthur Albuquerque Zopellaro Soares,Yona Lopes,Matheus Felipe Ayello Leite,Natalia Castro Fernandes,Adriel dos Santos Araujo,Giovanna Carvalho de Siqueira,Mateus Alexandrino

Resumo
A crescente digitalização do setor elétrico exige soluções que garantam a confiabilidade e a segurança dos Sistemas de Proteção, Controle e Supervisão (SPCS), especialmente frente aos requisitos do Submódulo 2.11 dos Procedimentos de Rede do Operador Nacional do Sistema Elétrico (ONS). Um dos principais desafios está na supervisão da integridade das mensagens em redes heterogêneas, dado que os diferentes fabricantes podem implementar as funcionalidades dos atributos dos nós lógicos LGOS e LSVS de maneira distinta, limitando abordagens convencionais baseadas no protocolo MMS. Este artigo apresenta uma contribuição técnica inédita para o monitoramento da integridade das mensagens GOOSE e SV no barramento de processo de subestações digitais IEC 61850 em ambientes com múltiplos fabricantes. Para demonstrar os desafios do monitoramento da integridade, foi desenvolvida uma Prova de Conceito (PoC) com testes práticos de perda de integridade em um ambiente contendo três fabricantes distintos, simulando aplicações reais de SPCS. O monitor de rede adotado demonstrou ser capaz de detectar de forma precisa e automatizada as alterações nos atributos das mensagens GOOSE e SV, consolidando as informações em um dashboard orientado aos requisitos do ONS. O card de integridade do monitor de rede permite visualizar fluxos íntegros e não íntegros, identificando claramente os atributos que causaram a não conformidade. Os resultados evidenciam a eficácia e inovação da abordagem proposta, que viabiliza um monitoramento padronizado, assertivo e alinhado às exigências regulatórias, mesmo em ambientes multifabricante. A experiência contribui diretamente para o fortalecimento da confiabilidade e da segurança operacional das subestações digitais brasileiras.
Perguntas e Respostas

1 - Baseado nos testes efetuados neste trabalho , que recomendações os autores podem deixar com relação aos cuidados quando do monitoramento do sistema de proteção?
2 - Considerando dos problemas identificados durante os testes, principalmente na verificação da integridade das mensagens, os autores vislumbram alguma indicação de melhoria nos requsisitos dos Procedimentos de Rede ?

1 - Baseado nos testes efetuados neste trabalho , que recomendações os autores podem deixar com relação aos cuidados quando do monitoramento do sistema de proteção?
2 - Considerando dos problemas identificados durante os testes, principalmente na verificação da integridade das mensagens, os autores vislumbram alguma indicação de melhoria nos requsisitos dos Procedimentos de Rede ?

1 - Baseado nos testes efetuados neste trabalho , que recomendações os autores podem deixar com relação aos cuidados quando do monitoramento do sistema de proteção?
2 - Considerando dos problemas identificados durante os testes, principalmente na verificação da integridade das mensagens, os autores

vislumbram alguma indicação de melhoria nos requsisitos dos Procedimentos de Rede ?

1 - Baseado nos testes efetuados neste trabalho , que recomendações os autores podem deixar com relação aos cuidados quando do monitoramento do sistema de proteção?
2 - Considerando dos problemas identificados durante os testes, principalmente na verificação da integridade das mensagens, os autores vislumbram alguma indicação de melhoria nos requsisitos dos Procedimentos de Rede ?

1 - Baseado nos testes efetuados neste trabalho , que recomendações os autores podem deixar com relação aos cuidados quando do monitoramento do sistema de proteção?
É fundamental manter atenção às atualizações de firmware dos IEDs e ao comportamento dos atributos de dados em conformidade com a IEC 61850. Embora a norma forneça descrições completas, ela também abre margem para diferentes interpretações, o que pode levar a variações de comportamento entre fabricantes ou até mesmo entre modelos distintos de um mesmo fabricante.
Recomenda-se ainda a adoção de mais de um método de monitoramento no Monitor de Rede, de forma redundante e complementar, a fim de aumentar a confiabilidade na validação das informações coletadas e assegurar um monitoramento robusto, minimizando a ocorrência de falsos positivos e falsos negativos.
O ponto central, contudo, é não perder de vista que o objetivo do monitoramento é garantir a integridade e a saúde do barramento de processo. Assim, não se deve inserir pontos de falha desnecessários ou excessivos apenas para ampliar a visibilidade. O monitoramento precisa ser eficiente e robusto, mas sem comprometer a confiabilidade intrínseca do barramento de processos.

2 - Considerando dos problemas identificados durante os testes, principalemnte na verificação da integridade das mensagens, os autores vislumbram alguma indicação de melhoria nos requsiisitos dos Procedimentos de Rede ?

Foi avaliado tambem o aspecto de ter na mesma instalação IEDs com versões diferentes da norma? Isto pode acontecer à medida de ampliações na subestação.
No escopo deste teste não foi avaliado. Contudo, em testes anteriores verificou-se que a presença de IEDs com versões diferentes da norma IEC 61850 pode impactar de forma distinta os requisitos estabelecidos pelo ONS. Ou seja, alguns requisitos são diretamente afetados, enquanto outros permanecem inalterados. Observou-se ainda que o impacto geral é menor do que o esperado inicialmente e bastante similar ao efeito provocado por mudanças de firmware, exigindo cuidados adicionais de validação e testes do Monitor de Rede.

Os autores citam no artigo as dificuldades de padronização do método de monitoramento da rede IEC61850.Poderiam detalhar um pouco mais quais são essas dificuldades?
As principais dificuldades de padronização do método de monitoramento em redes IEC 61850 estão relacionadas à própria flexibilidade da norma. Embora a norma defina modelos de dados e serviços, ela deixa margem para diferentes interpretações pelos fabricantes, o que pode resultar em variações no comportamento dos IEDs.
Outro ponto crítico é a heterogeneidade das versões da norma e das implementações de firmware, que podem impactar atributos de dados e serviços de maneira distinta, comprometendo a comparabilidade entre diferentes equipamentos. Soma-se a isso a diferença entre os métodos de monitoramento, como por captura de rede, MMS, ou híbrido.
Por fim, há desafios práticos associados à inserção de pontos de monitoramento. É necessário equilibrar a qualidade da visibilidade da rede com a qualidade do barramento de processos. Esses fatores combinados tornam a padronização mais complexa e reforçam a necessidade de um plano de testes para verificar o funcionamento dos monitores de rede.

Título - Aplicação de Processo de Engenharia Top-Down em Sistemas de Proteção, Controle e Supervisão de Subestações Digitais
Entidade(s) - Companhia de Geração e Transmissão de Energia Elétrica do Sul do Brasil - Eletrobras CGT Eletrosul,CENTRAIS ELETRICAS BRASILEIRAS SA ELETROBRAS,WEG EQUIPAMENTOS ELÉTRICOS S/A - Transformadores,Weg Equipamentos Eletricos S/A
Autor(es) - Mateus Alexandrino,Vitalcir Pietta,Adriano de Oliveira Ferreira,Bruno Alexandre Oleskowicz,Carlos de Souza Moraes Neto,Rafael Bonet Scheffer,Mateus Cruz Lunardi
Resumo
A aplicação do Barramento de Estação (SB – Station Bus) em Sistemas de Proteção, Controle e Supervisão (SPCS) de sistemas de transmissão de energia elétrica concebidos de acordo com a norma IEC 61850 é uma realidade nos sistemas de potência modernos. Cada vez mais a aplicação de Barramentos de Processo (PB – Process Bus) em SPCS com SAMU (Stand Alone Merging Units) ou Unidades de Interface de Processo (PIU – Process Interface Units) publicando fluxos de Sampled Values (SV) para uso por parte dos Dispositivos Eletrônicos Inteligentes (IED – Intelligent Electronic Devices) tem sido também realizada pelas empresas transmissoras de energia elétrica. O uso de protocolos de redundância de rede com tempo de recomposição nulo e o sincronismo dos dispositivos pela própria rede de comunicação, com uso do Protocolo de Tempo Preciso (PTP – Precision Time Protocol), estão cada vez mais presentes no SPCS. Com o avanço nas aplicações do PB e o uso de SV tornando-se mais familiar, uma das próximas etapas no avanço tecnológico dos SPCS seria o uso de LPIT (Low Power Instrument Transformers) com Merging Units (MU) ao invés de SAMU. Ambos os dispositivos podem ter estratégias similares para configuração, com a possibilidade de aplicação do conceito de configuração top-down através da definição de uma especificação escrita em formato computacional. O arquivo de Descrição da Especificação do Sistemas (SSD – System Specification Description), definido pela

norma IEC 61850-6, pode ser aplicado para automação da configuração inicial dos dispositivos do SPCS a partir dos requisitos escritos em Linguagem de descrição da Configuração do Sistema (SCL – System Configuration description Language). Este processo de automação pode reduzir o tempo de projeto do SPCS, reduzir os erros humanos na configuração dos dispositivos e garantir a padronização das soluções. O presente trabalho apresenta a aplicação do processo de engenharia top-down no desenvolvimento do SPCS referente ao retrofit da subestação Itajaí 230 /138 kV desde a concepção da especificação, desenvolvido fazendo uso dos recursos definidos pela norma IEC 61850, até a fase de Testes de Aceitação em Fábrica.

Perguntas e Respostas

1 - Quais os principais dificuldades encontradas no desenvolvimento e implantação do projeto?

2 - Os autores consideram fundamental a padronização deste tipo de projeto , desde as definições das funções lógicas ate na definição dos alarmes de supervisão?

3 - Houve necessidade de alguma alteração no projeto durante os testes de fábrica?

Durante o TAF houve a necessidade de prever a possibilidade de comando remoto para habilitação dos modos de Test, Test/Block e Simulation de maneira remota, via sistema SCADA. Na fase de projetos haviam sido previstos somente comandos locais. A estrutura de dados necessária e padronizada para atender esta demanda foi desenvolvida, implantada e validada durante o TAF.

A configuração Top-down recomenda ter uma ferramenta agnostica para ela gerar o SSD. Foi utilizada qual ferramenta, e como foi sua eficiencia para poder ajustar todos os detalhes do projeto?

Para validação do SSD foi utilizada a ferramenta SCL Manager (fabricante Kalkitech), além da realização de testes com outras ferramentas de fabricantes diversos (fabricantes de malas de testes; fabricantes de dispositivos; etc.). As ferramentas em geral apresentam boa funcionalidade para a criação da estrutura de dados em IEC 61850 mas ainda demanda um bom nível de conhecimento sobre a estrutura de dados por parte do usuário para viabilizar a preparação da especificação.

O esforço da engenharia top-down é grande, e seus beneficios são na escala de aplicação. Na visão dos autores isto será possivel a partir da SE Itajai?

Esta primeira aplicação em SPCS real servirá de base para a evolução da própria especificação, a qual está prevista para ser utilizada novamente nos empreendimentos seguintes da transmissora. O grande esforço de engenharia concentra-se, principalmente, no desenvolvimento da primeira estrutura de dados. Nos empreendimentos seguintes, a especificação desenvolvida pode (e deve) ser reutilizada para manter a padronização das instalações da transmissora.

Considerando os padrões previamente desenvolvidos pela empresa através do processo de engenharia top-down, qual o esforço necessário para adaptar

esses padrões a cada empreendimento de implantação de uma nova SE ou modernização do SPCS?

Título - Monitoramento de sistemas de automação na norma IEC 61850: Riscos, oportunidades e recomendações
Entidade(s) - Hitachi Energy Brasil LTDA,HITACHI ENERGY BRASIL LTDA.
Autor(es) - Julio Oliveira,Antonio José Guglielmi Filho
Resumo
A aplicação de redes Ethernet em sistemas de automação de subestações vem sendo cada vez mais explorada, agregando diversos serviços e funcionalidades inovadoras. Exemplo disso é a implantação do barramento de processo em subestações, onde a rede é utilizada para envio de medidas analógicas e sinais digitais provenientes dos equipamentos de campo. Uma atualização recente no Submódulo 2.11 dos Procedimentos de Rede do ONS incluiu a obrigatoriedade de instalação de um sistema de monitoramento das redes de comunicação utilizadas por sistemas de proteção, como é o caso do barramento de processo. Entre os objetivos deste sistema estão a garantia de desempenho, segurança e eficiência operacional da infraestrutura de comunicação.
Este trabalho discute, com base em experiências obtidas em empreendimentos de subestações digitais implementados nos últimos 10 anos, como um sistema de monitoramento pode contribuir com a manutenção destes projetos, ao mesmo tempo que identifica os principais problemas encontrados nestas subestações digitais e suas causas raízes para conduzir à seleção do que deve ser monitorado. Ele ainda apresenta como mitigar riscos e custos para a implementação desta supervisão, bem como sugere como a norma IEC 61850 pode agregar mais valor neste quesito em suas revisões futuras.
Perguntas e Respostas

1 - No artigo é apontado que erros de configuração das mensagens GOOSE ocorrem no comissionamento , onde são corrigidas e não mais ocorrem. No entanto , erros podem ocorrer quando de intervenções e inclusões de novas aplicações nos IEDs. Os autores concordam que também nestes casos um sistema de monitoramento poderia ajudar na correção destes problemas?
O artigo aborda que erros de tal natureza podem acontecer em quaisquer fases do projeto:: Configuração, integração, testes em fábrica, testes em campo, intervenções de manutenção e nas ampliações. O sistema de monitoramento pode ajudar de fato a encontrar estas falhas, mas seguramente não se faz necessário o uso de um artefato 24x7 com escuta/intervenção em todos os segmentos da rede para essa tarefa, e tampouco é relevante medir tempos entre mensagens que tem um comportamento conhecido cujo o mau funcionamento tem consequências que podem ser detectadas por meio de recursos já oferecidos pela norma. Soma-se a esta argumentação que a instalação deste artefato mencionado (o sistema de monitoramento) agrega um custo significativo para o sistema de monitoramento por subestação.

Ferramentas especializadas podem ser usadas para diagnosticar, documentar e certificar que o sistema de automação está funcionando como o planejado, bem como contribuir para resolver ocorrências em cada uma das fases mencionadas,

forma pontual, sem o grau de intervenção na rede que o sistema de monitoramento sugerido no sbmódulo 2.11 sugere. Alia-se a este fato o uso dos recursos já presente na norma IEC 61850 (a classe L) para tomar as informações dos IEDs e MUs de forma contínua e "on the band" que podem facilmente ser mapeadas para o sistema SCADA de forma eficiente e sem custos adicionais.

2 - Do ponto de vista dos autores, que pontos de monitoramento devem ser exigidos para uma subestação digital além dos existentes nos Procedimentos de Rede do ONS?

3- Com relação à medição da latência das mensagens os autores podem exemplificar os casos em que o sistema de monitoramento pode apresentar falsos alarmes mesmo em situações que não são problema para os IEDs envolvidos, como foi citado no trabalho?

No artigo é comentado que alem do monitoramento dos sinais podemos ter o monitoramento de autodiagnose para degradação ou comprometimento de hardware. Consideram os autores que isto deve ser parte de um monitoramento corretamente aplicado?
Sem dúvida estes dados adicionais são importantes para um cross-checking de falhas e seu rastreamento é algo relevante. Assim como a classe L da norma IEC 61850, estes sinais podem ser facilmente mapoeados para o sistema SCADA com evidências docuimentadas nas listas de eventos, alarmes e ainda comsidera-se a possibilidade de indicações gráficas na IHM da arquitetura do sistema supervisório. Estes recursos podem ser usados sem agregar mais custos uma vez que estão disponíveis nos IEDs, MUs, switches, GNSS, computadores industriais e outros componentes de um sistema de automação de subestações. Convém, portanto, usá-los.

Como esta a visão mundial na aplicação de Subestações Digitais com relação ao monitoramento?

Os autores afirmam no IT que um sistema de monitoramento pode abrir brechas de segurança para ataques cibernéticos em uma rede IEC61850. Poderiam detalhar um pouco mais ou exemplificar que tipos de vulnerabilidades podem ser criadas?
Sem dúvidas, assim como ocorre em sistemas de TI - e certamente aumentar esta brecha para uma aplicação de OT da "tríade crítica - petróleo + gás, saneamento e energia elétrica" não é uma boa ideia se pensamos na disciplina Segurança da Informação (não cibersegurança que é algo mas restrito).

Um artefato de monitoramento como o sugerido no submódulo 2.11 que utilize as técnicas de SPAN ou Probe possibilitam imediatamente a aplicação de uma técnica extremamente poderosa adotada pelos crackers: O footprint. Esta técnica permite o mapeamento da topologia de rede, suas conexões, protocolos & serviços em uso. Este é o primeiro passo para a tomada de decisão de qual técnica subsequente será usada para explorar vulnerabilidades.

Um segundo quesito que pode ser usado como um vetor de ataque é a captura de tráfego dos diversos segmentos da rede. Com este conhecimento, o ataque de man-in-the-middle pode ser explorado para algo propor algo ainda mais danoso, a injeção de mensagens não autorizadas conhecida como ataque de replay.

Terceiro aspecto: Ataque aos cabeçalhos de VLANs por meio de xploits dedicados para essa finalidade, causando problemas para a segmentação de camada 2 da rede Ethernet e potencialmente para as mensagens dos protocolos que operam nessa camada (GSE, PRP, PTP, SV, HSR). Uma vez que um sistema de monitoramento 24x7 para todos os segmentos da rede é estabelecido, os acessos para esta possibilidade são abertos.

Quarto aspecto (e provavelmente o que mais expande a superfície de ataque): Se a máquina do artefato - a estação de monitoramento, independente se é um computador ou appliance dedicado - é comprometido por uma vulnerabilidade explorada com sucesso, estando este artefato conectado aos diversos segmentos da rede um ataque de escalada de privilégios ao seu sistema operacional pode permitir um deslocamento horizontal nesta rede. Isso significa que pode-se explorar por meio do artefato comprometido os serviços dos computadores do sistema SCADA, estações de engenharia, de oscilografia e operação que estejam eventualmente conectados à topologia. A partir dai, o acesso aos IEDs e MUs estaria aberto.

Certamente o artefato de monitoramento pode ser protegido na arquitetura com diversas técnicas de cibersegurança. Entretanto isso agregará ainda mais custos e mais complexidade ao sistema de automação. E os autores aproveitam para uma provocação adcional: Nas fases de configuração, integração, testes em fábrica, testes em campo, intervenções de manutenção pu expansões da subestações, em qualquer um delas, erros na configuraçao do artefato "supostamente passivo" podem ocorrer expondo brechas de segurança. Quem ou o que "monitora o monitoramento" ?

Frente à possibilidade de abertura a vulnerabilidades apontada no artigo, os autores consideram que as medidas de proteção contra ciberataques atualmente adotadas nas subestações digitais são suficientes?

Título - Avaliação de Desempenho de Teleproteção via R-GOOSE sobre MPLS-TP: Estudo de Caso e Resultados
Entidade(s) - GENERAL ELECTRIC DO BRASIL LTDA
Autor(es) - GUILHERMME LISBOA,João Márcio Jorge,Rafael Cesar Jabor Fagundes Nogueira
Resumo
Este artigo apresenta a avaliação do desempenho da teleproteção entre subestações utilizando o protocolo R-GOOSE (Routable Generic Object-Oriented System Event) sobre infraestrutura MPLS-TP (Multiprotocol Label Switching - Transport Profile). Com base na norma IEC 61850, o R-GOOSE oferece uma

alternativa moderna às interfaces seriais legadas, como a IEEE C37.94, permitindo a comunicação de sinais críticos entre subestações com maior flexibilidade, interoperabilidade e padronização.

A crescente adoção de R-GOOSE e R-SV (Routable Sampled Values) representa uma tendência tecnológica natural, tanto pela necessidade de migrar comunicações seriais para infraestruturas baseadas em pacotes Ethernet, quanto pela iminente obsolescência de interfaces como a C37.94, que dependem de hardwares e protocolos dedicados. Nesse cenário, a aplicação de R-GOOSE e R-SV se destaca como solução convergente, compatível com os modelos digitais previstos pela IEC 61850 e adaptável a redes modernas com controle de latência e alta disponibilidade.

O ambiente de testes incluiu IEDs com suporte simultâneo a R-GOOSE e C37.94, enlaces redundantes MPLS-TP e ferramentas de monitoração com suporte à norma IEC 61850. A metodologia adotada envolveu simulações de eventos de proteção de distância e medições de latência, repetibilidade e confiabilidade das mensagens trocadas entre os terminais.

Os resultados demonstraram que o R-GOOSE apresenta desempenho técnico compatível com os requisitos de teleproteção, comportamento determinístico e ausência de perdas, mesmo durante comutação de caminhos na rede. A análise reforça o potencial do R-GOOSE como alternativa viável para aplicações de proteção entre subestações, especialmente em arquiteturas baseadas em Ethernet e sistemas de proteção centralizados ou virtualizados.

São propostas recomendações para sua adoção segura, além da expansão dos testes para R-SV, que exigirá validações adicionais relacionadas à temporização absoluta e integridade das amostras.

Perguntas e Respostas

1 - Com relação ao tempo de latÊncia, os autores podem exemplificar os valores de temos encontrados em cada arquitetura utilizada nos testes ?

Os resultados demonstraram que os tempos de transmissão do R-GOOSE sobre MPLS-TP foram equivalentes aos obtidos com a teleproteção tradicional via C37.94. Ambos permaneceram dentro dos limites estabelecidos pela IEC 61850 para esquemas de bloqueio e intertravamento. Embora o artigo não apresente valores numéricos específicos de latência, reforça-se que os atrasos ponta-a-ponta foram comparáveis e consistentemente adequados aos requisitos das aplicações de proteção

2 - Com relação aos testes de perda de um dos caminhos de transporte, em que foi usada a comutação 1+1, fi reportado que não houve perda de pacotes, mas como ficaram os tempos de latencia das mensagens?

Nos testes de perda de um dos caminhos de transporte, o mecanismo de proteção 1+1 do MPLS-TP garantiu a entrega contínua das mensagens. Não houve perda de pacotes nem degradação observada, e os tempos de latência permaneceram dentro de limites determinísticos e aceitáveis. O sistema manteve comportamento estável, com consistência de sequência e sem falhas de integridade. Mais detalhes podem ser verificados no IT GTL-1253 que detalham o recurso 1+1 Hitless Switching mencionado

Os tempos numa rede MPLS podem ser diferentes, ou seja por não ser uma rede sincrona, variar dentro de uma media?

Os testes confirmaram que o MPLS-TP, diferentemente de redes baseadas em pacotes de melhor esforço, opera com latência determinística e caminhos simétricos. Isso garante que as variações (jitter) sejam minimizadas e permaneçam dentro de limites rígidos, adequados às aplicações de proteção. Aliado ao sincronismo PTP (IEC 61850-9-3), a solução manteve estabilidade temporal em todos os cenários avaliados

É necessária a adaptação de alguma lógica interna nos IEDs para a implementação do esquema de teleproteção via R-Goose e MPLS-TP?

Título - Experiência prática de implementação de PMU com utilização do protocolo PTP para sincronização de tempo.
Entidade(s) - CTEEP - Companhia de Transmissão de Energia Elétrica Paulista,Siemens Infraestrutura e Indústria LTDA
Autor(es) - Eric Antônio Cantarutti,Wanderley Dias Xavier Filho
Resumo
O objetivo deste trabalho é apresentar a experiência prática de aplicação do protocolo Precision Time Protocol (PTP) para sincronização de tempo de alguns Phasor Measurement Unit (PMU) durante o comissionamento das Subestações Araxá, 3 Nova Ponte e Uberlândia 10 pertencentes a ISA Energia. Até então, o histórico da ISA Energia para projetos de subestações convencionais, foi a utilização de IRIG-B para o sincronismo do PMU. Estas subestações em questão, a solução de engenharia adotada para o projeto SPCS foi em process bus full digital , assim, com intuito de aproveitar a estrutura local do Global Positioning System (GPS) da rede de processo, estas foram as primeiras subestações da ISA Energia cujo sincronismo de tempo do PMU foi em PTP.
Perguntas e Respostas

1- Considerando os testes e parametrizações das switches e GPs efetuadas , para os próximos projetos , vocês já poderiam ter uma padronização destas configurações
A Isa Energia possui a área de Desenvolvimento de Proteção e Controle, cuja sigla é TMxD. Esta área em especifico tem a responsabilidade de criar documentos de padronização relacionados a lógicos, lista de pontos, configurações de supervisórios, como também, configurações de VLANs, Switches e GPS. Atualmente, temos o documento "REFERÊNCIA TÉCNICA TMxD_01_2024 – Padrão de VLAN" para ser utilizado no momento inicial do projeto, o qual explica como deve ser a padronização de VLANs e suas repectivas prioridades. Além do mais, há uma planilha com o plano de configurações de APPID, MAC Address e o PTP nos switches e GPS, que após serem preenchidas pelos fornecedores, indicam exatamente quais são as VLANs que devem ser configuradas em cada uma das portas do Switches. Sem dúvida, a experiência prática do projeto contribuiu para a construção de ambos documentos.

A pratica anterior era utilização do IRIG-B, que exige uma infraestrutura especifica de conexões e cuidados. Como os autores avaliam as vantagens da utilização da rede Ethernet local?

A utilização da rede PTP local para sincronismo da PMU foi de grande valia, pois na verdade a solução trouxe grande economia ao projeto. A princípio, para instalar as PMUs dentro da sala de comando seria necessário adquirir mais quatro IEDs(2NPOT, 1ARX3 e 1UBE10) somente para esta função, visto que, os RDPs já estavam com suas capacidades máximas atingidas e não poderiam receber mais portas de comunicação para PMU. Então, observamos que as MUs que faziam as medições de tensão de barras estavam disponíveis e conseguiam receber as portas de comunicação do PMU, porém ficavam em painéis instalados no pátio com distâncias significavas. Estas distância inviabilizava a aplicação do IRIG-B vindo da sala de comando, pois há problemas relacionados a atrasos do cabo, assim, só saberíamos se a aplicação iria funcionar com testes reais no campo durante o comissionamento. Em um primeiro momento, cogitou-se adquirir 3 extensores de GPS(Reason RT431) que seriam instalados nos painéis das MUs no campo para fazer o sincronismo em IRIG-B de forma "local". Mas como já tínhamos a MUs sincronizadas via PTP, não houve necessidade de outro sincronismo apenas para a PMU, sendo assim, descartamos a compra de pelo menos quatro IEDs e três extensores de GPS.

Os autores podem comentar qual o impacto em termos de custos resultou da adoção da sincronização temporal das PMU com PTP ao invés do IRIG-B?
Houve uma economia de pelo menos quatro IEDs para instalação das PMUs e três extensores de GPS(Reason RT431).

Título - Impacto da penetração de fontes de energias renováveis com inversores no SIN
Entidade(s) - Operador Nacional do Sistema Elétrico,Pontifícia Universidade Católica de Minas Gerais,CENTRAIS ELETRICAS BRASILEIRAS SA ELETROBRAS
Autor(es) - Denise Borges de Oliveira,Tatiana Maria Tavares de Souza Alves,Julio Cesar Marques de Lima,Pablo Humeres Flores
Resumo
O objetivo deste trabalho é descrever as principais constatações e problemas elencados no Workshop sobre o impacto das fontes com inversores nos sistemas de Proteção, Automação e Controle das instalações do SIN. Este evento foi realizado pelo Comitê de Estudos B5 de Proteção e Automação do CIGRE com apoio do ONS, em junho de 2024, no escritório do ONS, com cerca de 200 participantes, entre plateia e apresentadores. O evento contou com apresentações de fabricantes de aerogeradores (NORDEX e SIEMENS Gamesa), de representantes de usinas eólicas e solares (Sol do Cerrado-Vale S.A. e Casa dos Ventos), fabricantes de IED de proteção (SEL, HITACHI e GE), agentes de transmissão (ELETROBRÁS) e distribuição (Energisa Paraíba), representantes da EPE – Empresa de Pesquisa Energética, CEPEL - Centro de Pesquisas de Energia Elétrica, das áreas de Operação e Engenharia do ONS, e ainda das Universidades da Paraíba (UFPB), Federal do Rio de Janeiro (UFRJ) E Universidade de Brasília (UNB).
Perguntas e Respostas

A aplicação de estudos que empreguem modelos mais fidedignos dos conversores e seus controles se refere aos modelos fornecidos por cada IBR ou tambem o comportamento da soma deles?

A modelagem mais detalhada servirá para estudos específicos de cada IBR e também para estudos do comportamento da soma deles. Os modelos detalhados devem ter como objetivo representar o comportamento das IBR no sistema, como elas respondem as variações e distúrbios na rwede, de forma a permitir estudos dinâmicos do sistema mais fidedignos

Como promover o diálogo constante entre todos os envolvidos sobre os problemas citados, reunindo fabricantes, Transmissoras, Distribuidoras, agentes de Geração (IBR) e Universidades? Eventos? Procedimentos de Rede?

Quais os principais impactos tem sido sentidos na atividade de cálculo e definição de ajustes de sistemas de proteção com o crescimento das conexões de fontes baseadas em inversores?
Os impactos tem sido visto nas proteções sistêmicas, cujos ajustes são atribuição do Operador, demandando maior cuidado na definição destas funções em face das dificuldades encontradas no SIN, como por exemplo baixa inercia, que aceleram a trajetória das impedâncias e o baixo nivel de curto-circuito

Que ações estão ao alcance do Operador Nacional e dos Agentes para obter dos fabricantes dos geradores que utilizam inversores modelos mais fidedignos do comportamento desses equipamentos?
Está sendo solicitado para os novos empreendimentos a modelagem detalhada e validada em campo aos responsáveis pelas IBRs , para fornecimento do termo de liberação do empreendimento. Para os empreendimentos antigos foi efetuada a mesma solicitação por meio de providências .

Título - Avaliação de Algoritmo de Seleção de Fases Baseado em Componentes Pseudo-Incrementais Frente a Cenários Complexos de Falta em Sistemas de Transmissão Reais
Entidade(s) - Universidade Federal da Paraiba,Universidade de São Paulo,Fundação Parque Tecnológico Itaipu - Brasil,ITAIPU BINACIONAL,Itaipu Binacional
Autor(es) - Felipe Vigolvino Lopes,Raphael Leite de Andrade Reis,Moisés Junior Batista Borges Davi,Guilherme Zat,Hilton Carlos Miranda Lessa,Alfredo Javier Mezger Szostak
Resumo
Avalia-se neste trabalho o desempenho de um algoritmo inovador de seleção de fases frente a cenários reais de faltas em linhas de transmissão, considerando distúrbios com características atípicas que impõem maior complexidade à análise do curto-circuito. O algoritmo desenvolvido se baseia no conceito de grandezas pseudo-incrementais, que mescla fundamentos de análise de faltas via circuito puro de falta, porém contando com um reforço de sensibilidade em casos de desequilíbrio nas grandezas de pré-falta. No total, 9 (nove) cenários reais de curtos-circuitos ocorridos no Sistema Interligado Nacional são estudados, incluindo casos de: faltas em linhas de interligação de Inverter-Based Resources ; faltas em linhas de circuito duplo com compensação série; faltas com saturação de transformadores de corrente; faltas de alta impedância sobre vegetação com longa e curta duração; e falta trifásica com elevada componente de decaimento exponencial. Para tanto, o algoritmo de seleção

de fases idealizado foi embarcado em um Software de Análise de Registros e Fasores, permitindo a realização dos estudos propostos de forma prática, tal como realizado rotineiramente por empresas do setor elétrico. Por meio dos resultados obtidos, verifica-se que o algoritmo de seleção de fases proposto identificou corretamente os loops de falta em todos os casos avaliados, comprovando a confiabilidade das métricas empregadas na solução desenvolvida. Com isso, atesta-se a utilidade do algoritmo para estudos de casos reais de faltas em linhas de transmissão, mesmo que resultem em assinaturas atípicas de curto-circuito.
Perguntas e Respostas

1 - Que requisitos são necessários para a implementação deste algoritmo em dispositivos já existentes, como foi efetuado no exemplo mostrado?

Que requisitos são necessários para a implementação deste algoritmo em dispositivos já existentes, como foi efetuado no exemplo mostrado ?

Qual foi o criterio na escolha de casos para validação?
A escolha dos casos se baseou no nível de atipicidade e diversidade das formas de onda verificadas em cada cenário. dado que o algoritmo desenvolvido já havia sido testado e validado em casos típicos, priorizou-se a análise de cenários cujas formas de onda de tensão e corrente apresentam comportamentos diferentes do tradicional, impondo maiores dificuldades à análise do distúrbio.

Os autores realizaram algum tipo de validação do novo algoritmo para faltas de alta impedância?
Sim. Foram considerados casos de faltas em vegetação com resistências iniciais da ordem de várias centenas de ohms (aprox. 500 ohms), com longa e curta duração. Esse tipo de falta é considerada de alta impedância, e evolui ao longo do tempo no sentido de reduzir a resistência de falta em virtude da carbonização da vegetação. Os valores finais de resistência em ambos os casos foi da ordem de 100 ohms, segundo relatórios técnicos disponibilizados pelas empresas proprietárias dos ativos analisados.

Qual a viablidade da incorporação desse novo algoritmo em relés de proteção comerciais?
O algoritmo é simples e pode ser empregado em dispositivos comerciais sem grandes problemas. Dispositivos que permitam a implementação livre podem incorporar o algoritmo com poucas linhas de código, visto que o método faz uso de fasores prontamente disponíveis em equipamentos de prateleira. Outros dispositivos que possuam programação fechada careceriam de intervenção dos fabricantes no sentido de incorporar a solução. Ressalta-se que, apesar de não ter sido abordado no trabalho, o algoritmo já se encontra disponível em um RDP desenvolvido pela Itaipu Parquetec, o Registrador de Perturbações e Medição Fasorial (RPMF).

Título - Experiência da CEMIG GT na Análise de Perturbações utilizando o SIPROTEC DigitalTwin
Entidade(s) - Cemig GT

Autor(es) - Jonathan Naves Coelho,Marcos Baeta Miranda,PAULO RUBENS BENEDETTO DE CARVALHO,Victor Pereira do Carmo Neto,ANDERSON ADRIANO DIAS

Resumo

O presente trabalho tem por finalidade apresentar as experiências obtidas pela Engenharia de Proteção da Cemig GT no uso da ferramenta de gêmeos digitais para IEDs de proteção da Siemens durante as análises de perturbação. O SIPROTEC DigitalTwin é capaz de fornecer uma réplica digital em tempo real dos IEDs (Intelligent Electronic Devices) da linha SIPROTEC 5 com os mesmos algoritmos, funcionalidades e interfaces de comunicação que um dispositivo físico real.

A virtualização dos IEDs de proteção permite aprofundar no funcionamento dos algoritmos desses equipamentos durante uma ocorrência, assim como na validação das correções ou melhorias a serem implantadas nas proteções dos equipamentos. Nesse contexto, serão apresentadas três ocorrências às quais se fez o uso dos gêmeos digitais: atuação da cadeia de proteção principal de um transformador para retorno em operação após manutenção; atuação da proteção diferencial de barras durante energização normal de transformador; e a operação em tempo superior ao esperado para proteção de linha durante falha de equipamento no terminal remoto.

Conclui-se que o uso dos gêmeos digitais permite realizar modificações nos sistemas de proteção de forma mais assertiva e ágil. Contudo, entende-se que os testes realizados no ambiente virtual não excluem a necessidade dos testes nos dispositivos físicos, porque a interação dessas modificações com o hardware dos equipamentos afetados e com a estrutura de comunicação da estação não foram validadas. Porém, logrando-se êxito nos testes virtualizados, o tempo desprendido nos testes em campo tende a ser menor e com maiores chances de sucesso.

Perguntas e Respostas

1 - Quais as maiores dificuldades encontradas na utilização de gemeos digitais?

2 - Pelos resultados obtidos a CEMIG pretende fazer da utilização de gemeso digitais uma prática da empresa?

Sim. Tem-se buscado integrar a ferramenta SIPROTEC DigitalTwin na rotina do time de proteção, mas existem dificuldades. Por exemplo: não é permitido o acesso de múltiplos integrantes à plataforma. A licença permite um acesso apenas. Em adição, por se tratar de algo executado em servidores do fabricante, não é incomum a plataforma apresentar lentidão. Com relação às atividades, temos utilizado para análise de perturbações, modificação de ajustes em operação e ajustes de novos equipamentos.

Qual a avaliação que pode se fazer sobre a performance do ambiente virtualizado na resposta necessaria para sistemas de proteção (milisegundos)

Não se realizou uma avaliação desse desempenho de forma sistemática. Observa-se, no entanto, respostas semelhantes para os sinais internos dos relés de proteção.

Qual o esforço necessário para a modelagem de um IED na ferramenta virtual utilizada?

O esforço é pequeno, porém é preciso cautela. Primeiramente, não se é necessário realizar toda a parametrização do IED virtual na plataforma. A ferramenta permite

importar um ajuste pronto para o SIPROTEC DigitalTwin por meio de arquivos de extensão ".sim" que são gerados pelo próprio DIGSI 5. Assim, tendo o projeto das proteções no DIGSI 5, basta exportar no formato ".sim".

Deve-se, no entanto, definir os canais analógicos de tensão e corrente, e os canais digitais de entradas e saídas binárias. Esses canais podem ser definidos a depender do teste a ser executado, utilizando-se de arquivos de oscilografia formato COMTRADE ou não. Existem alguns pontos dessas definições dos canais que ainda não estão muito claras para nós. Por exemplo, há momentos que o gêmeo digital inverte a polaridade do canal de corrente de neutro quando se utiliza a replicação de COMTRADE. Porém, é possível verificar a oscilografia gerada pelo próprio relé virtual com a aplicada e adaptá-la se for o caso.

Dessa forma, para o caso do relé diferencial de barras, gastou-se em torno de 6 horas até as validações dos casos. Porém, uma vantagem do SIPROTEC DigitalTwin, que uma vez que o caso foi montado, ele permanecerá montado enquanto estiver presente na plataforma.

Título - Os Impactos de Inversores Grid-Forming em Proteções de Linhas de Interconexão de Fontes Renováveis
Entidade(s) - Universidade de São Paulo,Universidade Federal da Paraiba
Autor(es) - Moisés Junior Batista Borges Davi,Mário Oleskovicz,Felipe Vigolvino Lopes
Resumo
O avanço da transição energética tem impulsionado uma transformação estrutural nas redes elétricas, marcada pela crescente inserção de geradores baseados em inversores (IBRs). Nesse sentido, enquanto a grande maioria dos estudos existentes sobre os impactos de IBRs em sistemas de proteção concentra-se em inversores Grid-Following (GFL), surge um novo paradigma com os inversores Grid-Forming (GFM), que, ao operarem de forma autônoma e estabelecerem suas próprias referências de tensão e frequência, oferecem vantagens operacionais significativas, especialmente em cenários com alta penetração de fontes renováveis. Nesse contexto, o presente trabalho analisa como as características de controle das IBRs GFM influenciam funções de proteção convencionais, como a de distância (autopolarizada e com polarização cruzada), direcional baseada em impedância de sequência negativa, e seleção de fases por ângulos de corrente de sequência negativa e zero. Para isso, um sistema com topologia típica para a interconexão de IBRs GFM à rede primária (500 kV) foi modelado no software PSCAD, sendo realizadas simulações de faltas na linha de interconexão. Testes em um relé comercial validam os resultados e discussões demonstrando que os inversores GFM, assim como os GFL, exigem requisitos específicos de controle para garantir desempenho adequado das proteções tradicionais, mesmo considerando controles como o de Máquina Síncrona Virtual (VSM) que operam visando aproximar o comportamento de IBRs ao de geradores convencionais. Análises quantitativas e discussões técnicas, incluindo o esboço de trajetórias de impedância e comparadores de fase, reforçam a necessidade de padronização dos requisitos de controle para essas tecnologias. O estudo contribui para a compreensão dos desafios relacionados à proteção de sistemas com IBRs GFM, fornecendo subsídios técnicos para uma transição energética segura.

Perguntas e Respostas

1- Das conclusões obtidas no caso de IBRs Grid Forming, os autores acham que devem ser inseridos requisitos ou indicações para as filosofias de ajustes das proteções das linhas adjacentes, ou em parÂmetros de controle das IBRs?
O artigo evidencia que, embora a modernização e o emprego estratégico de determinadas funções de proteção tenham sua importância, os maiores desafios para a atuação confiável das proteções tradicionais surgem das características de controle das IBRs GFM. Enfatiza-se que, para que as funções de proteção operem corretamente em cenários com alta penetração de IBRs GFM, é fundamental a padronização de boas práticas para as estratégias de controle das IBRs, especialmente com relação à injeção de componentes de corrente reativa de sequência positiva e negativa durante faltas.

Portanto, os autores sinalizam maior importância para os requisitos nos parâmetros e estratégias de controle das IBRs, enquanto ajustes nas proteções das linhas adjacentes (por exemplo, alcances de zonas e temporizações) podem ser necessários e importantes, mas têm efeito limitado se a IBR conectada não garantir respostas que aproximem sua operação da operação de geradores convencionais (por exemplo, pela injeção de reativo de sequência positiva e negativa mediante faltas).

2 - Vocês pretendem testar o comportamento de outras funções de proteção nesta rede com os 2 tipos de controle de IBRs Grid Forming?O que esperam encontrar?

Os IBRs do tipo GFM conseguem se aproximar do comportamento dos geradores convencionais e reduzir os impactos na proteção?
As IBRs do tipo GFM conseguem, sim, emular muitos aspectos do comportamento dinâmico dos geradores síncronos convencionais, por exemplo, quanto à formação da rede, controle de frequência e tensão, e resposta dinâmica. Isso é especialmente verdadeiro para controles como o avaliado no artigo, baseados em Virtual Synchronous Machine (VSM), que buscam replicar a reação inercial e a referência da rede elétrica.

Contudo, o artigo mostra que, na atuação da proteção (ou seja, em janelas mais restritas de tempo), essa aproximação depende fortemente da estratégia empregada no controle de corrente e ainda fica restrita à limitação de corrente característica das IBRs. O controle do tipo GFM com ajuste “básico” (só sequência positiva, sem reforço de injeção reativa durante a falta) tenderá a suprimir as correntes de sequência negativa, criando situações onde proteções tradicionais (como as que dependem dessa componente) apresentam baixos percentuais de acerto.

Apenas com controles mais avançados, alinhados a normas como a IEEE Std 2800, que incluem lógica explícita para injeção de sequências adicionais de corrente durante faltas (caso do “GFM-C2” do artigo), é que o comportamento das IBRs GFM se aproxima suficientemente do de geradores convencionais, permitindo que as proteções tradicionais operem de forma mais satisfatória e minimizando os impactos típicos das fontes baseadas em inversores.

Em suma, o controle GFM tem potencial para emular o comportamento dinâmico de um gerador convencional, mas em se tratando da análise de contribuições das IBRs para faltas, são os controles de corrente que ditam o comportamento das IBRs, sendo reduzida a influência de malhas de controle mais externas como a do controle VSM.

Em suas conclusões os autores sugerem "...adaptar e padronizar os controles, mesmo para IBRs do tipo GFM, seguindo requisitos como os estabelecidos em IEEE Std 2800, 2022". De maneira prática, como essa ação pode ser implementada para os geradores já conectados ao sistema?
Os autores acreditam que tal implementação deve ser discutida diretamente com fabricantes para o levantamento de possíveis dificuldades no processo de atualização dos geradores já conectados no sistema.

Contudo, entende-se que a implementação prática dessa recomendação exige uma abordagem que envolve atualização de firmware/software dos inversores, revisão das lógicas de controle e possíveis testes de campo. De forma básica, os passos principais seriam:

- Coordenação com o operador do sistema: Toda a padronização deve ser feita em diálogo com o operador do sistema (ONS ou equivalente), que pode exigir certificações, ensaios e auditorias para garantir que os ajustes de controle não impactem outros requisitos operacionais (estabilidade de tensão e frequência);

- Atualização de firmware/lógicas de controle: Fabricantes e operadores devem providenciar atualizações de firmware ou ajustes parametrizáveis nas unidades já instaladas para adequar a resposta das IBRs ao novo requisito.

Assim, entende-se que esse processo demandará esforços da indústria e do setor regulatório.

Título - Análise de Desempenho da Proteção de Distância com Supervisão Weak-Infeed para Linhas de Interconexão de Fontes Interfaceadas por Inversores
Entidade(s) - Universidade Federal da Paraiba,Universidade de São Paulo
Autor(es) - Felipe Vigolvino Lopes,Moisés Junior Batista Borges Davi,Mário Oleskovicz
Resumo
Estuda-se neste trabalho o esquema de proteção de distância com supervisão weak-infeed (21WI), visando avaliar o seu desempenho e aprofundar o conhecimento sobre possíveis ajustes para aplicações em linhas de transmissão (LTs) de interconexão de Inverter-Based Resources (IBRs). Para tanto, realizam-se simulações no PSCAD de um modelo detalhado de IBR seguidora de rede (GFL), que contempla o esquema de Voltage Grid Support (VGS), conforme preconizado nos procedimentos de rede do Brasil. A IBR é interligada a uma rede elétrica usando uma LT de 500 kV/60 Hz, na qual são realizados os estudos de curto-circuito de interesse. Nas simulações, variam-se os locais, resistências e tipos de faltas, bem como a força da rede elétrica interligada em relação à IBR, permitindo caracterizar a influência da resposta atípica de IBRs GFL sobre a proteção de distância

convencional, especialmente quanto à influência do Phase-Locked Loop (PLLs) e do esquema VGS. Em seguida, explicam-se os princípios operacionais do esquema 21WI, ressaltando aspectos de implementação e o documento de referência onde o referido esquema foi originalmente proposto. Na sequência, avalia-se o desempenho do esquema 21WI no contexto da operação da zona 1 da proteção de distância em casos de faltas diretas internas e externas à zona protegida, bem como faltas reversas ao ponto de medição. Com isso, viabiliza-se a demonstração de desempenho do esquema 21WI e o mapeamento de recomendações de ajuste, fomentando ainda um o debate sobre potencialidades e desafios ainda existentes para esquemas de proteção aplicados em LTs próximas a IBRs.

Perguntas e Respostas

1 -O bom desempenho do esquema 21WI depende dos ajustes implementados. Os autores recomendam alguma diretriz na definição destes ajustes?

Recomendamos fortemente a realização de estudos transitórios para definição das características de operação e restrição empregadas no esquema 21WI. Ressaltamos que estudos de regime permanente não servem para esse tipo de definição, visto que não permitem a visualização das trajetórias circulares vistas na impedância estimada, que são causadas pelo efeito de infeed (decorrente de faltas com resistência elevada) combinado com variações de frequência durate o período de falta (causadas por instabilidades dos PLLs). Em posse desses estudos, as trajetórias circulares devem ser estimadas e os casos mais críticos de referência devem ser definidos, visando definir características de operação e restrição de modo a maximizar segurança e confiabilidade para as trajetórias consideradas.

2 - Pelas análises efetuadas , os autores recomendariam o uso do esquema 27WI como uma função de proteção que deveria ser obrigatória para a utilização da proteção 21 nas linhas adjacentes a IBRs?

Na comunidade de proteção, em nível mundial, já há o entendimento que o emprego de soluções menos dependentes da característica das fontes é promissor, muito embora soluções deste tipo não resolvam todos os problemas possíveis. Nesse sentido, a solução 21WI se mostra promissora. Porém, esta filosofia parte do pressuposto que a rede interligada segue sendo forte o suficiente para ter contribuições de curto-circuito maiores do que as provenientes do terminal dominado por IBRs. Assim, ao invés de sugerir uma obrigatoriedade do esquema, os autores consideram mais adequado recomendar e ativar o esquema 21WI em linhas específicas, que sejam mais afetadas pela resposta atípica de IBRs. Tal decisão seria tomada com base em estudos transitórios prévios sobre as contribuições de falta nos terminais da linha, incluindo o estudo das características transitórias dessas contribuições. Assim, a ativação do esquema 21WI seria definida tal como realizado para algumas proteções sistêmicas, que são ativadas em locais mais críticos da rede elétrica.

Com relação aos resultados que revelaram fragilidades da proteção, especialmente relacionados a situações de sobrealcance, que possibilidades podem ser desenvolvidas?

Quanto a este problema, acreditamos que o uso de zonas instantâneas reduzidas seria uma solução possível, com o risco de temporizar a eliminação de faltas mais centrais na linha protegida. Nesse caso, uma alternativa seria combinar o esquema 21WI com funcionalidades de proteção capazes de tomar decisões ainda no tempo

de reação dos controles, a exemplo de funções baseadas em transitórios. Tal tipo de combinação tem se mostrado bastante promissora, especialmente se considerados os requisitos de tempo de eliminação de curtos-circuitos.

Na implementação da função 21WI proposto no IT, como deve ser ajustada a supervisão de sobrecorrente reversa?

Título - Projeto Athena: Laboratório de Automação de Subestações para o Grid 4.0 na escola SENAI
Entidade(s) - Hitachi Energy Brasil LTDA
Autor(es) - Julio Oliveira
Resumo
Este artigo descreve uma iniciativa na área de educação em TI/TO, desde sua concepção com as devidas motivações até a implementação, junto à escola SENAI Jorge Mahfuz em São Paulo com o propósito de formar novos profissionais na era do Grid 4.0, ou atender especialistas no mercado com o desejo de ampliar seus conhecimentos sobre a jornada de transformação digital no setor elétrico. O escopo se conecta especialmente às modernas aplicações de automação de subestações com o uso da norma IEC 61850 e agregam-se às tradicionais aplicações de proteção e controle os quesitos de gestão de ativos, cibersegurança e disciplinas de TI como redes de computadores, monitoramento de equipamentos primários e arquiteturas de comunicação. Desta forma, a iniciativa se destina a preparar tais profissionais para lidar com o cenário de subestações digitais holísticas que integram diferentes serviços por meio de sua topologia de comunicação/telemetria.
Perguntas e Respostas

1 - Qual a maior dificuldade demonstrada pelos alunas no aprendizado sobre subestações digitais , que poderá levar a complementações futuras dos cursos?
O gap em disciplinas conectadas à área de TI como redes de computadores, modelos de datos e interfaces de comunicação Ethernet e seus serviços e protocolos.

O entendimento de uma subestação digital pressupõe uma trilha de construção de conhecimento, iniciando em conceitos basicos de modelo de dados, redes Ethernet, protocolos e assim por diante. Como isto esta mapeado no projeto?
Há duas abordagens dentro do projeto Athena para este quesito, a saber:
- Da empresa conveniada (Hitachi): Há uma trilha de certificação para os funcionários chamada "Hitachi Budokan" que se divide em níveis Foundation, Intermediate, Advanced e Expert. Os conhecimentos básicos são mapeados dentro do nível Foundation que remetem justamente ao alicerce para a base de entendimento de modelos de dados, redes, sistemas de potência, proteçãoe controle e sistemas de automação. No nível Expert é experado que o profissional esteja capacitado a criar aplicações complexas aplicando todos estes conceitos integrados.
- SENAI: Como uma escola com reconhecida qualidade em sua didática, o SENAI modelou cursos básicos da norma IEC 61850 e suas características, proteção e controle e sistemas elétricos, além de uma pós-gradiução (inicialmente) focada em

proteção e controle para os modernos sistemas de automação de subestações em um programa que oferece um entendimento desde conceitos fundamentais até técnicas mais avançadas.

Em ambos os casos, esta estratégia ainda está em construção.

Qual o formato dos cursos oferecidos? Existem disciplinas oferecidas em regime remoto/EAD ou somente presencial?
No caso da conveniada (Hitachi): A formação do "Hitachi Budokan" está disponível apenas para os funcionários, alguns
cursos EAD e outros somente presenciais. Há também treinamentos similares ministrados para clientes.
No caso do SENAI: Há uma ementa defininda para a pós-graduação de proteção e controle, presencial apenas. Inclui disciplinas de arquiteturas de comunicação, sistemas de potência, seletividade de proteção, cálcuolo de curto-circuito e sistemas supervisórios.

Título - Modernização de Currículo de Engenharia Elétrica – Estudo de Caso da Universidade Federal Fluminense
Entidade(s) - Autarquia Federal
Autor(es) - Andre Abel Augusto,Yona Lopes,Felipe Sass
Resumo
Os currículos de Engenharia estão em acelerado processo de reformulação, orientados tanto por resoluções oficiais (como a Resolução CNE/CES nº 7/2018) quanto pelas novas Diretrizes Curriculares de Engenharia, que enfatizam competências, flexibilidade e forte articulação entre teoria e prática. Neste cenário, a formação em Engenharia Elétrica precisa acompanhar as demandas do setor elétrico, marcado pela transição energética, digitalização e crescente automação dos sistemas de potência. O presente informe técnico traz como contribuição técnica a proposta curricular desenvolvida pela Universidade Federal Fluminense (UFF), inspirada no framework CDIO e focada em projetos aplicados na prática, soft skills e formação multidisciplinar. Essa nova estrutura valoriza a formação generalista, permitindo que o discente aprofunde conhecimentos em sistemas de energia elétrica, automação ou eletricidade industrial, atendendo às competências demandadas pela indústria e pelas organizações governamentais e profissionais. Os resultados iniciais, após dois semestres de vigência, indicam maior engajamento discente, bem como melhor adequação às necessidades do mercado, que tem exigido profissionais capazes de lidar com geração distribuída, IEC61850, medição fasorial e outras tecnologias avançadas. A proposta curricular da UFF destaca-se, portanto, como uma experiência inovadora e potencialmente replicável em outras instituições, oferecendo subsídios para a formação de engenheiros elétricos mais completos, preparados para os desafios futuros do setor.
Perguntas e Respostas

1 - Qual a visão do autor sobre a criação de faculdades de engenharia com subáreas da Engenharia Elétrica, como por exemplo, Engenharia de Energias Renováveis?
A quantidade de conceitos acumulados no campo de conhecimento da Eng. Elétrica aumentou muito rapidamente nos últimos 20 anos, com processos alavancados por

novas fontes de energia, transição digital, novas tecnologias de informação e comunicação, e aprendizado de máquina. Ao considerarmos a redução da carga horária dos cursos de graduação, percebe-se uma demanda por especialização nos cursos de graduação, para ser possível desenvolver durante a formação todas as habilidades essenciais aos profissionais do futuro. A criação de cursos especializados ou percursos formativos são soluções possíveis para este problema, como o currículo atual da UFF propõe.

Relatórios de tendências mercadológicas (GETI Report, WEF Future of Jobs) e de estágio dos estudantes; a análise de cursos de graduação no exterior que recebem nossos estudantes; e o aumento considerável nos trabalhos de conclusão de curso relacionados à área observado nos últimos anos apontam, na visão do autor, para a necessidade de uma formação específica para Engenharia de Energias Renováveis.

Como poderia ser uma maior iteração com a industria, especialmente aquelas relacionadas ao sistema de potencia, para apontar uma formação que contribua ainda mais para o desenolvimento tecnologico da área?
A participação institucional das empresas que compõem o mercado de sistemas de potência nas atividades de pesquisa, ensino e extensão dos IES aumenta a iteração entre estes agentes. Um exemplo seria a aplicação de cursos de capacitação e nivelamento de profissionais dentro do mercado de trabalho, com participação de alunos de graduação e pós-graduação dos IES. Outro exemplo é a aplicação de projetos de extensão com a resolução de problemas e desafios das empresas como uma atividade de aprendizado baseado em problemas para alunos de graduação. Outra ação importante e que teve sucesso na instituição foram ações de melhoria da infraestrutura de salas e laboratórios de ensino, que viabilizou inclusive a proposta de formação em automação e controle apresentada no artigo. A participação das indústrias em eventos estudantis (como as semanas de engenharia) são um momento importante para estabelecer essa interação.

Considerando o rápido avanço das tecnologias na área de proteção, controle e automação e as dificuldads das unversidads em acompanhar esse avanço e as demandas do mercado, existe alguma abertura ou flexibilidade, talvez no futuro, para oferecer novas disciplinas de caráter optativo utilizando profissonais do mercado?
A oferta de disciplinas em carácter optativo ministradas integralmente por profissionais da indústria, embora louvável e recomendável(especialmente no último ano do curso), pode esbarrar em aspectos legais, exigindo um exame cuidadoso quanto à forma. Por outro lado, a realização de ações de extensão como oficinas e minicursos, cursos de aperfeiçoamento, participação em projetos finais de disciplinas/curso ou a constituição de disciplinas de seminário seriam formas alternativas de viabilizar essa participação da indústria.

Título - Método de Desenvolvimento e Métricas de Avaliação de treinamentos para profissionais e estudantes das áreas de proteção, controle e automação com enfoque em Subestações Digitais com implementação de barramento de processo
Entidade(s) - GRID SOLUTIONS TRANSMISSAO DE ENERGIA LTDA,Grid Solutions Transmissão de Energia S/A

Autor(es) - Annelise Anderson Bittencourt,Luiza Pio Costa da Silva,Antonio Henrique Cordeiro Paiva,CARLOS ALBERTO VILLEGAS GUERRERO,Rodrigo Reviglio Weishaupt

Resumo

O trabalho técnico tem como objetivo principal compartilhar a experiência da GE Vernova na estruturação de treinamentos com foco na aplicação das novas tecnologias de subestações digitais. A iniciativa visa capacitar equipes técnicas de diversas áreas da empresa e promover a transferência de conhecimento para instituições de ensino superior, incentivando a adoção de um novo mindset.

Na etapa de reestruturação dos treinamentos internos da GE Vernova observou-se a necessidade de desenvolvimento de ferramentas para apoiar a capacitação de equipes aproveitando a etapa de pré-testes e testes de aceitação em fábrica.

Como resultado do estudo para elaboração e aplicação dos treinamentos, assim como o desenvolvimentos de ferramentas para suportar o processo, será apresentado o framework com definição de métricas de avaliação dos mesmos, como a otimização do desempenho das etapas de projeto e implementação de uma subestação digital após a capacitação da equipe técnica da empresa, redução de tempo e maior abrangência de situações de testes nas etapas de ensaios de aceitação de fábrica e ensaios de comissionamento.

Os resultados da avaliação dos treinamentos utilizando o método de avaliação proposto pelo modelo de framework Kirkpatrick foram aplicados em treinamentos de equipes técnicas da GE Vernova e em docentes/discentes de universidades. Com os procedimentos e frameworks definidos e atualizados, esta proposta de treinamento e avaliação busca alinhar profissionais atuais e futuros às transformações tecnológicas em curso.

Perguntas e Respostas

1 - Qual a maior dificultada na aplicação do modelo de treinamento e de avaliação proposto pela GEVERNOVA?

2 - Com o modelo de avaliação de treinamento aplicado houve alguma necessidade de reavaliação ou melhorias no modelo de treinamento aplicado?

Com base na aplicação de um modelo estruturado de avaliação, os autores identificaram a necessidade de adaptações para atender públicos com diferentes níveis de familiaridade prévia com os temas abordados. Como resultado, foram propostas melhorias na ementa, nas avaliações e na duração do treinamento, culminando na definição de dois níveis distintos:

- Nível 1, com conteúdo introdutório e avaliações mais básicas, voltado a participantes com pouca ou nenhuma experiência prévia;
- Nível 2, com conteúdo técnico mais aprofundado e avaliações mais complexas, direcionado a profissionais com maior vivência no tema.

Essa diferenciação visa aumentar a efetividade do processo de capacitação e garantir que todos os participantes, independentemente de sua bagagem técnica inicial, possam absorver os conceitos fundamentais da digitalização em sistemas de proteção.

Os resultados tem sido apresentados para as empresas que solicitam treinamentos para motivar ações e estrategias para melhoria da efetividade dos cursos?
O modelo de treinamento apresentado neste artigo, com foco em barramento de processo, ainda não havia sido aplicado em empresas do setor elétrico até o momento da elaboração desta resposta. Sua primeira implementação ocorrerá no treinamento previsto no âmbito do projeto de Retrofit/Digitalização Eletrobrás/Chesf, denominado PDIG-1, no qual a GE Vernova é responsável pela digitalização da subestação Teresina II e das subestações remotas associadas.

O programa de treinamento apresentado no artigo trata exclusivamente dos temas relacinados à autmação da subestações. Existe algum motivo porque ao menos um tópico sobre fundamentos de sistemas de proteção não foi incluído neste programa?
Um dos motivos para essa abordagem é a premissa de que o público-alvo do treinamento já possui conhecimento básico e fundamental sobre sistemas de proteção. Além disso, busca-se evidenciar que a principal inovação trazida pela digitalização dos sistemas de proteção não está nos algoritmos ou nas funções de proteção em si, mas sim na forma como os dados são adquiridos, transmitidos e processados por meio do barramento de processo.

Título - Digital Twin : A Revolução na Manutenção da Proteção do Sistema Elétrico
Entidade(s) - PSI ENERGY SOLUÇÃO EM AUTOMAÇÃO DE ENERGIA LTDA
Autor(es) - Alvaro Inacio Ferreira Neto,Guilherme Maurício Bardocha Rezende,Marcos Henrique Figueiredo Cruz Horta Fonseca
Resumo
Com a rápida expansão do sistema elétrico brasileiro, impulsionada pela adoção de fontes renováveis, pela implementação de unidades conversoras via HDVC (High Voltage Direct Current) e pela incorporação de novas Pequenas Centrais Hidrelétricas (PCHs), surgem alterações significativas nas características do sistema elétrico. A redução da inércia, a presença de configurações obsoletas e falhas originadas durante os processos de comissionamento evidenciam a necessidade da reavaliação das proteções do sistema. Neste contexto, o estudo de caso apresentado utilizou a ferramenta Digital Twin, que permitiu a criação de uma réplica digital precisa do IED (Intelligent Electronic Devices) associado a uma linha de transmissão previamente diagnosticada com falhas operacionais. Por meio dessa abordagem, tornou-se viável a realização da manutenção e a verificação dos ajustes de maneira desacoplada do sistema, assegurando maior segurança e eficiência nos testes. A tecnologia demonstrou alta efetividade em diferentes aplicações, como a prevenção de intervenções diretas no sistema elétrico, a eliminação da necessidade de malas de teste para simulações e a exigência de IEDs sobressalentes. A utilização do Digital Twin viabiliza uma manutenção mais rápida e confiável, ajudando a aprimorar a eficiência da rede elétrica.
Perguntas e Respostas

1 - A partir desta experiencia o uso de digital twin será um uso padrão para solucionar problemas de ajustes e lógicas de proteção?
Na manutenção, sempre que forem observadas atuações incorretas das proteções, o uso do Digital Twin passa a configurar-se como prática padrão para análise e

correção do sistema de proteção, bem como para identificação de oportunidades de melhoria. Em redes elétricas em constante modificação, a criação de modelos computacionais detalhados, capazes de reproduzir formas de onda reais e gerar arquivos COMTRADE, permite simulações avançadas e avaliação precisa do desempenho dos dispositivos. Essa abordagem favorece a manutenção preditiva, pois antecipa cenários críticos, identifica fragilidades operacionais e viabiliza ajustes de maneira segura e rastreável. Dessa forma, o Digital Twin consolida-se como ferramenta estratégica para elevar a confiabilidade, a seletividade e a continuidade do fornecimento em sistemas de proteção complexos.

2 - qual uma estimativa de ganho no tempo gasto numa manutenção utilizando Digital Twin comparando com o uso de injeção de sinal em um IED sobressalente?

A estimativa de ganho com o uso do Digital Twin não se restringe apenas à redução do tempo de manutenção, mas também ao aumento significativo da disponibilidade operacional. Diferentemente do método tradicional, que depende de IEDs sobressalentes nem sempre disponíveis na mesma subestação, o ambiente digital permite realizar testes remotos sem restrições geográficas. Além disso, elimina a necessidade de espaço físico dedicado, malas de teste e deslocamentos de equipe, ampliando a flexibilidade e a eficiência dos procedimentos. Outra vantagem é a possibilidade de utilizar firmwares e modelos virtuais para simulação, evitando o estresse mecânico e elétrico dos equipamentos reais. Dessa forma, o Digital Twin oferece ganhos expressivos em agilidade, confiabilidade e rastreabilidade nos processos de manutenção, representando uma evolução frente ao uso exclusivo de injeção de sinal em IEDs físicos.

Cual a visão dos autores de utilizar Digital Twin como procedimento de validação de logicas e ajustes da proteção?

O uso do Digital Twin como procedimento de validação de lógicas e ajustes de proteção é de que se trata de uma ferramenta estratégica, desde que inserida em métodos e procedimentos bem estruturados. Embora não represente, por si só, uma solução milagrosa, o gêmeo digital possibilita reduzir drasticamente a necessidade de acessórios físicos para testes e permite examinar de forma minuciosa qualquer lógica implementada nos IEDs. Nesse contexto, torna-se plausível considerá-lo tão robusto quanto os testes de aceitação em fábrica (TAF), com a vantagem de replicar fielmente o ambiente real e assegurar a rastreabilidade das alterações. Além disso, a garantia de que se está operando sobre uma réplica idêntica do sistema confere confiabilidade às soluções validadas virtualmente, aumentando a segurança e a previsibilidade dos resultados em campo. Dessa forma, o Digital Twin consolida-se como elemento central no processo de validação e aperfeiçoamento dos esquemas de proteção.

Cual a visão dos autores de utilizar Digital Twin como procedimento de validação de logicas e ajustes da proteção?

Cual a visão dos autores de utilizar Digital Twin como procedimento de validação de logicas e ajustes da proteção?

4.0 – Constatações

Testes apresentados mostraram que o GOOSE roteável (R-GOOSE) é robusto e viável para utilização em esquemas de teleproteção, com recursos adicionais de flexibilidade e rastreabilidade.
Testes apresentados mostraram que o GOOSE roteável (R-GOOSE) é robusto e viável para utilização em esquemas de teleproteção, com recursos adicionais de flexibilidade e rastreabilidade.
As proteções virtuais têm como vantagens a redução de custo, a flexibilidade para implantação de novas lógicas, a facilidade para manutenção remota, a escalabilidade e maior segurança cibernética, porém ainda se encontra em fase de testes e desenvolvimentos para sua aplicação em larga escala.
As proteções virtuais têm como vantagens a redução de custo, a flexibilidade para implantação de novas lógicas, a facilidade para manutenção remota, a escalabilidade e maior segurança cibernética, porém ainda se encontra em fase de testes e desenvolvimentos para sua aplicação em larga escala.
Os sistemas de proteção virtualizadas podem ser implementadas em containers ou VM, cada um deles apresenta suas vantagens e desafios. Ainda foi apresentada uma ferramenta para testes durante comissionamentos e manutenção, podendo ser utilizadas um hardware dedicado ou equipamento virtual.
Os sistemas de proteção virtualizadas podem ser implementadas em containers ou VM, cada um deles apresenta suas vantagens e desafios. Ainda foi apresentada uma ferramenta para testes durante comissionamentos e manutenção, podendo ser utilizadas um hardware dedicado ou equipamento virtual.
Sistema de monitoramento visa verificar todo o sistema de proteção, e foi consenso da necessidade de sua utilização nas subestações digitais, porém ainda há discussões de como estes sistemas devem ser implementados.
Sistema de monitoramento visa verificar todo o sistema de proteção, e foi consenso da necessidade de sua utilização nas subestações digitais, porém ainda há discussões de como estes sistemas devem ser implementados.
Foi ressaltado que utilização apenas das informações provenientes dos IEDs podem não ser suficientes, considerando que nem todos os IEDs possuem as funções ou são projetados para fornecer as informações necessárias para monitoramento.
Foi ressaltado que utilização apenas das informações provenientes dos IEDs podem não ser suficientes, considerando que nem todos os IEDs possuem as funções ou são projetados para fornecer as informações necessárias para monitoramento.
Foi destacada a necessidade de Planos de teste para validar o sistema de monitoramento para cenários de múltiplos fabricantes, o que também faz parte do escopo de uma brochura do grupo de trabalho GT B5.03 do Cigre.
Foi destacada a necessidade de Planos de teste para validar o sistema de monitoramento para cenários de múltiplos fabricantes, o que também faz parte do escopo de uma brochura do grupo de trabalho GT B5.03 do Cigre.
Foi destacada a recomendação para que os fabricantes de IEDs caminhem para a padronização dos atributos e parâmetros necessários para implementação dos sistemas de monitoramento.
Foi destacada a recomendação para que os fabricantes de IEDs caminhem para a padronização dos atributos e parâmetros necessários para implementação dos sistemas de monitoramento.

A estratégia de investir em subestações digitais também é uma realidade na Distribuição, e o desempenho mostrado nas subestações digitais em operação confirmam ser uma diretriz acertada. É vislumbrado que a centralização e virtualização será um caminho adotado num futuro próximo na Distribuição.
A estratégia de investir em subestações digitais também é uma realidade na Distribuição, e o desempenho mostrado nas subestações digitais em operação confirmam ser uma diretriz acertada. É vislumbrado que a centralização e virtualização será um caminho adotado num futuro próximo na Distribuição.
O processo de engenharia TOP DOWN requer treinamento, além da necessidade de adaptações em alguns modelos de dados, e de adequações nas ferramentas para utilização deste processo de forma a permitir sua utilização por parte das Transmissoras.
O processo de engenharia TOP DOWN requer treinamento, além da necessidade de adaptações em alguns modelos de dados, e de adequações nas ferramentas para utilização deste processo de forma a permitir sua utilização por parte das Transmissoras.
Uma das vantagens do Digital Twin é poder reproduzir o sistema de proteção e suas falhas, possibilitando soluções sem a necessidade de uma manutenção real em campo para investigação, podendo também ser usado para reduzir o tempo de comissionamento, antecipando etapas de testes.
Uma das vantagens do Digital Twin é poder reproduzir o sistema de proteção e suas falhas, possibilitando soluções sem a necessidade de uma manutenção real em campo para investigação, podendo também ser usado para reduzir o tempo de comissionamento, antecipando etapas de testes.
O uso de LPIT proporciona aplicações combinadas de TC e TP, redução de OPEX e de obras civis, dos riscos de explosão e aplicação direta da IEC61850. Por outro lado, a aplicação desta tecnologia, pronta para uso, traz novos desafios, como necessidade de treinamento os custos envolvidos.
O uso de LPIT proporciona aplicações combinadas de TC e TP, redução de OPEX e de obras civis, dos riscos de explosão e aplicação direta da IEC61850. Por outro lado, a aplicação desta tecnologia, pronta para uso, traz novos desafios, como necessidade de treinamento os custos envolvidos.
Foram apresentadas as conclusões obtidas pelo WGB5.69, com recomendações para implementação de barramentos de processo nas subestações, e sinalizado que ainda existe uma barreira de custo envolvido na utilização desta tecnologia, que envolve implementação , treinamento e equipamentos envolvidos.
Foram apresentadas as conclusões obtidas pelo WGB5.69, com recomendações para implementação de barramentos de processo nas subestações, e sinalizado que ainda existe uma barreira de custo envolvido na utilização desta tecnologia, que envolve implementação , treinamento e equipamentos envolvidos.
Foram elencados os impactos das fontes baseadas em inversores nos sistemas de proteção, com destaque das fontes tipo GRID FORMING, mostrando simulações de diversos tipos de falhas nas linhas de conexão destas fontes e utilizando diferentes estratégias de controle.
Foram elencados os impactos das fontes baseadas em inversores nos sistemas de proteção, com destaque das fontes tipo GRID FORMING, mostrando simulações de diversos tipos de falhas nas linhas de conexão destas fontes e utilizando diferentes estratégias de controle.

Foi constata a necessidade de envidar esforços para aprimoramento das funções de proteção das linhas de conexão das IBRs, sendo apresentadas propostas de novos algoritmos e funções de proteção mais aprimoradas.
Foi constata a necessidade de envidar esforços para aprimoramento das funções de proteção das linhas de conexão das IBRs, sendo apresentadas propostas de novos algoritmos e funções de proteção mais aprimoradas.
É primordial o diálogo contínuo entre todos os agentes impactados com os problemas das IBRs, tais como fabricantes de turbinas eólicas e IEDs, Transmissoras, Distribuidoras, centros de pesquisa, universidades e ONS, em busca de uma operação segura e confiável do sistema.
É primordial o diálogo contínuo entre todos os agentes impactados com os problemas das IBRs, tais como fabricantes de turbinas eólicas e IEDs, Transmissoras, Distribuidoras, centros de pesquisa, universidades e ONS, em busca de uma operação segura e confiável do sistema.
Os sistemas especiais de proteção, diante da complexidade dos sistemas com alta concentração de fontes com inversores e do envelhecimento da rede, se tornam cada vez mais necessários.
Os sistemas especiais de proteção, diante da complexidade dos sistemas com alta concentração de fontes com inversores e do envelhecimento da rede, se tornam cada vez mais necessários.
Os SEPs são tema de trabalho conjunto dos grupos de estudo C2B5.46 do CIGRE.
Os SEPs são tema de trabalho conjunto dos grupos de estudo C2B5.46 do CIGRE.
Como exemplo, foi apresentado o SEP implementado na interligação Norte-Sudeste, que é o maior esquema deste tipo implantado no país, envolvendo 33 subestações distinta, e que traz como inovação , comandos de rampa de potência nos bipolos da SE Xingu .
Como exemplo, foi apresentado o SEP implementado na interligação Norte-Sudeste, que é o maior esquema deste tipo implantado no país, envolvendo 33 subestações distinta, e que traz como inovação , comandos de rampa de potência nos bipolos da SE Xingu .
Houve testes em simulador digital em tempo real para definição dos ajustes de proteções sistêmicas, tais como a função de Disparo por Oscilação de Potência, e a avaliação de seu desempenho.
Houve testes em simulador digital em tempo real para definição dos ajustes de proteções sistêmicas, tais como a função de Disparo por Oscilação de Potência, e a avaliação de seu desempenho.
O tronco de interligação em 230 kV do Acre/Rondônia possui sazonalidade dos fluxos, proximidade de elo de corrente contínua e onde a implementação das proteções sistêmicas foi efetuada com os recursos existentes e uso de filosofias inovadoras.
O tronco de interligação em 230 kV do Acre/Rondônia possui sazonalidade dos fluxos, proximidade de elo de corrente contínua e onde a implementação das proteções sistêmicas foi efetuada com os recursos existentes e uso de filosofias inovadoras.
Foi proposto um novo método para cômputo da frequencia (geometria diferencial), visto que a complexidade do sistema elétrico atual , com diversas fontes baseadas em inversores impõem dificuldades para os métodos usualmente aplicados.
Foi proposto um novo método para cômputo da frequencia (geometria diferencial), visto que a complexidade do sistema elétrico atual , com diversas fontes baseadas em inversores impõem dificuldades para os métodos usualmente aplicados.

Foram apresentados os testes aplicados ao cômputo da frequencia através da geometria diferencial, cujos resultados mostraram que este método foi bastante consistente.
Foram apresentados os testes aplicados ao cômputo da frequencia através da geometria diferencial, cujos resultados mostraram que este método foi bastante consistente.
A crescente utilização de reatores a núcleo de ar, foi apresentada uma função de proteção para falhas entre espiras, baseada em supervisão de impedância de sequência negativa e grandeza de operação de sequência zero, e mostrada sua eficiência tendo em vista testes e simulações realizadas.
A crescente utilização de reatores a núcleo de ar, foi apresentada uma função de proteção para falhas entre espiras, baseada em supervisão de impedância de sequência negativa e grandeza de operação de sequência zero, e mostrada sua eficiência tendo em vista testes e simulações realizadas.
Foram apresentados testes efetuados em Merging Unit considerando as informações injetadas (SV) similares às provenientes de LPIT, onde foram monitoradas as respostas dos SV, verificando precisão, erro, perda de pacotes, tempo de processamento, entre outros, comprovando as vantagens no uso de LPITs.
Foram apresentados testes efetuados em Merging Unit considerando as informações injetadas (SV) similares às provenientes de LPIT, onde foram monitoradas as respostas dos SV, verificando precisão, erro, perda de pacotes, tempo de processamento, entre outros, comprovando as vantagens no uso de LPITs.
A análise comparativa mostrou que a solução convencional para proteção diferencial de barramentos apresentou vantagens relacionadas a custo, tempo de resposta e confiabilidade, e a solução digital tem maior velocidade para implantação, interoperabilidade e menos espaço físico.
A análise comparativa mostrou que a solução convencional para proteção diferencial de barramentos apresentou vantagens relacionadas a custo, tempo de resposta e confiabilidade, e a solução digital tem maior velocidade para implantação, interoperabilidade e menos espaço físico.
A definição de projeto entre uso de proteção diferencial de barramentos com solução convencional ou uma solução usando o barramento de processos exige análise caso a caso.
A definição de projeto entre uso de proteção diferencial de barramentos com solução convencional ou uma solução usando o barramento de processos exige análise caso a caso.
Ensaios em RTDS são uma ferramenta fundamental para verificação de desempenho dos sistemas de proteção.
Ensaios em RTDS são uma ferramenta fundamental para verificação de desempenho dos sistemas de proteção.
Para as modernizações das proteções da UHE Itaipu, das barras, linhas e unidades geradoras, foram definidos cerca de 4000 casos com diferentes cenários, trazendo como inovação a aplicação deste tipo de testes em unidades geradoras de grande porte.
Para as modernizações das proteções da UHE Itaipu, das barras, linhas e unidades geradoras, foram definidos cerca de 4000 casos com diferentes cenários, trazendo como inovação a aplicação deste tipo de testes em unidades geradoras de grande porte.

Os ensaios em RTDS para as modernizações das proteções da UHE Itaipu, utilizaram 12 amplificadores, 51 canais de corrente e 27 canais de tensão, além de modelos dinâmicos de reguladores, estabilizadores dos geradores.
Os ensaios em RTDS para as modernizações das proteções da UHE Itaipu, utilizaram 12 amplificadores, 51 canais de corrente e 27 canais de tensão, além de modelos dinâmicos de reguladores, estabilizadores dos geradores.
Ainda relacionado às unidades geradoras , foi apresentado o resultado do Grupo de trabalho B5.04 do CIGRE sobre testes e ensaios de proteções de geradores.
Ainda relacionado às unidades geradoras , foi apresentado o resultado do Grupo de trabalho B5.04 do CIGRE sobre testes e ensaios de proteções de geradores.
O GT B5.04 proporcionou um banco de dados de oscilografias que representam falhas no sistema e geradores, energização, perda de excitação, perda de sincronismo e outras condições das UG, usando modelos de geradores típicos.
O GT B5.04 proporcionou um banco de dados de oscilografias que representam falhas no sistema e geradores, energização, perda de excitação, perda de sincronismo e outras condições das UG, usando modelos de geradores típicos.
Foi mostrado um dispositivo FACTS (M-SSSC) para controle de fluxo de potência, considerando a presença das IBRs e a entrada dos DATACENTERS, sobrecarregando as linhas de transmissão.
Foi mostrado um dispositivo FACTS (M-SSSC) para controle de fluxo de potência, considerando a presença das IBRs e a entrada dos DATACENTERS, sobrecarregando as linhas de transmissão.
O FACTS (M-SSSC) é inserido em série com a linha, modificando sua impedância. É composto por filtros, sistemas de bypass e sistemas conversores. Testes e simulações efetuadas mostraram a eficiência do dispositivo sem impactos nos sistemas de proteção.
O FACTS (M-SSSC) é inserido em série com a linha, modificando sua impedância. É composto por filtros, sistemas de bypass e sistemas conversores. Testes e simulações efetuadas mostraram a eficiência do dispositivo sem impactos nos sistemas de proteção.
Foram apresentadas as metodologias utilizadas para sincronização dos sistemas de PMUs de subestações, convencionais e digitais.
Foram apresentadas as metodologias utilizadas para sincronização dos sistemas de PMUs de subestações, convencionais e digitais.
A preocupação com a capacitação de pessoal em subestações digitais gerou a criação de metodologias de treinamento e de métricas para sua avaliação.
A preocupação com a capacitação de pessoal em subestações digitais gerou a criação de metodologias de treinamento e de métricas para sua avaliação.
A metodologia proposta pela GE VERNOVA tem como pilares a avaliação da satisfação dos participantes, o aumento do conhecimento adquirido e foco nos resultados obtidos.
A metodologia proposta pela GE VERNOVA tem como pilares a avaliação da satisfação dos participantes, o aumento do conhecimento adquirido e foco nos resultados obtidos.
A HITACHI, em parceria com o SENAI, montou o Laboratório para o GRID 4.0 onde a TI também foi trazida para a formação da engenharia elétrica.
A HITACHI, em parceria com o SENAI, montou o Laboratório para o GRID 4.0 onde a TI também foi trazida para a formação da engenharia elétrica.

Por conta das novas diretrizes de engenharia e com o objetivo de suprir as demandas de proteção e controle, houve a proposta de modernização do currículo da engenharia elétrica pala Universidade Federal Fluminense – UFF.
Por conta das novas diretrizes de engenharia e com o objetivo de suprir as demandas de proteção e controle, houve a proposta de modernização do currículo da engenharia elétrica pala Universidade Federal Fluminense – UFF.
A modernização do currículo da engenharia elétrica pala Universidade Federal Fluminense – UFF considerou as novas competências em temas como digitalização, fontes renováveis, segurança cibernética, entre outros.
A modernização do currículo da engenharia elétrica pala Universidade Federal Fluminense – UFF considerou as novas competências em temas como digitalização, fontes renováveis, segurança cibernética, entre outros.