Redefinindo a Complexidade de Sistemas de Proteção

Edmund O. Schweitzer, III e David E. Whitehead
Schweitzer Engineering Laboratories, Inc.

Edição revisada lançada em outubro de 2019

Originalmente apresentada na
46th Annual Western Protective Relay Conference, outubro de 2019

Traduzido para o português em maio de 2020

Redefinindo a Complexidade de Sistemas de Proteção

Edmund O. Schweitzer, III e David E. Whitehead, *Schweitzer Engineering Laboratories, Inc.*

***Resumo*—Em 1962, A.R. van C. Warrington escreveu em seu livro, *Protective Relays – Their Theory and Practice*: "Enquanto o principal requisito da instrumentação é a precisão sustentada, o requisito mais importante dos relés de proteção é a confiabilidade, pois eles podem supervisionar um circuito durante anos antes que uma falta ocorra; se ocorrer uma falta, o relé deve responder instantânea e corretamente. Por esse motivo, os projetistas devem sempre tentar usar construções e conexões simples de relés. Apesar das boas intenções a esse respeito, há uma tendência de estender a operação dos esquemas de relés, incluindo recursos adicionais até resultar em complexidade e, então, torna-se necessário redesenhar. Em outras palavras, um gráfico do progresso da engenharia de relés em relação à complexidade tende a seguir o formato de um dente de serra." [1]**

Em 1984, o primeiro relé baseado em microprocessador do mundo redefiniu nossa indústria com métodos de construção mais simples, autoteste, melhor sensibilidade para detecção de faltas e interfaces homem-máquina simples, consistindo em portas seriais, um conjunto modesto de comandos e menos de uma página de ajustes. A nova tecnologia foi solidamente adotada; no entanto, o desejo de inclusão de mais funções recursos começou a aumentar a complexidade, que incluía recursos como integração, automação, medição, protocolos SCADA, sincrofasores e valores amostrados (*sampled values*). Atualmente, a quantidade de códigos (*firmware*) que desempenham a automação e comunicação em um relé de proteção é nove vezes maior e mais complicada do que códigos que executam os algoritmos de proteção.

Como Warrington previu, o formato de dente de serra da complexidade da proteção continuou a aumentar, por isso é justo perguntar:

- **A atual proteção do sistema de potência é muito complexa?**
- **A complexidade é uma consequência natural e inevitável do avanço da proteção do sistema de potência?**
- **A proteção, a automação e a comunicação em dispositivos únicos são vantajosas ou essas funções devem ser separadas em dispositivos dedicados?**

I. Introdução

A Fig. 1 mostra um diagrama simplificado da proteção, automação, comunicação e equipamentos associados de uma subestação em uma extremidade de linha de transmissão.

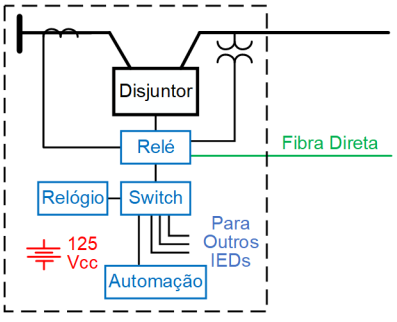

Fig. 1. Diagrama Simplificado de Proteção, Automação e Comunicação de Subestações

Os elementos mostrados na Fig. 1 incluem o seguinte:

- **Sensor e Atuadores**. Esses elementos medem e controlam sistemas físicos, por exemplo, transdutores de tensão e corrente e os disjuntores.
- **Relés.** Os relés monitoram o sistema de potência quanto a faltas. Quando uma falta é detectada, os relés emitem comandos aos disjuntores para eliminá-las.
- **Automação**. Os elementos de automação integram, combinam, processam e emitem comandos para conduzir o sistema de potência ao estado desejado e fornecer visibilidade aos operadores como parte dos sistemas SCADA.
- **Comunicação**. Os elementos de comunicação transmitem informações entre dispositivos de proteção, automação e IHMs de operadores locais.
- **Relógio**. Os relógios geram códigos de tempo precisos para relatórios de registro de data e hora e, em alguns casos, o tempo é usado para alinhar dados para uso nas funções de automação e proteção.
- **Fonte de Alimentação**. Essa fonte centralizada alimenta dispositivos em subestações. As fontes de alimentação normalmente contêm baterias para continuar fornecendo energia no caso de a fonte de energia primária não estar disponível.

II. História ou Como Chegamos Onde Estamos

Nos anos 1900, Edison, Insull, Westinghouse, Tesla e outros criaram o sistema de potência com o qual estamos familiarizados hoje. Aplicando a teoria com a tecnologia disponível na época, eles desenvolveram sistemas que com segurança e economia, geravam e distribuíam energia elétrica.

Embora a tecnologia para proteger os sistemas de potência tenha avançado, os princípios de proteção do sistema elétrico permanecem essencialmente os mesmos há décadas. A Fig. 2 mostra uma linha do tempo com os avanços da proteção de sistema elétricos de potência.

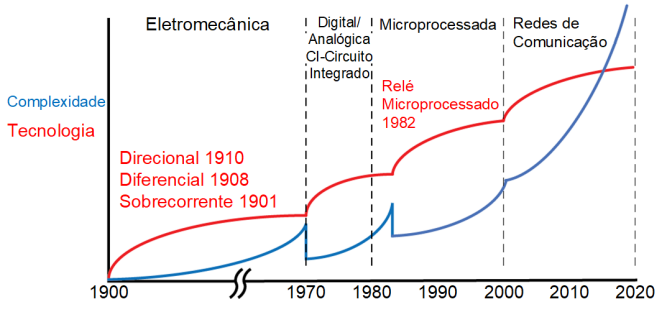

Fig. 2. Linha do Tempo da Proteção

A. Evolução da Proteção

Muitos dos princípios utilizados nos relés eletromecânicos foram desenvolvidos durante a primeira parte do século XX, como proteção contra sobrecorrente, direcional, distância e diferencial [2]. Os relés eletromecânicos forneciam pouca informação sobre o que aconteceu com o sistema elétrico.

Na década de 1980, com o avanço dos microprocessadores, algoritmos de relé de proteção foram implementados no primeiro relé baseado em microprocessador disponível no mercado.

A proteção baseada em microprocessador ofereceu não apenas os recursos de proteção de relés eletromecânicos, mas também inovações adicionais, como proteção de sobrecorrente de sequência negativa, fornecendo maior sensibilidade na detecção de faltas e detecção de invasão de carga para evitar disparos indevidos devido a carga elevada. Os relés microprocessados forneceram inovações impossíveis com a tecnologia eletromecânica e de estado sólido, incluindo localização de faltas, relatórios de eventos, autoteste e comunicação. Uma desvantagem é que os riscos cibernéticos surgiram, mas esses riscos foram atenuados desde o início por vários níveis de proteção por senhas, alarme por contatos respondendo a tentativas frequentes de alteração de senhas, bloqueios de firmwares e *checksums*, e em nível de sistema, criptografia de modems, relés controlados por SCADA isolando a linha discada dos modems, modems de discagem reversa, etc.

Os relés continuaram evoluindo, adicionando vários grupos de ajustes, mais recursos de comunicação, mais protocolos e mais recursos de automação. Esses avanços também resultaram em complexidade adicional. A Tabela I mostra a crescente complexidade do *software* dos relés.

TABELA I
ADICIONAR CAPACIDADES CONDUZ A COMPLEXIDADE EM RELÉS

Ano	Capacidades	KLOC[a]	Percentual Código Proteção
1982	4 amostras por ciclo, protocolos seriais simples e proprietários	20	40
1996	16 amostras por ciclo, comunicação serial, protocolos SCADA	80	27
2005	8.000 amostras por segundo, *Ethernet*, GOOSE[b], MMS[c], DNP3[d]	500	10
2018	8.000 amostras por segundo, *Ethernet*, GOOSE, MMS, DNP3, *sampled values*, PTP[e]	600	7

[a] Milhares de Linhas de codificação
[b] *Generic Object-Oriented Substation Event*
[c] *Manufacturing Message Specification*
[d] *Distributed Network Protocol*
[e] *Precision Time Protocol*

B. Evolução da Automação na Proteção

A automação de sistemas de potência começou na década de 1920. Consistiam em placas de controle e monitoramento localizadas nas usinas e subestações. Nos anos 30, as concessionárias começaram a interconectar seus sistemas para reduzir custos operacionais e melhorar a confiabilidade do sistema elétrico. Para fornecer melhor visibilidade do sistema de potência, foram desenvolvidas tecnologias analógicas que monitoravam e controlavam a saída do gerador, os fluxos de potência das linhas de interligação e a frequência do sistema [3].

Na década de 1950, os computadores analógicos foram desenvolvidos para programar a geração de cada gerador, a fim de fornecer o menor custo de geração. Esses computadores especiais foram o início dos Sistemas de Gerenciamento de Energia (*Energy Management System – EMS*). No final da década de 1960, computadores e *softwares* digitais foram desenvolvidos para substituir os EMSs analógicos. Os sistemas de automação começaram a aplicar unidades terminais remotas (UTRs) no final dos anos 70 e início dos anos 80. As UTRs mediam valores analógicos e variáveis digitais e transmitiam a telemetria de volta para um SCADA mestre e EMS.

Em 1985 foi lançada uma unidade terminal de relé de proteção (PRTU). Foi o primeiro dispositivo a se comunicar com vários relés. A PRTU integrou os dados de relés com o SCADA, reduzindo assim a necessidade de UTRs na subestação.

Os atuais dispositivos de automação evoluíram para plataformas de computação sofisticadas que incluem linguagens de programação avançadas como a IEC 61131; dezenas de protocolos proprietários, IEEE e IEC; e uma infinidade de opções de sensores de entradas e saídas, por exemplo, RTDs analógicos e variáveis digitais. A Tabela II mostra a crescente complexidade de *softwares* de automação.

TABELA II
ADICIONAR CAPACIDADES CONDUZ A COMPLEXIDADE NA AUTOMAÇÃO

Ano	Capacidades	KLOC
1985	Gateways de comunicação e distribuição de tempo	10
1995	Programação básica, alguns poucos protocolos e entradas e saídas digitais	110
2010	Programação avançada, múltiplos protocolos, muitas interfaces de entrada e saída	12.000

C. Evolução de Comunicações Para Proteção

As comunicações nos sistemas de potência começaram com simples entradas e saídas digitais. O estado do disjuntor era exibido em uma casa de controle usando um contato de saída (que representava o estado de um disjuntor) conectado a uma lâmpada com uma fonte de tensão. Da mesma forma, bastava um contato de relé conectado à bobina de disparo de um disjuntor com uma fonte de tensão para providenciar o comando de abertura. Ainda hoje, esses circuitos de comunicação são simples, confiáveis e fáceis de reparar.

À medida que as tecnologias de comunicação avançavam, novos esquemas de proteção baseados em comunicações foram introduzidos, tanto esquemas diferenciais de corrente de linhas como esquemas de teleproteção. As comunicações também permitiam acesso remoto a relatórios de oscilografias, relatórios de sequência de eventos, medição, estado do disjuntor e outros dados.

As tecnologias de rede foram implementadas e incluíram modems telefônicos em linhas alugadas, redes discadas, sistema *carrier* por ondas portadoras, fibra óptica direta, comunicações multiplexadas por divisão de tempo, rádio licenciado e não licenciado além de *Ethernet*.

Com a introdução dos relatórios de oscilografia e de sequência de eventos, tornou-se vantajoso estampar o tempo desses relatórios para comparar registros gerados por diferentes dispositivos em um sistema elétrico. Inicialmente, os dispositivos usavam um relógio interno para fornecer a estampa de tempo. No entanto, os relógios internos são sujeitos a desvios, resultando em diferentes estampas de tempo produzidos por dispositivos que medem o mesmo evento.

Em 1956, o Grupo de Trabalho de Telecomunicação (TCWG) do *American Inter Range Instrumentation Group* (IRIG) criou um formato padrão para distribuir sinais de tempo sincronizados que resultaram no Documento IRIG 104-60 [4]. Em 1984, os relés suportavam sincronismo de tempo por IRIG, resultando em eventos sincronizados dentro de milissegundos um em relação ao outro.

Em 6 de janeiro de 1980, o Observatório Naval dos EUA iniciou a operação do Sistema de Posicionamento Global (*Global Positioning System – GPS*). O GPS fornece uma posição precisa em praticamente qualquer lugar do mundo e também um tempo preciso. Os relógios de satélite produzem várias saídas de tempo, incluindo IRIG, pulsos por segundo e protocolos de tempo baseados em *Ethernet*, como SNTP (*Simple Network Time Protocol*) e PTP (*Precision Time Protocol*) com precisão nas dezenas de nano-segundos.

Embora os relógios de satélite tenham sido amplamente adotados nos projetos de proteção de sistemas de potência, eles são suscetíveis a interferências do clima, obstrução ou adulteração de sinal. Para solucionar essas vulnerabilidades, um sistema determístico de comunicações terrestres de área ampla foi lançado em 2011, capaz de fornecer precisão da distribuição do tempo nas dezenas de nano-segundos.

Assim como a complexidade de relés aumentou, a do sistema de distribuição de tempo também aumentou. Os sistemas de tempo iniciais consistiam em lógica digital e não incluíam *software*. Atualmente, os relógios via satélite suportam IRIG, SNTP e PTP e requerem milhões de linhas de código. A Tabela III ilustra o crescimento da complexidade do código de relógios.

TABELA III
ADICIONAR CAPACIDADES CONDUZ A COMPLEXIDADE DE TEMPOS

Ano	Capacidades	KLOC
1989	Módulo de distribuição de tempo	0
2005	Relógios por satélite GPS, IRIG e saídas por pulso	150
2015	Satélite multiconstelação, IRIG, SNTP, PTP e saídas por pulso.	17.000

III. ONDE A PROTEÇÃO DE SISTEMAS DE POTÊNCIA IRÁ TERMINAR SE FICAR NA ATUAL TRAJETÓRIA

Os atuais sistemas de proteção são impressionantes porque são:

- **Rápidos**. Os relés baseados em fasores detectam e disparam em 8 a 16 ms. Os relés no domínio do tempo disparam em menos de 2 ms.
- **Automatizados**. Os sistemas remotos coletam, processam e emitem comandos sem a necessidade de intervenção humana.
- **Interconectados**. Os sistemas de comunicação estão disponíveis nos sistemas de proteção, permitindo a troca de informações de proteção, SCADA e acesso da engenharia
- **Flexíveis.** A capacidade de programação dos relés, controladores de automação*, switches* de comunicação e outros dispositivos nas subestações fornecem esquemas de proteção e automação personalizados.

A tecnologia digital usada em proteção, automação e comunicação abriu muitas novas portas. Fornecedores e usuários trabalharam juntos na solução de problemas, aumentando o desempenho e melhorando a proteção, controle, monitoramento, automação e comunicação.

As coisas se tornaram cada vez mais complexas no processo—exatamente como Warrington observara meio século antes.

Não estamos descobrindo que se tornou, nas palavras de Warrington, "necessário redesenhar" novamente? Podemos redefinir novamente a complexidade?

IV. QUANTIFICAR A COMPLEXIDADE DE SISTEMAS DE POTÊNCIA

Warrington afirmou: "o requisito mais importante dos relés de proteção é a confiabilidade". À medida que adicionamos mais protocolos, amostramos cada vez mais rápido, acrescentamos novos recursos, adicionamos recursos aos recursos e continuamos a suportar tudo em qualquer coisa ... estamos aumentando exponencialmente a complexidade. Vamos quantificar essa complexidade e seus efeitos na disponibilidade usando a análise de árvore de falhas [3].

A referência [5] descreve como calcular a indisponibilidade a partir de uma taxa de falha, juntamente com o tempo necessário para detectar e reparar a falha.

$$q \cong \lambda T = \frac{T}{MTBF}$$

onde:

q é a indisponibilidade

λ é a taxa de falha

T é o tempo de inatividade médio, por falha

$MTBF = \frac{1}{\lambda}$ é o Tempo Médio Entre Falhas

(MTBF – *Mean Time Between Failures*).

Cada falha causa o tempo de inatividade T. Portanto, o sistema não está disponível durante o tempo T do tempo total de MTBF. A fração de tempo que o sistema não está disponível é T / MTBF. Para esta análise, as falhas são atribuídas ao *hardware*, *software* ou aplicação incorreta (fatores humanos, tais como erros de ajustes).

Utilizando a referência [3], definimos a indisponibilidade de vários componentes da subestação na Tabela IV, incluindo automação, um relógio e um *switch*. Os relés modernos compartilham muitos dos mesmos componentes usados em *hardwares* de automação, relógios e *switches*. Além disso, as mesmas práticas de projeto e padrões de ensaio de tipo aplicados aos relés também são aplicadas à automação, relógios e *switches*. Portanto, é razoável atribuir a indisponibilidade do *hardware* de relés a esses dispositivos.

TABELA IV
INDISPONIBILIDADE CAUSADA POR *HARDWARE*

Componente	**Indisponibilidade • 10^{-6}**
Disjuntores	300
Hardware de Relés de Proteção	100
Hardware de Automação	100
Hardware de Relógios	100
Hardware de *Switches*	100
Canal de Fibra	100
Sistema de Alimentação CC	50
TC (por fase)	10
TP (por fase)	10

Quando [3] foi escrito, os autores consideraram erros humanos, como erros de ajustes ou aplicação incorreta, como uma causa de indisponibilidade e calcularam um valor $100 \cdot 10^{-6}$. O valor de indisponibilidade foi baseado em um dispositivo de proteção com código de 100 KLOC. Se assumirmos que a chance de erro humano cresce linearmente com o número de ajustes em um dispositivo (essa é uma suposição conservadora) e o número de ajustes nos dispositivos cresce linearmente com KLOCs, podemos calcular a indisponibilidade causada por erros humanos para vários códigos em KLOC, conforme mostrado na Tabela V.

TABELA V
INDISPONIBILIDADE CAUSADA POR ERROS HUMANOS

KLOC	**Indisponibilidade • 10^{-6}**
100	100
500	500
800	800
1.000	1.000
1.500	1.500
2.000	2.000
2.500	2.500
3.000	3.000
3.500	3.500
4.000	4.000

Finalmente, estendemos o trabalho em [3] para tratar da indisponibilidade causada por erros de desenvolvimento. À medida que o tamanho do código aumenta, aumenta a chance de erros de codificação. Com o objetivo de calcular a indisponibilidade causada por erros de programação, assumimos o seguinte, com base na experiência de 35 anos de desenvolvimento de *firmware* de sistemas de proteção:

1. Defeitos de software se manifestam como um evento de indisponibilidade por ano para um dispositivo de 100 KLOC, que resulta em indisponibilidades de $100 \cdot 10^{-6}$.
2. Nossa experiência é que os erros de codificação não crescem linearmente com os KLOCs; em vez disso, os erros de codificação aumentam a uma taxa mais próxima da raiz quadrada dos KLOCs.

A Tabela VI define a indisponibilidade de dispositivos com base em erros causados por *software*.

TABELA VI
INDISPONIBILIDADE CAUSADA POR *SOFTWARE*

KLOC	**Indisponibilidade • 10^{-6}**
100	100
500	223
800	282
1.000	316
1.500	387
2.000	447
2.500	500
3.000	547
3.500	591
4.000	632

Para examinar os efeitos da complexidade na indisponibilidade, considere as duas topologias de sistema de proteção a seguir:

- Sistema 1: Esquema de Proteção Diferencial de Corrente de Linhas de Transmissão Convencional
- Sistema 2. Esquema de Proteção Diferencial de Corrente de Linhas com *Sampled Values*

A. Sistema 1: Cálculos da Indisponibilidade do Esquema de Proteção Diferencial de Corrente de Linhas de Transmissão Convencional

A Fig. 3 mostra duas subestações que fazem a proteção de uma linha de transmissão. Neste exemplo:

1. O esquema de proteção é o diferencial de corrente de linha (87L). A comunicação 87L é via fibra direta.
2. Os relés incluem funções de automação e lógica programável, comunicações Ethernet e IEEE C37.94 e protocolos como DNP3, IEC 61850, IRIG-B e PTP. O código base para este tipo de relé é 800 KLOC.
3. Os *switches* de rede usados para comunicação dentro da subestação têm um código base de 4.000 KLOC.
4. O relógio usado para distribuição de tempo na subestação tem uma base de código de 4.000 KLOC.
5. Um controlador de automação usado para SCADA, coleta de eventos etc. tem um código base de 2.000 KLOC.

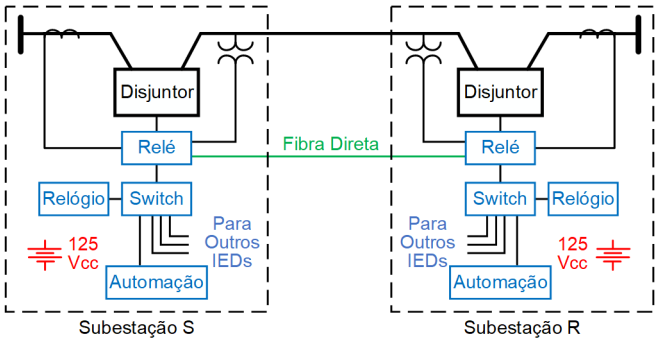

Fig. 3. Configuração da Proteção de Linha da Subestação no Sistema 1

Neste exemplo, os relés que executam a proteção diferencial de corrente de linha não requerem sincronização externa de tempo ou comunicação com outros dispositivos, exceto a conexão direta de fibra entre os dois relés. Como resultado, o *switch* de rede, o relógio e o controlador de automação—ao mesmo tempo que fornecem sincronização de tempo, automação e conectividade SCADA—não são críticos para detectar e eliminar faltas. Portanto, a análise da árvore de falhas e os cálculos de indisponibilidade não incluem esses dispositivos. A Fig. 4 mostra os elementos necessários para detectar e eliminar uma falta.

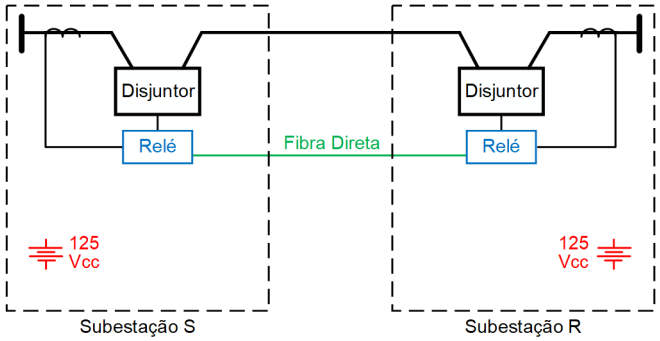

Fig. 4. Elementos de Proteção Necessários para Detectar e Eliminar uma Falta

Embora o controlador de automação, *switches* e os relógios não sejam necessários para a detecção de faltas, o código no relé e associados ajustes do usuário ainda contribuem para a indisponibilidade dos relés, ou seja, um erro de aplicação em um protocolo *Ethernet* pode causar indisponibilidade do relé. A Fig. 5 mostra a árvore de falhas da proteção diferencial de corrente de linha do Sistema 1.

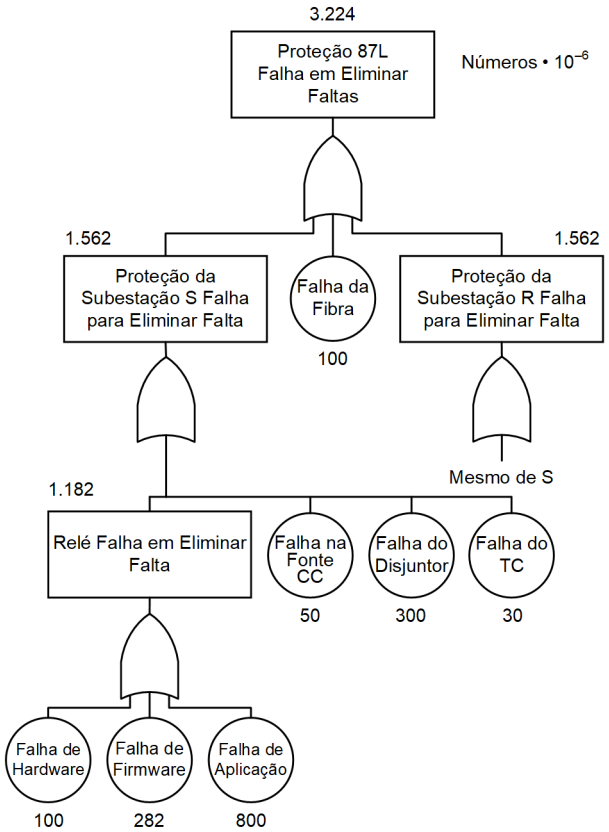

Fig. 5. Análise da Árvore de Falhas do Sistema 1 com Proteção Diferencial de Corrente de Linha

Usando o mesmo exemplo de indisponibilidade em [3], o esquema de proteção é aplicado em 100 linhas de transmissão, e cada linha possui 10 faltas por ano, resultando em 1.000 faltas por ano no total. Dado o cálculo da indisponibilidade de $3.224 \bullet 10^{-6}$ e 1.000 faltas, poderíamos esperar que 3 a 4 faltas por ano não sejam eliminadas pelo esquema diferencial de corrente da linha. Este exemplo não inclui outros elementos de proteção, tais como proteção de retaguarda dentro do relé, como elementos de distância ou um relé secundário que poderiam detectar e eliminar a falta quando o esquema de proteção diferencial de corrente de linha não estiver disponível.

B. Sistema 2 Cálculos da Indisponibilidade do Esquema de Proteção Diferencial de Corrente de Linhas de Transmissão com Sampled Values

A Fig. 6 mostra duas subestações que fazem a proteção de uma linha de transmissão. Neste exemplo:

1. O esquema de proteção é o diferencial de corrente de linha (87L). A comunicação 87L é via fibra direta.
2. Os relés incluem funções de automação e lógica programável, comunicação *Ethernet* e IEEE C37.94 e também protocolos como DNP3, IEC 61850, IRIG-B e PTP. O código base para este tipo de relé é 800 KLOC.
3. *Merging Units* (MU), são dispositivos de aquisição de dados que requerem redes *Ethernet* e tempo preciso para transmitir informações como volts e amperes ao relé. As MUs têm um código base de 100 KLOC.
4. *Switches* de rede usados para comunicação dentro da subestação têm um código base de 4.000 KLOC.
5. Os relógios usados para distribuição de tempo na subestação têm um código base de 4.000 KLOC.
6. Um controlador de automação usado para SCADA, coleta de eventos etc. tem um código base de 2.000 KLOC.

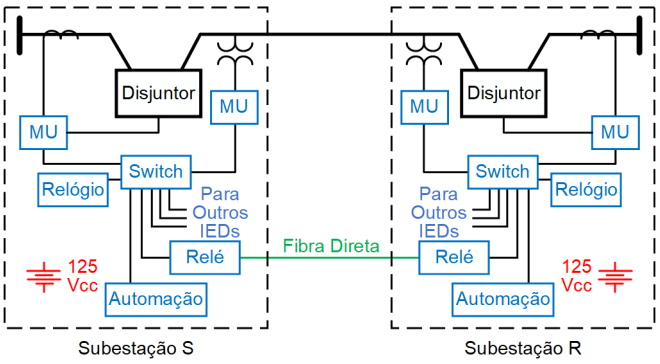

Fig. 6. Configuração da Subestação no Sistema 2 com Proteção de Linha com *Sampled Values*

Neste exemplo, o *switch* de rede e o relógio, juntamente com o relé e as *merging units*, são necessários para a proteção. Novamente, o controlador fornece funcionalidade de automação e visibilidade ao SCADA, mas não é crítico para detectar e eliminar faltas.

A Fig. 7 mostra o esquema de proteção diferencial de corrente de linha com *sampled values* do sistema 2 e a Fig. 8 mostra a árvore de falhas associada.

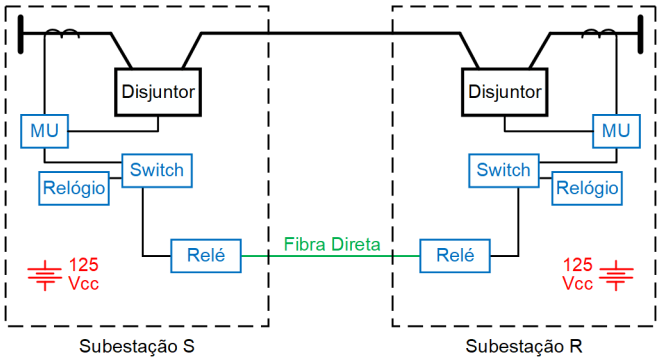

Fig. 7. Esquema do Sistema 2 com Proteção Diferencial de Corrente de Linha com *Sampled Values*

Novamente, suponha que esse esquema seja usado em 100 linhas de transmissão e cada linha tenha 10 faltas por ano, resultando em 1.000 faltas por ano no total. Dado o cálculo da indisponibilidade de $23.820 \bullet 10^{-6}$ e 1.000 faltas, poderíamos esperar que 23 a 24 faltas por ano não sejam eliminadas pelo esquema diferencial de corrente de linha. Este aumento da indisponibilidade é seis vezes a indisponibilidade do esquema diferencial de corrente de linha convencional.

Este exemplo não inclui outros elementos de proteção, tais como proteção de retaguarda no relé, como elementos de distância ou um relé secundário que poderiam eliminar a falta.

Essa análise mostra que o uso de mais dispositivos que são mais complicados, aumenta a indisponibilidade dos sistemas de proteção. Obviamente, os projetos podem ser desenvolvidos para reduzir a indisponibilidade de um sistema de proteção, por exemplo, adicionando proteção de retaguarda, incorporando redundância modular tripla (TMR), etc., todos os quais aumentam as taxas de falha, custo e a complexidade dos sistemas de proteção.

Existe uma oportunidade de redefinir a curva de complexidade e ainda obter sistemas de proteção simples, sensíveis, seletivos e de alta velocidade que forneçam automação, visibilidade do sistema e segurança cibernética? Acreditamos que a resposta seja SIM!

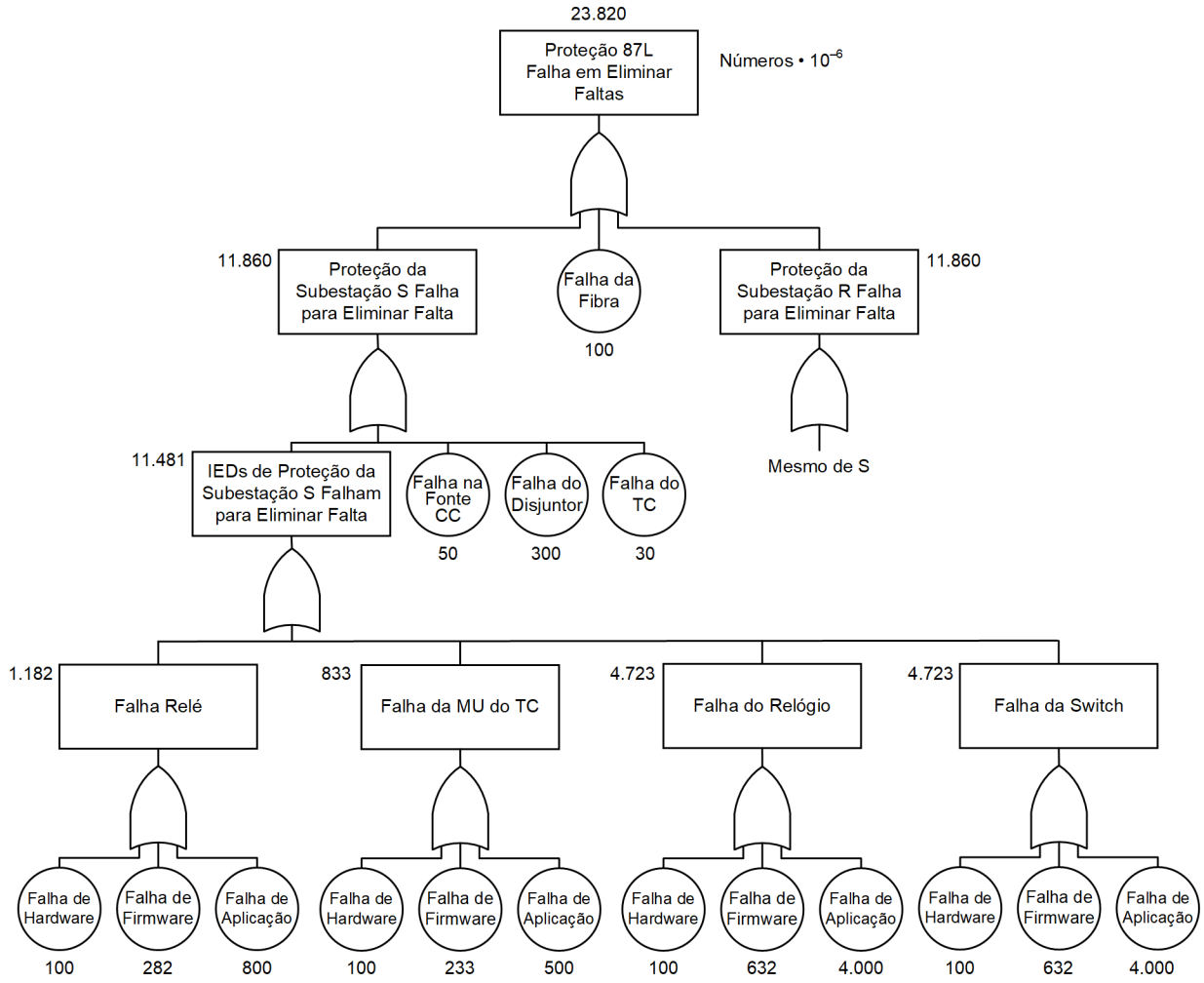

Fig. 8. Análise da Árvore de Falhas do Sistema 2 com Proteção Diferencial de Corrente de Linha com *Sampled Values*

V. EDEFININDO A CURVA DE COMPLEXIDADE

"… os projetistas devem sempre tentar usar construções e conexões simples de relés." [1]

Juntar recursos de proteção, automação, protocolos e comunicação em todos os relés de proteção tem um custo. Ajustar um relé moderno exige que o indivíduo seja especialista em proteção, *Ethernet*, códigos de tempo, lógica de programação, protocolos de comunicação, projeto de rede, segurança cibernética e assim por diante. Não apenas a pessoa que configura o relé precisa ser um engenheiro de sistemas de potência, mas também um especialista em controle de processos e cientista da computação.

Seguindo o conselho de Warrington, vamos projetar um sistema de proteção com os seguintes requisitos.

A. Proteção: Otimizada para Simplicidade, Dependabilidade, Confiabilidade e Desempenho

Os relés de proteção são instrumentos para fins especiais que medem tensões, correntes, estado dos contatos e trocam informações para fins de proteção. Quando o sistema de potência está em falta, os relés devem disparar os disjuntores RÁPIDO e seletivamente para isolar os problemas e não causar perda excessiva de serviço no processo. Todos as demais funções adicionadas a um relé, como recursos de automação e comunicação, embora ofereçam algumas vantagens, também aumentam a complexidade. Além disso, muitos recursos de automação e comunicação expõem relés a ameaças cibernéticas. Levando essas observações em consideração, os requisitos de um relé devem consistir no seguinte:

- Somente recursos de proteção. Isso resulta no seguinte:
  - *Hardware* mais simples
  - Menos códigos, o que reduz erros de firmware
  - Menos ajustes, o que reduz erros de configuração e de aplicação
- Um protocolo único e simples para se comunicar com automação ou outros relés. Não é desejável usar protocolos *Ethernet* comuns, como o IP, devido a grandes ameaças à segurança cibernética. Um protocolo único e simples simplifica o projeto e aumenta a eficácia da segurança cibernética.

- A capacidade de executar proteção unitária, por exemplo, incluir proteção de linha, barramento e transformador em um único dispositivo. Não separe o relé em dois dispositivos. Isso adiciona custo e complexidade. Se a redução de cobre for desejável, coloque os relés no pátio da subestação.
- Proteção que não seja dependente de sincronismo de tempo. Embora o tempo preciso seja valioso, os esquemas de relés de proteção não devem depender de fontes externas de tempo.
- Uma velocidade de inicialização mais rápida. Os relés de alto desempenho iniciam em 5 a 10 segundos; outros requerem um minuto ou mais para que a proteção seja ativada após a fonte auxiliar ser aplicada. No futuro, os relés devem inicializar em um segundo. Uma velocidade de inicialização mais rápida significa maior disponibilidade.

Mantendo o relé simples, estimamos que o tamanho do código possa ser mantido abaixo de 100 KLOC. Isso resulta nos números de indisponibilidade mostrados na Tabela VII.

TABELA VII
INDISPONIBILIDADE DE RELÉS

100 KLOC	**Indisponibilidade • 10^{-6}**
Hardware	100
Software	100
Aplicação	100

B. Automação: Integração de SCADA, Automação e Protocolos

O controlador de automação (CA) é a interface SCADA que fornece a função de automação local. Os atributos do CA incluem:

- O protocolo simples descrito acima para enviar e receber dados de relés. Os tipos de dados incluem medição, relatórios de oscilografias, relatórios de sequência de eventos, sincronização horária e acesso de engenharia.
- Para integrar-se ao SCADA, o CA suporta protocolos tradicionais, por exemplo, DNP3, IEC 61850 e MMS.
- O CA é a interface entre um usuário e um relé. Do ponto de vista de segurança cibernética, esse requisito reduz as ameaças para um único dispositivo na subestação, ao invés de exigir que todos os recursos de segurança cibernética sejam colocados em todos os dispositivos em uma subestação.
- A falha do CA não afeta a proteção.
- A indisponibilidade do CA usa um código base de 4.000 KLOC. O código base do CA é grande porque inclui funções de automação, vários protocolos de comunicação e protocolos de segurança cibernética.

Um código base grande é aceitável pelos seguintes motivos:

- A complexidade aumentada do CA é limitada a um único dispositivo que não é crítico para a proteção.
- Manter os protocolos no CA resulta em relés mais simples e com maior confiabilidade.
- As ameaças cibernéticas são gerenciadas no CA e não precisam ser gerenciadas nos relés.
- A indisponibilidade do sistema é reduzida usando um projeto com relés simples e um CA que executa as funções de automação.

A Tabela VIII mostra a indisponibilidade do controlador de automação para o sistema simples.

TABELA VIII
INDISPONIBILIDADE DE CONTROLADORES DE AUTOMAÇÃO

4.000 KLOC	**Indisponibilidade • 10^{-6}**
Hardware	100
Software	632
Aplicação	4.000

C. Comunicação: Projetada para Resiliência, Determinismo e Segurança Cibernética

A comunicação neste sistema é mantida simples e possui os seguintes atributos:

- Para fins de segurança cibernética, a comunicação entre os relés e o CA são um conjunto de dados fixos e não baseados em um padrão *Ethernet*. Um sistema de comunicação com conjunto de dados fixos se presta a *links* de comunicação determinísticos.
- A comunicação entre o CA e o SCADA inclui interface de rede padronizada e protocolos como DNP3 ou MMS.
- A falha da rede de comunicações entre o CA e o SCADA não afeta a proteção.
- É aceitável que uma falha de comunicação possa afetar o SCADA ou o acesso remoto ao CA e aos relés.

O código base para um s*witch* de rede de comunicação é de 4.000 KLOC. A Tabela IX mostra a indisponibilidade causada por falhas de *hardware*, *software* e aplicação.

TABELA IX
INDISPONIBILIDADE DE COMUNICAÇÃO

4.000 KLOC	**Indisponibilidade • 10^{-6}**
Hardware	100
Software	632
Aplicação	4.000

D. *Segregação: Funções Separadas de Proteção, Automação e Comunicação*

Atualmente, os dispositivos de proteção de sistemas de potência consistem em muitas características sobrepostas que requerem conhecimentos específicos para ajustá-los adequadamente. A Tabela X mostra um exemplo do número de ajustes necessários para os relés do Sistema 1 e do Sistema 2.

TABELA X
EXEMPLO DO NÚMERO DE AJUSTES DE PROTEÇÃO, AUTOMAÇÃO E COMUNICAÇÃO EM RELÉS

Relé	Proteção	Automação	Comunicação
Sistema 1	1.200	5.500	1.600
Sistema 2	1.200	6.100	2.300

A separação da proteção, automação e comunicação em dispositivos individuais oferece os seguintes benefícios:

- Especialistas em proteção, automação e comunicação podem definir ajustes e testar seus dispositivos com uma mínima sobreposição de outras funcionalidades.
- Com a abordagem simplificada de proteção, removemos o requisito de que os engenheiros de proteção precisam ser especialistas em automação ou projeto de redes de comunicação.

A Tabela XI mostra um exemplo do número de ajustes necessários para um relé simples com segregação de proteção, automação e comunicação.

TABELA XI
EXEMPLO DO NÚMERO DE AJUSTES PARA O RELÉ SIMPLES

Relé	Proteção	Automação	Comunicação
Sistema Simples	600	50	50

E. *Testes: Concepção para Facilitar Testes e Manutenção*

A separação das funções de proteção, automação e comunicação em dispositivos individuais simplifica o teste. Com os relés tradicionais, ao fazer alterações de ajustes, você deve considerar os possíveis impactos na automação e na comunicação dentro do relé, porque todos os três processos interagem no mesmo dispositivo. Com o sistema simplificado e sua segregação de proteção, automação e comunicação, a análise das alterações nos ajustes de proteção é limitada ao relé.

Os custos de manutenção são reduzidos. Se assumirmos que existe um problema no protocolo SCADA implementado nos relés que requer uma atualização de *firmware*, todos os relés na subestação devem ser retirados de serviço durante a atualização. Em nossa subestação simplificada, apenas o CA seria colocado fora de serviço para uma atualização do protocolo SCADA e os relés permaneceriam em serviço durante esta atualização de *firmware*. Referindo-se à Seção II, o KLOC do código para proteção é de 10 por cento, contra 90 por cento para a não-proteção. A probabilidade de a parte do código de automação e comunicação terem um erro de *firmware* é nove vezes maior do que no código de proteção. O sistema de proteção simplificado possui muito mais relés do que CAs. Eliminar as características de não-proteção dos relés resulta em menos atualizações, o que resulta em uma grande economia de manutenção.

A subestação simples descrita pelos critérios de projeto acima é mostrada na Fig. 9. Enquanto essa arquitetura é conforme o Sistema 1, as seguintes diferenças são significativas:

- O relé simples na Fig. 9 possui um sexto do código do relé mostrado na Fig. 3.
- A comunicação ponto a ponto entre o relé simples e a automação com um pacote de dados definido fornecem comunicação determinística e melhora a segurança cibernética. Observe os *links* de fibra entre o relé simples e a automação para reduzir a interferência eletromagnética.
- O relé simples é adequado para instalação em casas de controle tradicionais ou no pátio da subestação.

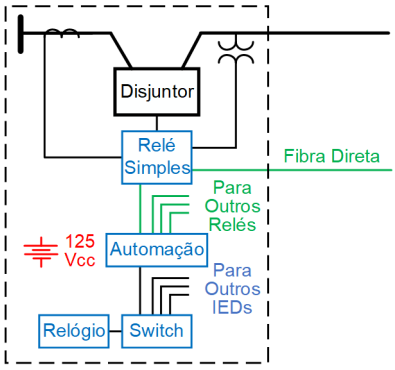

Fig. 9. Configuração da Subestação com Sistema de Proteção Simples

Retornando ao exemplo de indisponibilidade do relé diferencial de corrente de linha, a automação, *switch* e o relógio são removidos da Fig. 9, pois não são necessários para eliminar uma falta. A Fig. 10 mostra o equipamento usado nos cálculos da indisponibilidade. A Fig. 11 mostra a árvore de falhas do sistema de proteção simples.

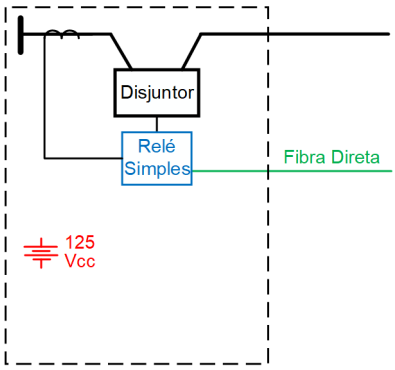

Fig. 10. Elementos do Sistema de Proteção Simples Necessários para Detectar e Eliminar uma Falta

Novamente, suponha que esse esquema seja usado em 100 linhas de transmissão e cada linha tenha 10 faltas por ano, resultando em 1.000 falhas por ano no total. Dado o cálculo da indisponibilidade de 1.460 x 10^{-6} e 1.000 faltas, poderíamos esperar que 1 a 2 faltas por ano não sejam eliminadas pelo esquema diferencial de corrente de linha. Trata-se de uma melhoria de 2 a 4 vezes na redução da indisponibilidade em

comparação com o sistema diferencial de corrente de linha convencional e uma melhoria 24 vezes na redução da indisponibilidade em comparação com o sistema com *sampled values*.

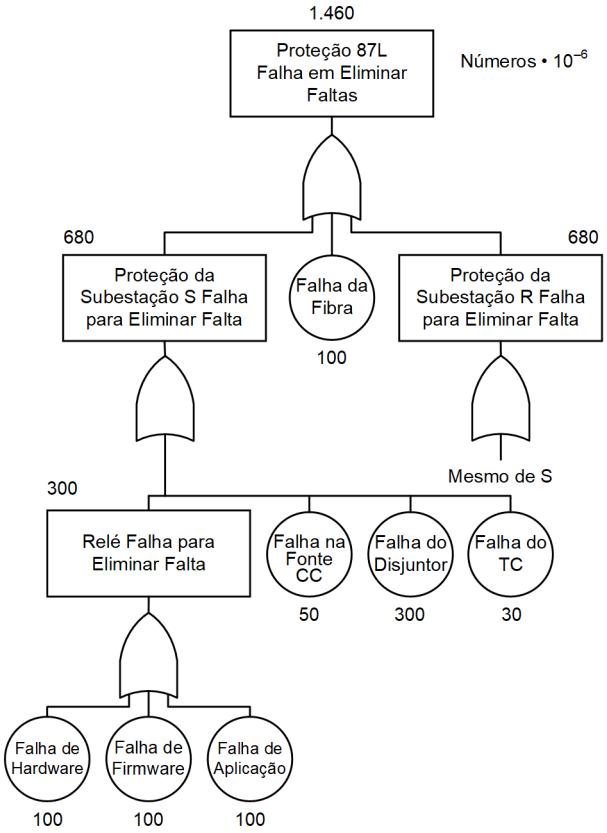

Fig. 11. Análise da Árvore de Falhas do Sistema Simples de Proteção Diferencial de Corrente de Linhas

VI. Conclusão

Os sistemas de proteção modernos avançaram a um ponto em que as faltas são eliminadas com rapidez e precisão, as tarefas que costumavam exigir informações humanas foram automatizadas e as informações criadas em um ponto do sistema de potência podem ser compartilhadas com vários dispositivos e processos instantaneamente através de todo o sistema elétrico. Os sistemas de potência são maravilhas tecnológicas.

No entanto, à medida que a proteção se torna mais rápida, a automação é mais prevalente e as comunicações se espalham amplamente, os sistemas de proteção se tornam mais complexos. O aumento em funcionalidades e recursos levou a projetos complexos de *hardware*, mais códigos nos dispositivos e mais ajustes que os engenheiros precisam entender e configurar. Essa complexidade, em última análise, torna os sistemas menos confiáveis.

Neste artigo, mostramos que a tendência no desenvolvimento de sistemas de proteção está aumentando em complexidade e que a complexidade resultará em mais indisponibilidade da proteção por um fator de seis.

Para lidar com essa tendência alarmante, descrevemos um sistema de proteção que simplifica o relé para incluir apenas funções de proteção e coloca as aplicações de automação e comunicação em outros dispositivos. Essa arquitetura demonstra os seguintes benefícios:

- A indisponibilidade do sistema de proteção é quatro vezes melhor que os sistemas de proteção modernos e vinte e quatro vezes melhor que os projetos de sistemas de proteção com essas tendências.
- Simplificação de ajustes por um fator de doze.
- Redução de ameaças de segurança cibernética de todos os dispositivos da subestação para apenas alguns, removendo os protocolos de TI dos relés.

Como Warrington sugeriu, a complexidade aumenta até que seja necessário redesenhar. Agora é a hora.

VII. Referências

[1] A. R. van C. Warrington, *Protective Relays: Their Theory and Practice*, Volume One, Chapman and Hall Ltd., London, 1968, pp 11–12.

[2] Z. Q. Bo, X. N. Lin, Q. P. Wang, Y. H. Yi and F. Q. Zhou, "Developments of Power System Protection and Control," *Protection and Control of Modern Power Systems*, Volume 1, Article number: 7 (2016).

[3] E. O. Schweitzer, B. Fleming, T. Lee, and P. Anderson, "Reliability Analysis of Transmission Protection Using Fault Tree Methods," proceedings of the 24th Annual Western Protective Relay Conference, Spokane, WA, October 1997.

[4] K. Behrendt and K. Fodero, "The Perfect Time: An Examination of Time-Synchronization Techniques," proceedings of the 32nd Annual Western Protective Relay Conference, Spokane, WA, October 2005.

[5] N. H. Roberts, W. E. Vesely, D. F. Haasl, and F. F. Goldberg, "Fault Tree Handbook," NUREG-0492m U.S. Nuclear Regulatory Commission, Washington DC, 1981.

VIII. Biografias

Dr. Edmund O. Schweitzer, III é reconhecido como pioneiro em proteção digital e detém o grau de Fellow Member no IEEE, um título concedido a menos de um por cento dos seus membros. Em 2002, ele foi eleito membro da National Academy of Engineering. Dr. Schweitzer recebeu a Medalha em Power Engineering em 2012, o maior prêmio concedido pelo IEEE, por sua liderança em revolucionar o desempenho de sistemas de energia elétrica com equipamentos de proteção e controle baseados em computador. Em 2019, o Dr. Schweitzer foi introduzido no National Inventors Hall of Fame por sua invenção do primeiro relé de proteção digital. O Dr. Schweitzer é o ganhador do Regents' Distinguished Alumnus Award e do Graduate Alumni Achievement Award concedidos pela Washington State University e também do Outstanding Electrical and Computer Engineer Award da Purdue University. Ele também recebeu doutorados honorários da Universidade Autônoma de Nuevo León, em Monterrey, México e da Universidade Autônoma de San Luis Potosí, em San Luis Potosí, México, por suas contribuições ao desenvolvimento de sistemas de energia elétrica em todo o mundo. Ele escreveu dezenas de documentos técnicos nas áreas de projeto e confiabilidade de relés digitais e detém mais de 200 patentes em todo o mundo relacionadas à proteção, medição, monitoramento e controle de sistemas de energia elétrica. Dr. Schweitzer recebeu seu diploma de bacharel e mestrado em engenharia elétrica pela Purdue University e seu doutorado na Washington State University. Ele lecionou nas faculdades de engenharia elétrica da Ohio University e na Washington State University e, em 1982, fundou a Schweitzer Engineering Laboratories, Inc. (SEL), para desenvolver e fabricar relés de proteção digitais e produtos e serviços relacionados.

David E. Whitehead é COO da Schweitzer Engineering Laboratories, onde supervisiona as operações globais da empresa. Por mais de uma década, Whitehead liderou a Divisão de Pesquisa e Desenvolvimento da SEL, uma equipe multidisciplinar de 800 pessoas responsável pela pesquisa, projeto, desenvolvimento e testes de sistemas que gerenciam, monitoram e controlam infraestrutura elétrica crítica. Líder reconhecido em cibersegurança de sistemas de controle de serviços públicos e industriais, Whitehead testemunhou perante o Senado dos EUA e a Federal Energy Regulatory Commission sobre a importância da inovação e da proteção contra ataques cibernéticos. Ele já se apresentou em várias conferências sobre segurança cibernética e escreveu dezenas de artigos sobre o assunto. Desde que ingressou na SEL em 1994, ele é um impulsionador do desenvolvimento de produtos e talentos e tem sido fundamental no desenvolvimento do fluxo constante de invenções que serão lançadas na SEL. Ele recebeu mais de 73 patentes em todo o mundo. Whitehead recebeu seu grau de bacharel em engenharia elétrica pela Washington State University e seu grau de mestre em engenharia elétrica pelo Rensselaer Polytechnic Institute. Ele é um membro sênior do IEEE e um engenheiro profissional registrado em Washington, Nova York, Michigan e Carolina do Norte.