

Interface



Fascículo Bônus: Cinco Descobertas em MHz

SEL

Edição 47
Mai/Jun 2019

ANO 14



GUIAS DE APLICAÇÃO
Facilidade na Utilização
de Produtos SEL

EDUCAÇÃO E CARREIRA
Ações da SEL Têm
Impacto na
Comunidade

INTERFACE ENTREVISTA
Diretor Técnico
Internacional fala sobre
Segurança Cibernética



Segurança Cibernética, Desafios e Tendências

A segurança cibernética é uma preocupação cada vez mais frequente e presente no dia a dia de empresas de diversos segmentos. No sistema de potência, esse tema é especialmente importante e deve ser tratado com seriedade dado os impactos que um ataque cibernético pode acarretar. Para abordar esse assunto, na edição do Interface deste mês, trazemos uma entrevista exclusiva com o diretor Técnico Internacional da SEL, David Dolezilek. Ele vai abordar as principais tendências tecnológicas em segurança cibernética, desafios e expectativas para o setor elétrico.

Em outra matéria especial do Interface, você poderá conhecer um pouco sobre as ações sociais que a SEL tem realizado que incluem a criação de laboratórios de matemática e química até a inauguração de um cantinho de leitura especial em uma escola de nossa comunidade. Com as iniciativas, houve melhora em indicadores de ensino mostrando que trabalho conjunto e solidário traz muitos resultados positivos.

Leia ainda um novo fascículo especial sobre a proteção de linhas no domínio do tempo. Desta vez, abordaremos cinco descobertas realizadas por meio da alta amostragem de equipamentos SEL e da análise de ondas viajantes.

Nesta edição preparamos um resumo dos principais guias publicados recentemente em nossa página para que você possa verificar qual será o ideal para te ajudar com nossas tecnologias.

Aproveite sua leitura!

Expediente Interface

Publicação da: Schweitzer Engineering Laboratories Comercial LTDA.

Endereço: Avenida Pierre Simon de Laplace, 633

Condomínio Techno Park - Campinas/SP CEP 13.069-320

Tel: (19) 3515-2060 | marketing_br@selinc.com.br | www.selinc.com.br

Editorial e redação:

BRSA - Branding & Sales: Agência de Comunicação Integrada

Telefones: (11) 5501-4007

Editora: Samara Monteiro Mtb. 39.948

Projeto Gráfico e Diagramação:

Schweitzer Engineering Laboratories Comercial LTDA.

Gráfica: Mundo

Tiragem: 7.500

SEL Promove Diversos Eventos



SEL promoverá em agosto, outubro e novembro as edições do Seminário Técnico de Proteção e Automação de Sistemas Elétricos Industriais, em Juiz de Fora (MG), Goiânia (GO) e São Luis (MA). O evento aborda inovações em proteção de motores e painéis de média e baixa tensão. Tecnologias que facilitam a modernização e gerenciamento de energia na indústria, com proteção e segurança das equipes e consequente ampliação da disponibilidade e receita serão discutidas no seminário. Também em agosto, no dia 19, em Belo Horizonte (MG), a SEL participa com estande e apresentações técnicas da **35ª edição do Circuito Nacional do Setor Elétrico, o Cinase**.

Já entre os dias 15 e 18 de setembro, em Recife (PE), os especialistas da SEL apresentarão dois artigos técnicos durante o **XIII Simpase - Simpósio de Automação de Sistemas Elétricos**. Serão discutidos os temas “Cibersegurança em Redes IEC 61850 Utilizando o Precision Time Protocol (PTP)” e “Comparação de Desempenho entre Relés Convencionais e Relés Baseados em IEC 61850 Sampled Values através de um Simulador em Tempo Real (RTDS)”.

Saiba mais sobre os eventos acessando link:

<https://selinc.com/seminarios>



Webinars

Além de eventos presenciais, a SEL também promove webinars, com exibição online e ao vivo.

Os webinars ocorrem sempre das 14h às 15h15. Inscreva-se através do link:

<https://selinc.com/webinars>



QUER RECEBER O INTERFACE ?

Acesse selinc.com/pt/support/Jornal-Interface





Guias de Aplicação Facilitam Aplicação de Produtos e Tecnologias SEL

A SEL possui ampla literatura técnica disponível em seu website para a disseminação de conteúdo técnico em proteção, controle e automação de sistemas elétricos. Para auxiliar os clientes, a SEL disponibiliza em sua página online diversos guias de aplicação que, de uma forma prática, ensinam como instalar, configurar e utilizar as ferramentas e funcionalidade de seus equipamentos e softwares. Confira os guias de aplicação disponibilizados recentemente pela SEL:

- **Melhorias no SEL-487E – elementos diferenciais:** apresenta as otimizações do SEL-478E na lógica de proteção dos elementos diferenciais. Explica quais foram as alterações desta lógica e como podem ampliar a velocidade e a segurança destes elementos.
- **Ativação do SEL-411L para proteção diferencial de linhas através de Ethernet:** mostra como ativar as configurações da proteção diferencial de linhas (87L) usando dois relés SEL-411L e o software AcSELerator QuickSet SEL-5030.
- **Configurando o SEL RTAC como uma única fonte para dados de evento de subestação:** apresenta os métodos existentes para recuperar dados de registros digitais e oscilográficos do processador de automação (RTAC) da SEL.
- **Curva de teste 46 em relés de proteção pra motores:** ensina como testar a curva térmica dos relés de proteção de motores SEL-710 e SEL-710-5.

- **Entendendo e efetivamente usando o SEL *Mirrored Bits Protocol*:** explica como usar o SEL *Mirrored Bits*, um protocolo seguro e confiável para transmitir dados digitais entre relés.
- **Aplicação da tecnologia Arc Sense nos relés da SEL:** esse guia mostra como a tecnologia pode ser usada para detectar faltas de alta impedância nos dispositivos SEL-451, SEL-751 e SEL-651R.
- **Usando a Extensão Event Mailer do acSELerator RTAC:** ensina como configurar um relé SEL e um RTAC para que este reúna os registros de eventos do relé, anexe-os a um e-mail e o envie conforme pré programado.

Esses e outros guias podem ser encontrados na página da SEL:
<https://www.selinc.com/guiaadeaplicacoes>



CURTAS



Custo de Aquisição versus Custos de Propriedade: Qual Utilizar?

O custo Total de Propriedade, em inglês TCO (*Total Cost of Ownership*), é um parâmetro que nos permite calcular o custo total de um produto ao longo de sua vida útil. Esse cálculo leva em conta não apenas o valor inicial da aquisição, mas todas as despesas, muitas vezes inesperadas, que este equipamento pode acarretar enquanto estiver em operação.

A SEL desenvolveu uma ferramenta online gratuita que permite calcular o custo total de propriedade, TCO, de um equipamento e assim permitir aos engenheiros, técnicos e profissionais que atuam na aquisição de material, calcularem exatamente



o quanto aquele produto custará em toda sua vida útil e não somente no momento da compra.

Há muitos equipamentos, que inicialmente apresentam custo mais elevado, podem fazer com que a empresa economize ao longo do tempo.

A calculadora já está disponível e pode ser acessada pelo link: <https://selinc.com/pt/app/computers-tco/>

Para utilizá-la basta fazer login em sua conta do mySEL (o cadastro pede apenas algumas informações básicas).





Ações da SEL para a Comunidade Têm Impacto no Ensino

Instalação de laboratórios de matemática e de química em escola de Campinas (SP), contribuíram com a melhora dos indicadores do ensino

Comunidade é um dos valores corporativos da SEL e para exercer na prática esse valor, a empresa promove diversas ações sociais. Uma delas é o “School Donation”, um projeto que contribui com iniciativas nas áreas de ciências e matemática em escolas públicas. Em Campinas (SP), a escolhida para receber o projeto foi a Escola Estadual Dr. Telemaco Paioli Melges, na Vila San Martin. A unidade ganhou um cantinho da leitura, dois laboratórios - um de química e outro de matemática - e, como consequência, registrou uma melhora no desempenho dos alunos e nos indicadores de ensino.

Com o laboratório de matemática funcionando, a escola tem colhido frutos como a melhoria no Índice de Desenvolvimento da Educação do Estado de São Paulo (IDESP). De 2016 para 2017 houve uma melhora de 56% nos indicadores do Ensino Fundamental e de 13% no

índice dos exames de matemática do Ensino Médio. De modo geral, o indicador cresceu cerca de 27% para os dois grupos neste mesmo período.

Os laboratórios

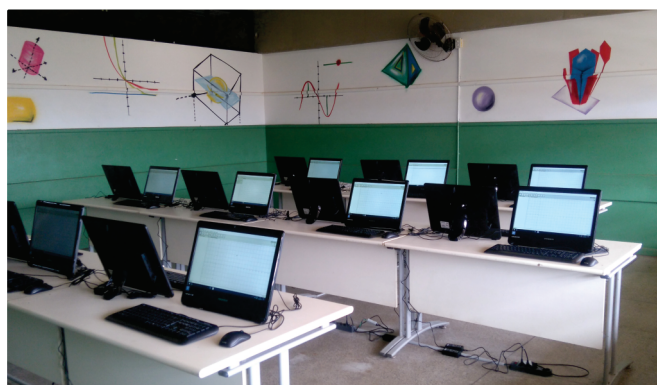
Em março de 2017, a SEL criou o laboratório de matemática na escola com um investimento superior a R\$ 38 mil. Computadores novos e de última geração foram entregues pela SEL, que montou o laboratório possibilitando aos alunos usarem os *softwares* de ensino com aulas práticas de matemática. “A escola já tinha os *softwares*, mas os alunos não podiam usá-los porque não havia computadores”, explica Ana Flávia Giroto, Analista de Recursos Humanos da SEL.

Já em setembro de 2018, o Laboratório de química foi montado com recursos de mais de R\$ 40 mil, o que viabilizou a compra de todos os equipamentos

De 2016 para 2017 houve uma melhora de 56% nos indicadores do ensino fundamental e de 13% no índice dos exames de matemática do Ensino Médio.



Sala antes da instalação do laboratório de matemática



Novo laboratório de matemática

necessários para que os alunos pudessem realizar experimentos de química e física.

“Entregamos o laboratório com ferramentas como tabelas periódicas, cilindros e equipamentos para que os alunos pudessem aprender e em 2019 estamos reformando o laboratório, com melhorias na alvenaria e infraestrutura”, enfatiza Ana Flávia.

De acordo com o Diretor da escola, Josemar de Toledo, o laboratório ajuda no desenvolvimento do raciocínio dos alunos. “Essa parceria nos proporcionou uma grande contribuição, inclusive com a criação do laboratório de química que é um espaço bastante utilizado pelos professores desta disciplina e também de biologia. Sempre que os professores levam os alunos para fazer essa aula prática, as crianças demonstram mais interesse e prestam mais atenção às aulas”.

Segundo o Diretor, este ano devem acontecer novas ações acordadas com a SEL, como a reforma do piso do laboratório de informática e benfeitorias no laboratório de química, incluindo a instalação de bebedouros de água.

Centenas de livros no Cantinho da Leitura

O Cantinho da Leitura, também construído pela SEL em 2017, recebeu mais uma grande doação de livros em outubro do ano passado. Colaboradores da SEL fizeram uma campanha, que uniu o Dia das Crianças com o Dia Internacional do Livro, e doaram quase 500 títulos. “A repercussão foi muito boa. Pensamos nessa campanha porque as crianças e os jovens vão para a escola e têm diversas matérias como matemática, história e geografia, por exemplo, mas

não tinham muitas opções de livros de literatura que pudessem ler em casa como lazer. Agora podem levar esses livros para casa e conhecer outras realidades por meio da leitura”, conta Ana.

Benefícios para toda a comunidade

Este ano, as campanhas da SEL passaram a incluir outras instituições de ensino no entorno da empresa, como a Escola Estadual Maria de Lourdes Bordini, voltada a alunos entre 6 e 11 anos. A campanha de Páscoa foi direcionada a esta escola e levou mais de 600 saquinhos de chocolate para as crianças. Neste momento, está a todo vapor a Campanha do Agasalho. A doação ocorrerá ainda neste mês e os colaboradores irão escolher para qual instituição entregarão roupas e cobertores. Em 2018, a empresa doou quase 170 itens.



Equipe SEL junto com a antiga diretora do colégio

Junte-se à SEL em prol da solidariedade



Hoje, todas as campanhas e doações feitas pela SEL, são viabilizadas graças a participação ativa de seus colaboradores. E agora, a companhia quer ampliar o alcance e os resultados dessas ações, incluindo a participação de parceiros, clientes e fornecedores, que já demonstram interesse em contribuir. Para se juntar à SEL nestas ações, basta enviar um e-mail para comunidade@selinc.com com seu nome e dados da empresa. A SEL entrará em contato para comunicar quais serão as próximas campanhas.



Cinco Descobertas Graças à Amostragem em Mega-Hertz e Análise de Ondas Viajantes

Durante as últimas edições do jornal Interface, foram abordados os princípios da Proteção no Domínio do Tempo. Após uma base teórica, que explorou o conceito por trás das grandezas incrementais e das ondas viajantes, foram abordadas as proteções envolvendo grandezas incrementais: elemento de distância (TD21) e elemento direcional (TD32) e as baseadas em ondas viajantes (*travelling waves*): elemento direcional (TW32) e elemento diferencial de linha (TW87).

Relés de proteção baseados em ondas viajantes com capacidade de amostragem de mega-Hertz, abriram caminho não só para as proteções citadas, mas também para monitoramentos com resolução que não era possível alcançar com os relés de proteção convencionais. Por estarem continuamente disponíveis (24/7), esses relés mantêm vigilância constante sobre o sistema de energia, gravando muitos eventos que permitem a observação inédita de vários fenômenos.

Durante dois anos, a SEL coletou mais de 20 mil registros abrangendo um amplo número de aplicações e níveis de tensão. Do monitoramento de uma rede de transmissão de 765 kV, à análise de transitórios da comutação de um reator shunt em 13,8 kV, conseguiu-se um consistente número de dados que possibilitou a empresa um melhor entendimento do sistema elétrico. Parte disso será compartilhado neste fascículo, que abordará cinco descobertas feitas graças à amostragem em mega-Hertz e à análise de dados de ondas viajantes.

Monitoramento de disjuntores

O disjuntor é um dos equipamentos mais importantes

do sistema elétrico e seu mau funcionamento pode danificar outros equipamentos e até impactar na segurança humana. Uma amostragem em mega-Hertz permite uma análise detalhada de cada operação do disjuntor, incluindo a discrepância de pólos, saúde do resistor de pré-inserção e possíveis reignições.

A Figura 1 mostra as correntes e tensões captadas por um relé do domínio do tempo SEL-T400L instalado no terminal local durante a energização de uma linha de 230 kV. As formas de onda da fase A são azuis, da fase B são verdes e da C são vermelhas. Este esquema de cores é usado de forma consistente em todo texto.

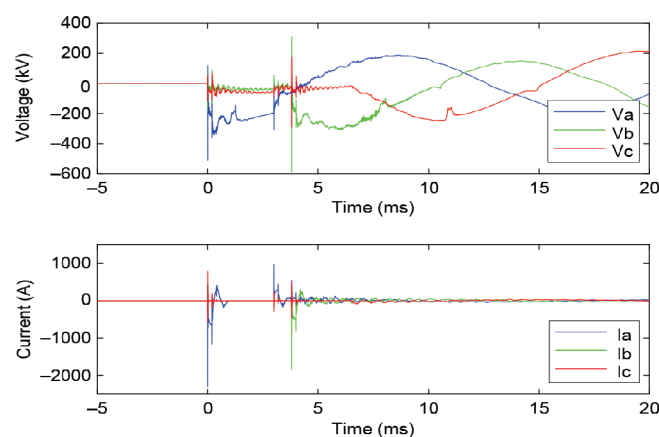


Figura 1 - Tensões e correntes no terminal local durante a energização de uma linha de 230 kV

É possível perceber que a fase A foi fechada primeiro, $t=0$. A fase B foi fechada em $t=3,8$ ms e a fase C foi fechada em $t=6,5$ ms. A fase A abre inesperadamente em $t=0,9$ ms e depois fecha novamente em $t=3$ ms. Observando o comportamento do disjuntor do terminal remoto na Figura 2, é possível observar algumas diferenças.

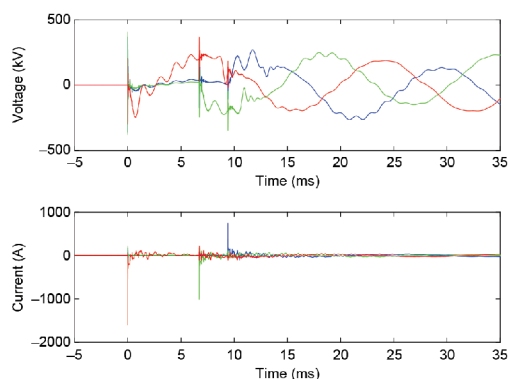


Figura 2 - Tensões e correntes no terminal remoto durante a energização de uma linha de 230 kV

A operação de fechamento do disjuntor remoto está de acordo com o esperado. No entanto, a discrepância entre os tempos de fechamento dos polos é relativamente alta, com a diferença de 10 ms entre o primeiro e o último. Já que a diferença de tempo típica gira em torno de 2 a 3 ms, estes 10 ms de diferença levantam questões sobre possíveis desalinhamentos mecânicos.

Rastreando tempestades

Relés no domínio do tempo SEL-T400L instalados em uma linha de 400 kV no México, conhecida por se situar em uma região com alta incidência de tempestades, permitiram que se conhecesse o perfil das ondas viajantes causadas pela incidência de raios.

A CFE, *Comisión Federal de Electricidad*, responsável por operar a linha, registrou, no dia 1º de agosto de 2017, 32 eventos no intervalo de 35 minutos. Os eventos registrados não eram faltas e sim distúrbios, o que levou o relé a não enviar sinais de *trips* aos disjuntores mas permitiu registro de oscilografias. Ao analisar as oscilografias, foi possível fazer algumas observações:

- A maioria dos registros continham transitórios de alta frequência, sem relação a uma fase específica;
- Cálculos da corrente diferencial mostram que as correntes transitórias foram injetadas na linha;
- Todos os eventos são originados dentro da linha de transmissão;
- A forma de onda injetada se assemelha ao padrão de 1,2 por 50 μ s, dos testes de impulso de curta duração;
- As assinaturas dos eventos são semelhantes nas diferentes fases, conforme Figura 3;
- O local dos distúrbios se move com o passar do tempo.

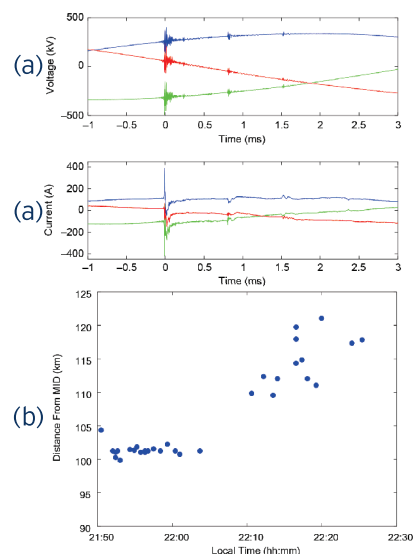


Figura 3 - (a) Tensões e correntes de um dos eventos registrados (b) Localização e horário dos distúrbios

Tais dados permitem concluir que os eventos foram causados por descargas indiretas. Estas descargas não atingiram efetivamente os condutores de fase, mas podem ter atingido cabos-guarda, torres ou o solo e estruturas nas imediações com amplitude insuficiente para provocar uma falta na linha. Foi constatado posteriormente que uma tempestade assolou a região no período estudado. Essa análise pode ser útil na identificação de uma falta causada por um raio que atinja alguma das fases, como mostrado a seguir.

Interrupção da corrente de falta

Outro caso interessante pode ser observado na análise de uma falta da fase B para a terra, em uma linha de 161 kV, comprimento de 117,1 km, apresentada na Figura 4.

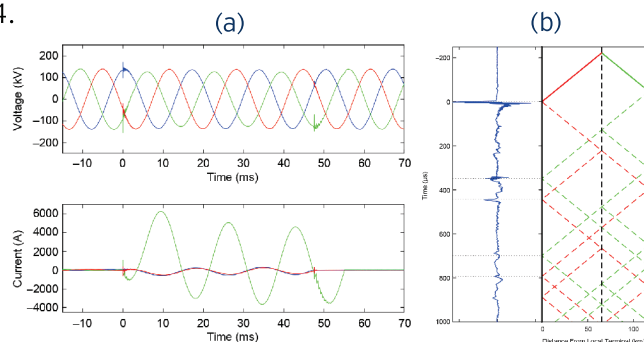


Figura 4 - (a) Tensões e correntes no terminal local durante uma falta (b) Diagram de Bewley das ondas viajantes geradas pela falta

Através das reflexões das ondas viajantes no diagrama de Bewley, é possível determinar a localização da falta em 65,5 km a partir do terminal local. Ao analisar a oscilografia pré-falta, especialmente o conteúdo de alta frequência, percebem-se dois distúrbios de baixa

>

amplitude, chamados de precursores, um a 76 ms e um 35 ms antes da falta, conforme a figura 5.

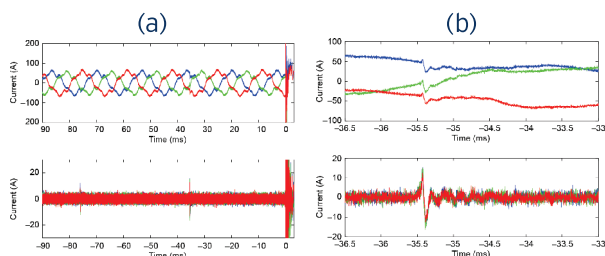


Figura 5 - (a) Correntes de fase e ondas viajantes de corrente pré-falta (b) Zoom das correntes e das respectivas ondas viajantes, no precursor

Ampliando um dos eventos precursor, como mostrado na Figura 5 (b), observa-se um transitório de corrente, com a mesma forma em todas as três fases. Como explicado na seção anterior, essa assinatura é característica de um transitório induzido por uma descarga indireta de um raio nas vizinhanças da linha de transmissão. É então provável que vários raios tenham causado descargas indiretas e um deles uma descarga direta, que gerou o *flashover* e consequentemente a falta.

Outro momento que merece atenção é a abertura do disjuntor. Observa-se um elevado conteúdo transitório na fase B com uma série de reflexões de ondas viajantes. Ao serem analisadas no diagrama de Bewley da figura 6, essas reflexões informam a mesma localização encontrada na falta: 65,5 km do terminal local.

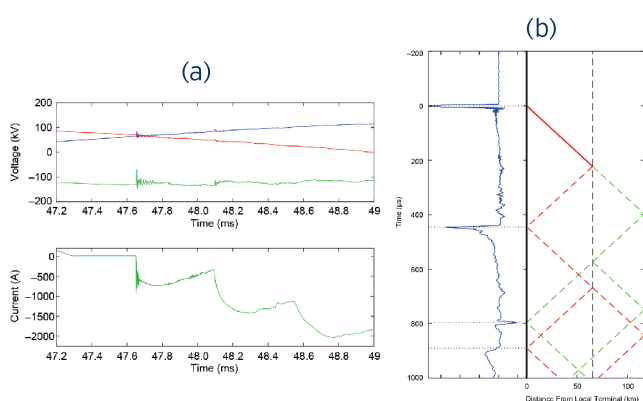


Figura 6 - (a) Tensões e correntes no instante da abertura do disjuntor (b) Diagrama de Bewley das ondas viajantes geradas da reignição da fase B

Pode-se concluir que o que causou as TWs foi uma reignição da fase B 360 μ s após a interrupção da corrente.

Monitoramento do sistema de transmissão

Relés SEL-T400L amostrando em mega-Hertz com

tecnologia de ondas viajantes podem auxiliar na obtenção de uma melhor compreensão dos efeitos eletromagnéticos presentes em subestação de alta e extra-alta tensão. Esses efeitos não podem ser percebidos através da amostragem tradicional dos relés baseados em fasores. A Figura 7 é referente a uma linha de 400 kV e apresenta as diferenças entre as oscilografias dos dois relés medindo as mesmas grandezas elétricas.

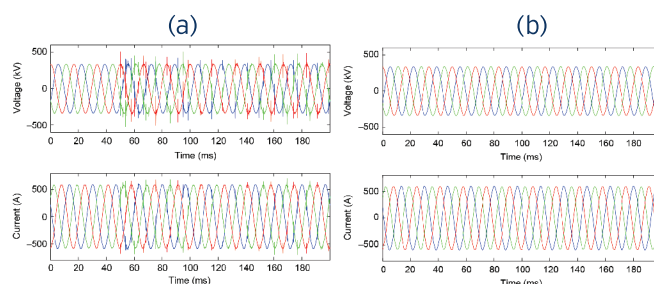


Figura 7 - (a) Tensões e correntes registradas por um relé no domínio do tempo (b) Tensões e correntes registradas por um relé convencional

Uma característica importante desses eventos é que eles não são exclusivos de faltas no sistema de potência. Eles também acontecem durante as sobretensões do sistema e ocorrem perto dos picos de tensão em 60 Hz. De modo geral, os eventos registrados caem na categoria de descargas parciais, em que capacitores séries da linha descarregam energia que é logo acomodada em capacitores séries subsequentes. Aplicando transformada de Fourier e exibindo o resultado em um diagrama *Waterfall* na Figura 8, percebe-se a presença dos sinais de comunicação através da linha (PLC) em 110 kHz, sinais vizinhos ao sinal PLC com menor magnitude e o sinal de alta frequência devido à a ressonância do PLC (indicado pela seta). Essa análise abre a possibilidade de que os transitórios medidos sejam injetados pela baixa tensão (115 kV).

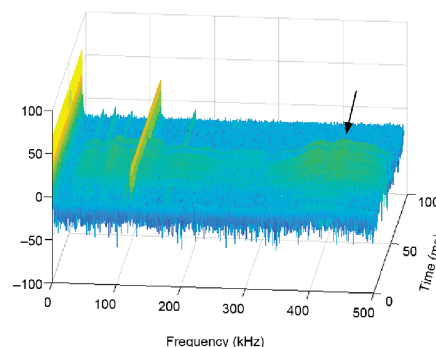


Figura 8 - Diagrama "Waterfall" mostrando conteúdo de alta frequência causado pelos eventos de descarga de alta energia em função do tempo

Outras análises foram feitas também em uma subestação de 765 kV, observando resultados similares. Pode-se concluir que os transitórios observados são comuns em subestação de alta e extra-alta tensão.

Essas informações, após mais estudos e análises podem ser usadas no futuro para auxiliar na manutenção preditiva e na avaliação do funcionamento das subestações.

Evolução de uma falta durante abertura monopolar

Por fim, outro fenômeno interessante observado é a falta evolutiva. Dois relés de proteção no domínio do tempo SEL-T400L, instalados um em cada terminal de uma linha de 230 kV na Guatemala, registraram a evolução de uma falta de fase C para terra para uma falta bifásica CA para terra após um ciclo de religamento. A Figura 9 apresenta a oscilografia do evento.

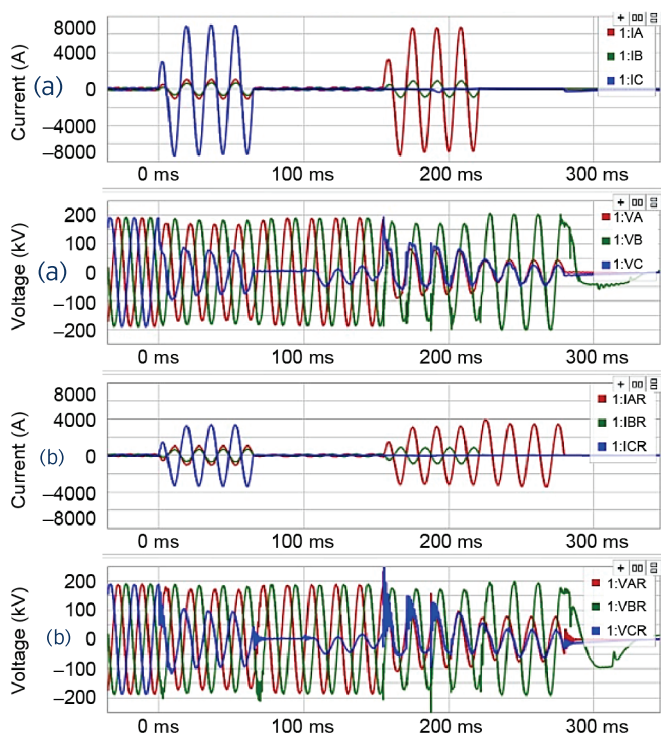


Figura 9 - (a) Tensões e correntes registradas pelo terminal local
(b) Tensões e correntes registradas pelo terminal remoto

Os sinais de tensão fornecem informações valiosas sobre a evolução da falta. A figura 9 (a) mostra as tensões das fases A e C. A aparência da tensão de fase C durante a condição de polo aberto indica que o arco secundário se extinguiu 108,4 ms após o início da falta.

Após 46,1 ms depois, a falta evolui para uma falta CAG com a diferença de tensão entre fase C e A tendendo a zero, como mostrado na Figura 10.

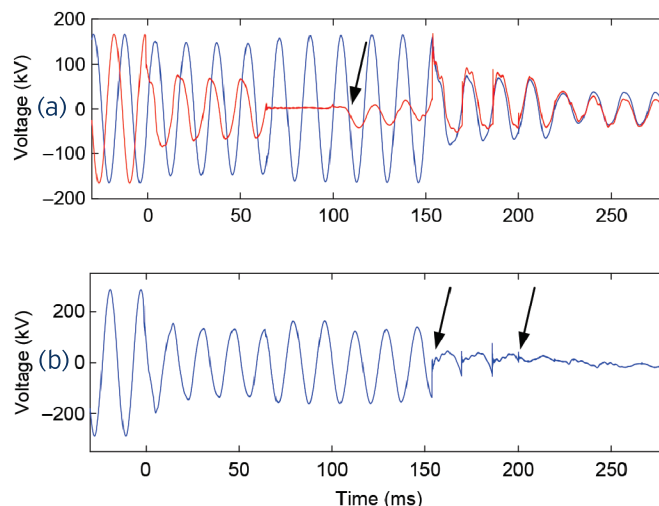


Figura 10 - (a) Tensões das fases A e C durante a evolução da falta
(b) Diferença entre as tensões da fase C e A durante a evolução da falta

Oscilografias em alta resolução com amostragem em mega-Hertz, que têm uma duração de até 1,2 segundos, permitem a análise da evolução da falta ao longo de toda a sequência de religamento. Transitórios de tensão durante o religamento após a condição de falta também são visíveis graças a alta taxa de amostragem. Observe que neste evento, os transitórios de tensão não excederam os valores operacionais normais.

Os cinco casos expostos são pequenos exemplos do que se pode descobrir graças à amostragem em mega-Hertz aliada à análise de ondas viajantes. Além da rápida velocidade na atuação da proteção, por volta de 2 ms, os relés de proteção no domínio do tempo possibilitam uma compreensão profunda de fenômenos antes impossíveis de serem observados com os relés convencionais. Esse conhecimento abre portas para um entendimento mais abrangente do sistema elétrico de potência, permitindo que os engenheiros busquem soluções cada vez mais seguras, confiáveis e econômicas.

Veja mais exemplos de eventos e oscilografias registradas pelos relés SEL-T400L acessando:
<https://selinc.com/pt/mktg/122973/?fallback>





Automação e Segurança Cibernética

O Diretor Técnico Internacional, David Dolezilek, fala sobre os principais desafios de cibersegurança até as últimas tendências do setor

No Brasil para participar do Seminário Técnico de Automação e Segurança Cibernética, realizado entre os dias 29 e 30 de maio, o Diretor Técnico Internacional da SEL, David Dolezilek, conversou com o Interface sobre os temas do evento. Responsável por diversas pesquisas inovadoras na área de segurança cibernética, Dolezilek está na SEL há 23 anos e tem experiência em proteção, automação e integração de sistemas de potência, sendo autor de diversos artigos, inventor patentado e membro de comitês técnicos na área de segurança e padronização global de sistemas de comunicação. Na conversa com o Interface, ele abordou desde os motivos que levaram a ataques cibernéticos conhecidos como o da Ucrânia em 2015 até as últimas tendências do setor. Confira a entrevista completa:

Interface: Quais são os principais desafios de cibersegurança encontrados pelas concessionárias e indústrias? O que pode ser feito para evitar ciberataques como os que ocorreram na Ucrânia em 2015?

Dolezilek: Ao redor do mundo o que vemos é que as pessoas estão preocupadas com regras e regulações. Há inúmeros padrões internacionais, políticas e procedimentos mas a solução mais efetiva é desenvolver um sistema de cibersegurança que atue em profundidade, em que várias camadas de proteção sejam erguidas, dificultando assim os ataques. Além disso, cibersegurança é usar também informação digital em tempo real para tomar uma decisão e estar em controle. Não é apenas proteger dos *hackers*, mas fazer o sistema funcionar mesmo se houver um comando indevido ou uma configuração errada.

A maior ameaça são as pessoas desconhecendo como funciona o sistema de potência ou fazer sugestões que podem tornar produtos mais vulneráveis.

A SEL foi a única fabricante a participar da comissão designada a descobrir o que havia ocorrido na Ucrânia, junto a organizações internacionais. A maior lição é que a parte mais vulnerável a ataques em uma companhia são os funcionários. E assim como outros grandes ataques este partiu de um vírus em um e-mail. No caso da concessionária Ucrâniana, enviado em nome do presidente da empresa. Todos os registros mostram que a empresa tinha soluções para isso e se elas tivessem sido colocadas em prática, isso não teria ocorrido. Hoje temos tecnologias que analisariam o sistema de controle e comparariam com o que já estava predefinido. Se houvesse um comando que mudasse o estado do sistema, sem que isso já tivesse autorizado, barraria a ação.

Interface: Qual seria a importância de um manual de conduta para minimizar os riscos de ataques cibernéticos no Brasil (assim como já foi implementado nos EUA e na União Europeia)?

Dolezilek: Cada empresa deve ter um plano de operação que é um *checklist* que garante que todos os aspectos na questão das políticas de trabalho e até da cultura organizacional estão sendo seguidas como manter o treinamento das equipes, por exemplo. É preciso saber como implementar as políticas de cibersegurança de uma forma consistente, porém ter um plano para o caso do sistema não funcionar. O que recomendamos em adição a isso é usar padrões internacionais de segurança que são bem documentados e podem ser replicados.

Você tem que conhecer todos os riscos em sua companhia para que possa implementar um sistema de gerenciamento de riscos e estabelecer suas estratégias de defesa. Toda companhia deve ter liberdade para escolher suas práticas mas se você fornece ou consome energia em altos níveis de outros agentes, uma falha na segurança cibernética poderia afetar a estabilidade do sistema de potência, o que justificaria a existência de uma regulação mínima a nível nacional para os agentes de energia e grandes consumidores. O sistema elétrico é a chave para a economia estar forte, o que é a chave para um país saudável e ser um bom país para seu povo viver.

Interface: Como a SEL lida com vulnerabilidades em seus softwares ou equipamentos? Qual é seu procedimento?

Dolezilek: Temos um registro de todos os equipamentos que vendemos com seu número de série e quem os comprou. Quando detectamos uma vulnerabilidade cibernética ou uma falha em algum equipamento, enviamos um comunicado a todos os consumidores informando sobre a falha, suas implicações no funcionamento do equipamento ou sistema e já enviamos a solução. Essa tem sido nossa cultura desde o início, mantemos essa informação em privado, passando-a somente a funcionários da empresa que adquiriu o equipamento. O que é completamente diferente de nossos concorrentes que não sabem quem é dono dos equipamentos e não tem alternativa que tornar publicamente conhecida essa vulnerabilidade. Recentemente tivemos o primeiro ataque cibernético em uma empresa de distribuição nos Estados Unidos. Pouco após uma empresa fabricante de *switches* tornar pública a vulnerabilidade descoberta em um de seus produtos, criaram uma arma explorando essa vulnerabilidade e atacaram os *switches* na parte ocidental dos Estados Unidos, causando uma interrupção das comunicações por mais de cinco minutos entre o controle central, várias plantas de geração e subestações de transmissão. Se houvesse ocorrido uma falta neste meio tempo, as chances da proteção não atuar corretamente seriam altas, o que poderia levar a danos em equipamentos e até ao óbito.

Interface: Qual o papel da SEL no desenvolvimento de inovações no setor elétrico? Quais são as tendências para os próximos anos?

Dolezilek: A SEL possui história gada na inovação.

O primeiro relé digital microprocessado foi criado pelo Dr. Schweitzer, fundador da empresa. Desde então, somos conhecidos por trazermos tecnologias inovadoras para o mercado, como o primeiro relé de proteção no domínio do tempo.

Mas inovação reside não só em criar algo, mas em também dar novo uso a tecnologias já existentes. Adicionar redes definidas por *software* (SDN) a subestações, por exemplo, foi uma resposta inovadora para uma necessidade de mitigar as perdas de pacotes e aumentar a segurança cibernética da rede. Em vez de inventar algo, trouxemos uma tecnologia que já existia e já era amplamente utilizada no mundo de TI, entendemos, modificamos e a aplicamos no sistema elétrico de potência.

Somos muito transparentes e abertos sobre as invenções que estamos fazendo. Compartilhamos com o mundo e dizemos o que fizemos, como funciona e como pode interagir com tecnologias de outras empresas.



Interface: Você possui algumas patentes relacionadas à segurança cibernética. Poderia nos contar um pouco do sobre sua última patente e pesquisas?

Dolezilek: A mais recente patente de segurança cibernética foi um monitor capaz de detectar uma mensagem vinda de uma fonte confiável mas com objetivo escuso. É basicamente um esquema para prevenir mudanças indesejadas no sistema, advindas de uma fonte que não é possível detectar se é maliciosa. Essa invenção também previne consequências e ações de alguém que não é malicioso mas não é bem treinado ou cometeu um erro que gerou uma mensagem de controle errada. Devemos ter em mente que qualquer interrupção é uma interrupção cibernética não

>

somente um ataque *hacker* de um local remoto. Qualquer interrupção é inaceitável e nós desenvolvemos uma tecnologia que previne operações indesejadas vindas de um ataque externo ou de algum erro interno de operação.

Na América do Norte, e isso é similar no Brasil, verificamos que as razões mais comuns para atuações indevidas são em primeiro lugar os erros humanos, em segundo falhas eletromecânicas e em terceiro erros da rede de comunicação. Há um mês houve ciberataques em sistemas de controle nos Estados Unidos, o da Ucrânia em 2015 e no Brasil em 2009 que depois descobriu-se que era apenas por conta de isoladores sujos. São três em três anos versus interrupções ocorridas todos os dias por conta de erros de parametrização, comandos indevidos, falhas nos equipamentos, comunicações ruins, etc. É nestas questões que devemos focar a maior parte se o objetivo é servir os consumidores com energia segura e confiável.

Interface: Em sua avaliação, como está o desenvolvimento do setor elétrico brasileiro? O que podemos esperar em termos de evolução para a SEL no Brasil?

Dolezilek: Temos visto companhias de outros países comprarem empresas brasileiras e trazerem suas estratégias cibernéticas e de controle de sistemas para o Brasil. O mesmo ocorre com outros países da América do Sul, porque grandes companhias veem que são regiões mais abertas a inovações e que se adaptam mais rapidamente que outras. Minha experiência mostra que colocar relé no campo levou outros países como a República da Geórgia e Vietnã a fazerem o mesmo por terem visto que isso foi um sucesso no Brasil. A maior usina do mundo em geração de energia, a Itaipu, se mostra como um grande modelo ao utilizar SDN. Passa uma boa percepção mostrando que adotou uma tecnologia que tem alta segurança cibernética e é interoperável. Outros países já avançaram mais em *compliance* o que não os torna mais protegidos que Itaipu ao adotar SDN que é uma tecnologia superior. Eu nunca vi ciberataques no Brasil, mas espero que os sistemas atuem muito rapidamente, uma vez que vocês têm uma grande área de serviço.

Interface: Quais as principais tendências para o setor elétrico?

Dolezilek: O futuro da indústria elétrica é muito similar

ao da indústria aérea e da indústria médica no que se refere à tecnologia. Um novo equipamento tem que ser avaliado antes de ser usado, ser capaz de atuar em missões críticas, ser confiável e disponível. Continua a haver um movimento não intencionado em nossa indústria de adaptação de tecnologias que não são apropriadas ou que possuem vulnerabilidades que são ignoradas. Sou constantemente acusado de ser fixado nisso ou preocupado demais com falhas e sou orgulhoso disso. Construo sistemas há 20 anos ao redor do mundo e sou chamado a consertar problemas. Eu sei que as coisas vão falhar. A indústria aérea é segura como é porque eles aprenderam a duras penas que é necessário usar *checklists* de como proceder e evitar falhas.

O sistema elétrico é responsável por mover todo o mundo e todas as economias. Devemos desenvolver sistemas que funcionem mas esperar que eles falhem tendo um plano de operação eficiente. Agora se for preciso conviver com alguma vulnerabilidade em um sistema é preciso explicar isso a seus consumidores, internos ou externos, e decidir junto a eles se vale a pena correr riscos, aceitando as consequências disso. Permanecer em silêncio, porém, é algo que a indústria não deve fazer.

Conhece a galeria de posters de segurança cibernética da SEL?

Acesse e faça o download desses e muitos outros.

<https://selinc.com/solutions/sfci/cybers/ecurity-posters/>

