



**XXII SNPTTE  
SEMINÁRIO NACIONAL  
DE PRODUÇÃO E  
TRANSMISSÃO DE  
ENERGIA ELÉTRICA**

BR/GTL/05  
13 a 16 de Outubro de 2013  
Brasília - DF

## **GRUPO-XV**

### **GRUPO DE ESTUDO DE SISTEMAS DE INFORMAÇÃO E TELECOMUNICAÇÃO PARA SISTEMAS ELÉTRICOS - GTL**

#### **REDES DE COMUNICAÇÃO E SINCRONIZAÇÃO DE DADOS PARA ESQUEMAS DE PROTEÇÃO DIFERENCIAL DE CORRENTE DE LINHA**

**Bogdan Kasztenny, Normann Fischer, Ken Fodero e Adrian Zvarych  
SCHWEITZER ENGINEERING LABORATORIES**

## **RESUMO**

Este artigo considera os esquemas diferenciais de corrente de linha sob o ponto de vista da comunicação de dados e alinhamento dos dados de corrente. O objetivo consiste em melhorar o conhecimento dos especialistas em relés sobre alguns aspectos essenciais e exclusivos dos esquemas de proteção diferencial de corrente de linha digital: comunicação, manipulação de dados e alinhamento de dados. Este artigo procura também aumentar a compreensão das aplicações da proteção diferencial de corrente de linha e requisitos do sistema relacionados entre os engenheiros de comunicação das concessionárias de energia elétrica.

## **PALAVRAS-CHAVE**

Diferencial, Multiplexadores, SONET, SDH, Comunicação

### **1.0 - INTRODUÇÃO**

O princípio da proteção diferencial de corrente de linha torna-se cada vez mais atrativo nos sistemas de potência atuais devido a sua boa imunidade à mudança nas condições do sistema e à penetração cada vez maior de fontes não tradicionais de correntes de falta, excelente sensibilidade, bom desempenho nas linhas com compensação série e multiterminais, e simplicidade da aplicação sob o ponto de vista da engenharia de proteção tradicionalmente conhecida. A expansão e o custo reduzido dos sistemas de comunicação das concessionárias promovem ainda mais este princípio de proteção avançada.

Contudo, a proteção diferencial de corrente de linha requer um canal de comunicação de longa distância para troca dos dados de corrente, bem como um mecanismo de sincronização para alinhamento dos valores de corrente medidos nos terminais de linha geograficamente distribuídos. Essas dimensões da aplicação são relativamente novas para um engenheiro de proteção, mas são absolutamente essenciais para a segurança e confiabilidade dos esquemas de proteção diferencial de corrente de linha.

Este artigo foca nas questões de troca e alinhamento de dados dos esquemas diferenciais de corrente de linha (87L), visando permitir uma melhor compreensão dos domínios da proteção e comunicação, uma vez que eles se cruzam nesta aplicação específica.

### **2.0 - PROJETO DOS RELÉS 87L PARA QUESTÕES DE COMUNICAÇÃO**

#### **2.1 Erros de Bits e Integridade dos Dados do 87L**

Ruídos no canal de comunicação podem corromper os dados. O termo "ruído" refere-se à interferência acoplada ao meio do canal ou dispositivos eletrônicos, componentes com defeito nos dispositivos eletrônicos, incluindo a rede, má qualidade das terminações da fibra óptica e perdas associadas, budget de potência marginal para transceptores de fibra óptica, e assim por diante.

Os relés 87L modernos usam normalmente um código de integridade de dados de 32 bits para proteger os dados do 87L. Por exemplo, ao usar um código Bose-Chaudhuri-Hocquenghem (BCH) para proteger um pacote de 255 bits, a distância mínima para detecção de erro é 10 bits, ou seja, todos os 9 erros de bits são detectados. Assumindo uma distribuição uniforme da probabilidade de corromper qualquer bit simples do pacote, a probabilidade de um erro não detectado é abaixo de  $1.2 \cdot 10^{-10}$ . Tipicamente, os relés 87L não usam nenhum algoritmo de correção de erros porque esses algoritmos degradariam a capacidade da proteção de dados. Pacotes corrompidos são rejeitados, e o algoritmo do relé recua elegantemente

## 2.2 Supervisão por Detecção de Perturbação

Qualquer proteção de integridade de dados tem uma probabilidade de falha finita, diferente de zero. Considerando que os relés 87L enviam, recebem e usam um elevado número de pacotes durante seu tempo de vida, uma segunda camada de proteção contra dados corrompidos é necessária. Por exemplo, enviando pacotes a cada 4 milissegundos, um relé trabalha com aproximadamente 7.884 bilhões de pacotes por ano. Uma verificação da integridade de dados de 32 bits é suficiente se o canal for relativamente livre de ruídos. No entanto, as aplicações de relés de proteção precisam assumir o cenário do pior caso de um ruído permanente no canal de comunicação, tal como aquele causado por um componente óptico defeituoso nos equipamentos de comunicação ou no relé. Uma probabilidade muito pequena de falha da proteção de integridade de dados ( $1.2 \cdot 10^{-10}$ , por exemplo) multiplicada pelo número extremamente alto de tentativas ( $7.884 \cdot 10^9$  por ano, por exemplo) efetuadas sob o ruído permanente resultará numa probabilidade finita, diferente de zero, de os dados corrompidos serem eventualmente aceitos, propiciando uma operação indevida do 87L. Isso não pode ser tolerado por um relé de proteção avançado. Com referência à Fig. 1, a lógica de detecção de perturbação rápida e ultrasensível supervisionando tanto a operação do 87L baseado em corrente quanto a ativação do bit de recepção da transferência direta de trip do 87 (87DTT) é a solução preferida.

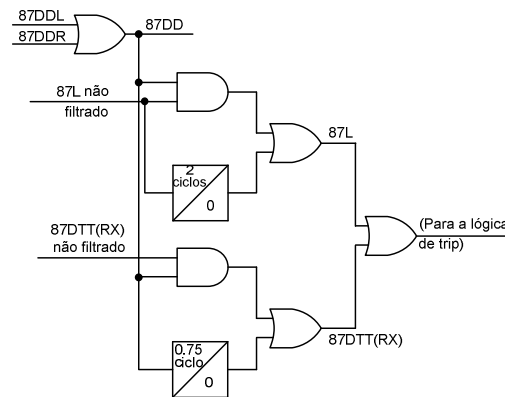


Fig. 1. Aplicação da detecção de perturbação do relé 87L

Observe que os dados corrompidos que ativariam a função 87L não filtrada ou habilitariam ilegalmente o bit 87DTT recebido seriam de curta duração, tipicamente apenas um pacote simples. Portanto, uma abordagem com retardo de tempo é usada ao supervisionar o 87L com a detecção de perturbação — a resposta da proteção é instantânea se a falta for confirmada pela detecção de perturbação e apenas ligeiramente temporizada se a detecção de perturbação falhar e não atuar. Esta precaução é implementada para maximizar a confiabilidade e atender, ao mesmo tempo, ao principal objetivo da supervisão por detecção de perturbação, validando os dados remotos com a existência de um distúrbio nas correntes ou tensões locais.

O detector de perturbação local (87DDL) pode responder às correntes de sequência (sequência-zero e positiva) e tensões de sequência (sequência-zero, positiva e negativa). As tensões são usadas para considerar as condições de alimentação fraca ("weak infeed").

Os sinais locais usados na lógica do 87DDL são obtidos antes de qualquer processamento do 87L, em particular o alinhamento dos tempos. Dessa forma, o detector de perturbação opera mais rápido, pois ele não precisa retardar os dados locais para alinhar os dados com os sinais remotos. Além disso, sendo independente do alinhamento dos tempos, o detector de perturbação local protege contra possíveis problemas associados ao alinhamento de dados que possam ser causados por qualquer desempenho incomum do canal de comunicação do 87L.

O detector de perturbação remota (87DDR) pode responder aos componentes de sequência-zero, positiva e negativa de todas as correntes remotas. Se uma determinada corrente for muito baixa, como por exemplo, quando da abertura de um disjuntor remoto ou durante condições de alimentação fraca, a corrente não é usada e a permissão é concedida para operar. Isso tem como objetivo preservar a confiabilidade da operação do 87L.

Uma vez que a perturbação tenha sido detectada, o bit 87DD é mantido por um período prolongado de tempo (dez ciclos de potência, por exemplo) para garantir uma operação confiável do 87L.

Em uma abordagem [5], ambas as partes local e remota da lógica de detecção de perturbação usam o mesmo algoritmo adaptativo representado na Fig. 2. Em primeiro lugar, uma diferença de um ciclo é calculada para o fasor de entrada IN. Esta operação é executada em uma base de amostra por amostra e produz uma resposta muito rápida e sensível devido à subtração do valor permanente do fasor de entrada IN. Subsequentemente, a magnitude

deste sinal incremental é calculada. Esta magnitude, DX, é filtrada através de um filtro de resposta ao impulso de duração infinita ("infinite impulse response" – IIR) visando ter uma indicação do ruído permanente no sinal de DX. Normalmente, este ruído permanente é muito pequeno porque mesmo sob a presença de harmônicos, os erros fasoriais tendem a ser periódicos e, como tal, serão anulados como parte do cálculo da diferença ao longo de um ciclo de potência. A entrada para o filtro IIR é limitada em valores mínimo e máximo apropriados para efeito de segurança e confiabilidade. O valor permanente do sinal de DX, multiplicado por uma constante de fábrica  $k_{TH}$ , torna-se um limiar adaptativo do comparador. Se o sinal de DX exceder tal limite, a saída OUT é ativada.

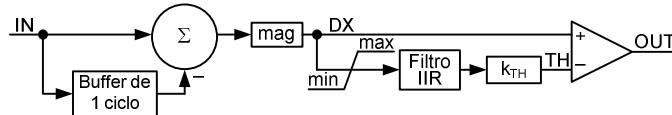


Fig. 2. Lógica do detector de perturbação adaptativa

Dessa forma, o algoritmo de detecção de perturbação é muito sensível, mas não vai atuar para condições de carga, mesmo se a corrente de carga ou as tensões forem muito distorcidas, contanto que sejam periódicas. Com a implementação desta detecção de perturbação, não há nenhuma preocupação com a confiabilidade das saídas 87DTT e 87L não filtrada supervisionada. Em primeiro lugar, a lógica de detecção de perturbação é muito confiável e rápida. Segundo, mesmo se ela falhar, o resultado final é retardado, mas ainda resulta numa operação quase instantânea da função 87L não filtrada, com um pequeno atraso de dois ciclos, e não numa falha de operação.

### 2.3 Outros Benefícios da Supervisão por Detecção de Perturbação

Considere o diagrama simplificado do esquema 87L mostrado na Fig. 3. Um esquema diferencial de corrente de linha consiste de dois ou mais relés independentes localizados em diferentes subestações, alimentados por diferentes baterias, conectados a diferentes circuitos secundários, e submetidos a diferentes condições ambientais, incluindo transitórios eletromagnéticos conduzidos e radiados e condições de descarga estática. Como os relés integrantes da zona de proteção não devem ser expostos ao mesmo ruído transitório ou problema de hardware, existe uma oportunidade para implementar esquemas 87L que executem autodiagnoses (autotestes) mais eficazes através do cruzamento de dados ("cross-checking") entre relés individuais do esquema visando proporcionar maior segurança para falhas e eventos de comunicação.

A este respeito, vale a pena observar que a detecção de perturbação protege não apenas contra erros de comunicação não detectados, mas contra vários problemas, tais como falhas do relé, aumentando enormemente a segurança do esquema 87L.

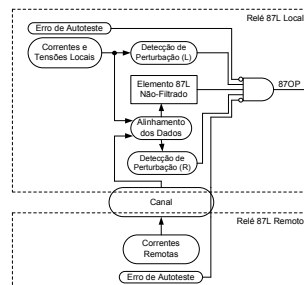


Fig. 3. A detecção de perturbação protege contra vários problemas, aumentando enormemente a segurança

Considere os seguintes modos de falha:

- Erro de comunicação não detectado (falha na verificação da integridade de dados). Neste cenário, a função 87L não filtrada, assim como o 87DTT não filtrado, pode atuar ilegitimamente devido aos dados remotos fortemente corrompidos. Pela mesma razão, o detector de perturbação respondendo às correntes remotas pode atuar (87DDR). No entanto, a parte da detecção de perturbação que responde às correntes e tensões locais (87DDL) não será ativada, evitando uma operação incorreta.
- Falha na cadeia de aquisição ca do relé local, tal como um problema no conversor analógico-para-digital ("analog-to-digital converter" – ADC). Neste cenário, a função 87L não filtrada pode atuar ilegitimamente devido aos dados locais fortemente corrompidos. Pela mesma razão, o detector de perturbação que responde às correntes e tensões locais pode atuar (87DDL). Contudo, a parte da detecção de perturbação que responde às correntes remotas (87DDR) não será ativada, evitando uma operação incorreta. Subsequentemente, o erro da autodiagnose (autoteste) será ativado no relé local em resposta ao problema, retirando-o de serviço. Dessa forma, a lógica de detecção de perturbação fornece um tempo extra para a lógica de autodiagnose e, em combinação, melhora enormemente a segurança do esquema 87L.

- Falha na cadeia de aquisição ca do relé remoto (tal como um problema no ADC). Neste cenário, a função 87L não filtrada pode atuar ilegitimamente devido aos dados remotos fortemente corrompidos. Pela mesma razão, o detector de perturbação que responde às correntes remotas (87DDR) pode atuar. No entanto, a parte da detecção de perturbação que responde às correntes e tensões locais (87DDL) não será ativada, evitando uma operação incorreta. Subsequentemente, o erro da autodiagnose (autoteste) será ativado no relé remoto em resposta ao problema, retirando-o de serviço, incluindo a função 87L remota e todas as outras instâncias da função 87L através do bit de bloqueio fornecido no pacote de dados do 87L. Dessa forma, a lógica de detecção de perturbação fornece um tempo extra para a lógica de autodiagnose e, em combinação, melhora enormemente a segurança do esquema 87L.
- Problema com o alinhamento de dados. Vamos supor um evento do canal hipotético ou uma falha de um componente interno do relé que leva transitoriamente a um desalinhamento dos dados locais e remotos (como um evento de um único distúrbio em um microprocessador). Neste cenário, a função 87L não filtrada pode atuar ilegitimamente porque dados errados das correntes locais e remotas foram comparados. Contudo, a parte da detecção de perturbação que responde às correntes e tensões locais (87DDL) não será ativada porque ela *bypassa* a operação de alinhamento totalmente, evitando uma operação incorreta do esquema 87L.

## 2.4 Verificação do Endereço do Relé

A conexão cruzada dos relés 87L consiste em outro evento de comunicação a ser considerado. Neste cenário, um determinado relé é inadvertidamente conectado a um relé remoto errado, ou o relé é conectado em loop, incorretamente, a ele mesmo ("loopback") como parte dos testes do circuito de comunicação. Os multiplexadores da classe de proteção podem evitar e acionar um alarme nas conexões cruzadas dentro do sistema SONET/SDH, mas a conexão cruzada pode ainda acontecer no nível do cabo ou do patchcord da fibra óptica entre os multiplexadores e relés. Para se proteger contra esta ameaça, os relés 87L usam endereços de transmissão, os quais são verificados na recepção de acordo com a parametrização do endereço de recepção esperado. Se os endereços, recebido e esperado, não forem compatíveis, os dados não são usados e a função 87L é retirada de serviço, emitindo, ao mesmo tempo, um alarme para o usuário.

A capacidade de cancelar a verificação do endereço é normalmente fornecida para facilitar o teste de loopback dos relés 87L.

## 3.0 - MONITORAMENTO DO CANAL NAS APLICAÇÕES DO 87L

Os esquemas diferenciais de corrente de linha são dependentes do canal e, portanto, é importante monitorar algumas características essenciais do canal em tempo real. Isso ajuda no comissionamento e na solução de problemas, mas também melhora o desempenho global do esquema ao descobrir e corrigir problemas do canal em tempo hábil. Além disso, certas características do canal podem ser usadas automaticamente pela função 87L para efetuar ajustes mais seguros, chavear para um canal redundante, se aplicável, e muito mais.

### 3.1 Tempo de Ida e Volta e Mudança Súbita na Temporização

O termo "tempo de ida e volta do canal" refere-se à soma da latência do canal nas direções de transmissão e recepção. Este é um atributo importante do canal porque tem impacto sobre o tempo de trip total do esquema 87L. Nas aplicações com conexões de fibra óptica direta ponto-a-ponto, o tempo de ida e volta do canal é constante e não deve variar. Nas aplicações com canais multiplexados, o tempo de ida e volta pode variar quando o sistema SONET/SDH redireciona o tráfego de dados em resposta à perda nas conexões de fibra óptica ou falha de um multiplexador.

Em qualquer caso, é de grande utilidade monitorar o tempo de ida e volta e emitir um alarme se este atraso exceder o valor máximo admissível, ou se o valor for muito alto e claramente indicar uma operação anormal do sistema de comunicação.

Uma mudança brusca no tempo de ida e volta é outro atributo importante do canal. Variações no tempo de ida e volta do canal significam eventos de chaveamento na rede de comunicação.

Emitir um alarme na ocorrência desses eventos de chaveamento pode ajudar a descobrir problemas no sistema de comunicação, independentemente de o tempo de ida e volta total estar ou não dentro da especificação de projeto do sistema.

### 3.2 Assimetria do Canal

Se fontes de tempo válidas forem conectadas a ambos os relés de um determinado canal de comunicação, é possível medir a latência do canal nas direções de recepção ( $t_{CH\_RX}$ ) e transmissão ( $t_{CH\_TX}$ ) individualmente. A diferença entre os atrasos nos dois sentidos é a assimetria do canal.

A assimetria do canal é um atributo importante do canal. Uma consideração típica é relacionada ao uso de canais simétricos no modo de alinhamento baseado no canal do 87L. Os relés com acesso ao tempo absoluto podem monitorar constantemente se o canal é realmente simétrico durante as condições de serviço, como parte do comissionamento do esquema, ou durante a solução de problemas. Isso é especialmente benéfico para os canais multiplexados ou quando forem considerados os potenciais modos de falha de qualquer componente de comunicação ativo entre quaisquer dois relés 87L.

Observe que a medição da assimetria depende das fontes de tempo de ambas as extremidades de um determinado canal. A precisão das fontes de tempo utilizadas afeta também a precisão da medição da assimetria. Esta é uma consideração importante para evitar alarmes espúrios de assimetria do canal.

### 3.3 Contagens de Pacotes Perdidos

Tipicamente, um relé 87L declara um pacote do 87L perdido se ocorrer qualquer uma das seguintes situações:

- Os dados, conforme detectados pelo código de integridade, estão corrompidos.
- O tempo decorrido desde o último pacote recebido pelo relé ultrapassa 100% mais uma margem de tempo normal entre os pacotes (tempo limite do pacote).
- A diferença entre o número de sequência que o relé recebe no pacote atual e o número de sequência que ele recebe no último pacote é diferente de exatamente 1.

O relé pode executar um contador de pacotes perdidos para contar os pacotes que foram perdidos nas dezenas de segundos mais recentes (medida instantânea da qualidade do canal). Além disso, o relé pode executar um contador de pacotes perdidos de 24 horas (medida de longo prazo da qualidade do canal). Valores limites usados para alarme são normalmente fornecidos para alertar e forçar uma ação corretiva se o canal se tornar muito barulhento, resultando em elevadas contagens de pacotes perdidos.

As contagens de pacotes perdidos podem ser usadas para estimar a BER ("Bit Error Rate" – Taxa de Erros de Bits) do canal e compará-la com a BER solicitada do departamento de comunicação que possui os canais do 87L.

### 3.4 Outras Características do Canal

Outras funções de monitoramento podem ser também fornecidas nos relés 87L, incluindo medidas como interrupção momentânea do canal ou rajada ("burst") de ruídos.

### 3.5 Monitoramento do Canal do 87L nos Multiplexadores

Algumas das funções de monitoramento e alarme do canal são similares entre os relés 87L e os multiplexadores da classe de proteção. Isso é benéfico porque a comparação das medições dos relés e multiplexadores pode ajudar enormemente na solução de alguns problemas.

Adicionalmente, como regra, os sistemas de comunicação e os relés são mantidos por grupos separados, e os alarmes de ambos os sistemas asseguram que os proprietários de ambos os equipamentos estejam cientes do problema, ao mesmo tempo, através dos respectivos sistemas de alarme familiares e confiáveis.

Além disso, os multiplexadores sempre têm acesso a uma referência de tempo comum através do princípio de transporte de dados TDM e, portanto, podem medir mais parâmetros do canal quando comparados aos relés.

Os sistemas de multiplexadores típicos SONET/SDH fornecem monitoramento de desempenho e alarme no nível de transporte, mas são cegos para problemas no nível de circuitos individuais.

Atualmente, existem sistemas SONET/SDH projetados para o transporte de dados de missão crítica, incluindo a proteção 87L. Esses sistemas fornecem um nível de monitoramento de desempenho e notificação necessários para uma rápida identificação e resposta a problemas de comunicação. Esses sistemas têm a capacidade de:

- Redirecionar as comunicações do 87L dentro de 5 milissegundos em caso de falhas dos multiplexadores ou no caminho da fibra óptica.
- Monitorar a latência e a assimetria do canal e fornecer alarmes para atrasos ou assimetria que afetem o desempenho do 87L.
- Fornecer informações do desempenho do canal sem interrupção do circuito de dados do 87L.
- Evitar conexões erradas não intencionais entre as portas de acesso para dispositivos 87L.

Existe uma enorme expectativa do usuário em relação às funções de monitoramento fornecidas para aumentar a segurança e a disponibilidade do sistema. O sistema de comunicação e o multiplexador podem fornecer em conjunto as informações necessárias para isolar e identificar rapidamente problemas de comunicação.

## 4.0 - CONSIDERAÇÕES SOBRE O ALINHAMENTO DE DADOS DO 87L

As aplicações dos esquemas 87L que exigem tempo externo precisam garantir que as fontes de tempo externas sejam desenvolvidas de acordo com as normas de proteção, considerando o caso de perda das informações de tempo. Esta seção foca nestas duas considerações importantes. O Apêndice B analisa os conceitos básicos do

alinhamento de dados nas aplicações do 87L, incluindo o alinhamento baseado no tempo externo e baseado no canal.

#### 4.1 Considerações Sobre as Aplicações das Fontes de Tempo do 87L

Os relés baseados em microprocessadores são frequentemente conectados a relógios sincronizados via GPS para garantir que os registros de faltas e da sequência de eventos sejam significativa e facilmente comparáveis ou para habilitar as aplicações de sincrofasores. Isso se aplica também aos relés 87L.

Contudo, os relés 87L podem ou não usar uma fonte de tempo externa nas respectivas funções 87L. Usar uma referência de tempo na proteção 87L (para canais assimétricos) ou abster-se em usar o tempo (para canais simétricos) consiste numa importante decisão de aplicação que tem impacto na confiabilidade do esquema global, seus modos de falha, e na necessidade de um projeto adequado das fontes de tempo e dos circuitos de distribuição de tempo em uma subestação.

Em geral, os três cenários de aplicação seguintes são possíveis:

- A função 87L não utiliza nenhuma fonte de tempo externa. Esta aplicação é possível para canais simétricos ou quase simétricos e é a mais robusta porque não depende de equipamentos extras necessários para fornecer o tempo. Ao invés disso, ela exige garantia de que os canais permanecerão simétricos. Isso funciona melhor com conexões de fibra óptica direta ponto-a-ponto.
- A função 87L usa uma fonte de tempo externa apenas para monitoramento do canal. Esta aplicação é possível para canais simétricos ou quase simétricos. Os relés usam tempo externo para melhorar o monitoramento do canal. Em particular, com a ajuda do tempo comum, é possível medir os atrasos do canal, independentemente das direções de transmissão e recepção, e calcular a assimetria do canal. Como resultado, esta aplicação pode monitorar o canal para verificar a assimetria e recuar para um modo seguro se o canal se tornar assimétrico. Portanto, esta aplicação é bastante adequada para canais multiplexados (SONET/SDH) projetados e configurados para uma operação simétrica. A aplicação requer o monitoramento da qualidade do tempo fornecido para evitar indicações falsas ou incorretas da assimetria do canal, mas a aplicação do tempo não é extremamente crítica.
- A função 87L usa uma fonte de tempo para proteção e monitoramento do canal. Esta aplicação permite canais assimétricos, mas requer que as fontes de tempo sejam projetadas de acordo com as normas de proteção e que sejam monitoradas. Uma lógica alternativa de recuo ("fallback") é necessária para cobrir situações em que o tempo externo é degradado ou está indisponível.

Historicamente, o sinal de tempo em uso é o IRIG-B. Por sua natureza, o sinal de tempo não é dinâmico, mas sim um padrão de repetição (marcação de 1 pulso por segundo [pps], código de dados e tempo, e indicação de qualidade do tempo). Como resultado, dispositivos que usam o tempo, tal como os relés 87L, têm capacidade para facilmente sustentar deficiências e perda temporária do sinal de tempo IRIG-B.

Tipicamente, o dispositivo de recepção do tempo depende do próprio relógio interno e bloqueia a fase ("phase-locks") do relógio interno para a entrada IRIG-B. Isso pode incluir uma calibração on-line do relógio interno — um ajuste contínuo da frequência do relógio baseado no tempo decorrido entre pulsos de 1 pps consecutivos. Como resultado, o relógio interno torna-se muito preciso e pode fornecer suporte durante a perda do sinal IRIG-B na faixa de dezenas de segundos, apesar da precisão finita e variabilidade dos componentes do relé ou variações de temperatura.

Sob esta perspectiva, a segurança da distribuição do tempo IRIG-B é mais importante do que a confiabilidade.

Para fornecer uma segurança apropriada, o dispositivo de recepção de tempo monitora a integridade do sinal IRIG-B. Isso normalmente inclui um jitter no sinal de 1 pps, consistência do código de dados e tempo e, mais importante, os bits de qualidade de tempo incorporados ao sinal IRIG-B conforme IEEE C37.118 [6].

Aplicações de tempo críticas, tais como a proteção 87L e os sincrofasores, requerem o uso de relógios com capacidade de ativação dos bits de qualidade de tempo para informar aos dispositivos de recepção de tempo sobre possível erro de tempo, tal como durante "freewheeling", uma operação sem restrições, quando é incapaz de bloquear os satélites do GPS.

Ao usar o tempo para a proteção 87L, precisamos tratar os circuitos de distribuição e fontes de tempo como parte do esquema de proteção. Isso exige o seguinte:

- Usar a devida diligência ao selecionar componentes da rede de tempo.
- Aplicar blindagem e aterramento adequados às conexões baseadas em cobre, observando a carga ("burden") máxima para as saídas, e seguindo as recomendações para a distância máxima dos cabos de cobre.
- Aplicar a distribuição de IRIG-B baseada em fibra óptica para caminhos mais longos.
- Documentar as redes de distribuição de tempo com diligência.
- Incluir os relógios e as redes de distribuição de tempo nos rigorosos procedimentos de comissionamento e programas de testes periódicos [3].
- Monitorar os relógios do satélite e os relés para falhas dos sinais de tempo e atender aos alarmes de forma oportuna.

Quando for aplicar os esquemas diferenciais de corrente de linha sobre canais assimétricos, os sinais de tempo tornam-se tão importantes quanto a corrente, tensão ou sinais de trip e precisam ser projetados, fabricados, comissionados e mantidos em conformidade com as normas de proteção.

#### 4.2 Estratégias Alternativas para o Alinhamento Baseado no Tempo

Os esquemas 87L que usam fontes de tempo externas têm que fornecer uma resposta bem definida que atenda às preferências do usuário nas situações em que a fonte de tempo é perdida ou degradada. Isso é frequentemente conhecido como lógica alternativa de tempo (“time fallback logic”). Um relé moderno pode fornecer vários modos alternativos de tempo (“time fallback mode”), variando em relação ao equilíbrio entre segurança e confiabilidade com a perda do tempo. Ao selecionar um modo fallback, geralmente consideramos a disponibilidade do segundo esquema de proteção redundante, bem como as restrições regulamentares ou práticas internas da concessionária relativas à operação de uma linha sem esquemas redundantes com capacidade de eliminação instantânea da falta. Considere a aplicação de dois terminais com dois canais representada na Fig. 4. Tipicamente, um canal (assumir o Canal 1) é uma conexão de fibra óptica direta ponto-a-ponto, enquanto o canal de retaguarda (Canal 2) é um canal multiplexado. Assumir também que o canal multiplexado não pode ser considerado, com certeza, como sendo simétrico. Esta aplicação pode usar o alinhamento baseado no canal para o Canal 1 e o alinhamento baseado no tempo para o Canal 2, com ambos os relés conectados a fontes IRIG-B válidas. Vamos assumir que seja usado o modo fallback de tempo, Modo 2. Neste cenário, o esquema é imune a problemas relativos ao tempo desde que o Canal 1 esteja disponível. Se qualquer um dos relés perder a fonte de tempo, o Canal 2 é marcado como inutilizável, indicando que o esquema perdeu a redundância do canal, mas continua operando enquanto o canal primário estiver disponível. É necessário que haja tanto a perda de qualquer uma das fontes de tempo quanto a perda do Canal 1 para que o esquema da Fig. 4 perca a confiabilidade.

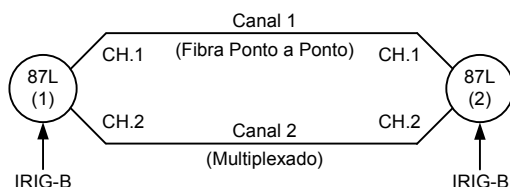


Fig. 4. Aplicação de dois terminais com canais redundantes

Considere a aplicação mestre de três terminais representada na Fig. 5. Assumir que o Canal 1 não pode ser considerado, com certeza, como sendo simétrico, enquanto os Canais 2 e 3 têm a garantia de serem simétricos. Como resultado, o CH.1 do Relé 2 e o CH.2 do Relé 1 são configurados para usar o alinhamento baseado no tempo e os Relés 1 e 2 têm que ter fontes de tempo válidas conectadas. Vamos assumir que seja usado o modo fallback de tempo, Modo 2. Se o Relé 1 ou o Relé 2 perder a fonte de tempo, o Canal 1 é marcado como inutilizável, indicando que o Relé 1 não pode usar os dados do Relé 2 e o Relé 2 não pode usar os dados do Relé 1. Como resultado, os Relés 1 e 2 comutam para os modos escravos, enquanto o Relé 3 recebe todos os dados via Canais 2 e 3 simétricos, e continua protegendo a linha no modo mestre, enviando trips diretos para os Relés 1 e 2 escravos. Dessa forma, a confiabilidade é preservada apesar da perda dos sinais de tempo.

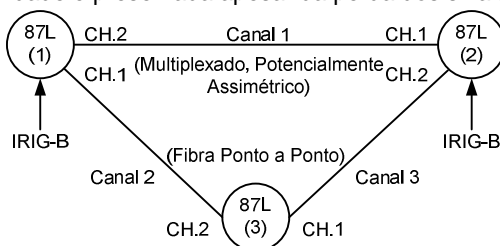


Fig. 5. Aplicação de três terminais com três canais (todos os relés são mestres)

Considere a aplicação de dois terminais com um canal representada na Fig. 6. O canal pode ou não ser simétrico e, portanto, o alinhamento baseado no tempo é usado, e ambos os relés têm que ser conectados a fontes IRIG-B válidas. Tendo o tempo absoluto disponível, ambos os relés medem a assimetria do canal. Vamos assumir que seja usado o modo fallback de tempo, Modo 4.

Se a assimetria do canal for pequena no instante da perda do tempo em qualquer um dos relés, os relés vão chavear para o modo baseado no canal e continuar a fornecer proteção. Se o canal for subsequentemente comutado na rede multiplexada, conforme detectado por uma mudança súbita no tempo de ida e volta, a função 87L é bloqueada.

Se no instante da perda do tempo, o canal não for simétrico, a função 87L é bloqueada imediatamente no modo fallback de tempo, Modo 4.

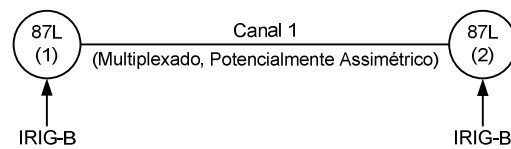


Fig. 6. Aplicação de dois terminais com um único canal potencialmente assimétrico

#### 4.3 Distribuição de Tempo Terrestre

O uso do tempo em uma área ampla nas aplicações de proteção tem sido historicamente abordado com alguma relutância. Não apenas o esquema de proteção global é mais complexo e, portanto, menos confiável, mas também o tempo da área ampla depende da acessibilidade do sistema GPS originalmente configurado para aplicações militares e controlado pelo Departamento de Defesa dos Estados Unidos ("Department of Defense" – DoD). Recentemente, um método de distribuição de tempo terrestre foi proposto, superando as diversas preocupações relativas ao uso do GPS nas aplicações de proteção [7].

#### 5.0 - CONCLUSÃO

A proteção diferencial de corrente de linha fornece um excelente desempenho e simplicidade de aplicação sob o ponto de vista da engenharia de proteção tradicional. Os modernos relés e multiplexadores executam diversas funções de monitoramento do canal. Essas medições em tempo real devem ser habilitadas e usadas para emitir alarmes. Elas melhoram o desempenho global dos esquemas 87L ao chamar a atenção para os problemas, forçando a manutenção adequada dos equipamentos para condições que poderiam eventualmente impactar os esquemas de proteção 87L, se não atendidas em tempo hábil. Além disso, elas são úteis no comissionamento, testes e solução de problemas. A segurança no uso do tempo nas aplicações do 87L torna-se possível devido à disponibilidade da distribuição de tempo mais segura em uma ampla área terrestre. Os sistemas de tempo terrestres tornam os sinais de tempo menos dependentes do sistema GPS, eliminando assim muitas das preocupações tradicionais associadas ao alinhamento das correntes do 87L baseado no tempo e aplicações através de canais assimétricos. As aplicações do 87L são inerentemente multidisciplinares e envolvem ambos os departamentos de proteção e comunicação da organização do usuário. Promover a educação cruzada, incentivando análises conjuntas de mudanças, e usando a mesma linguagem, mais precisa, entre os grupos de engenharia de proteção e comunicação, resulta numa melhor compreensão dos requisitos essenciais e no melhor desempenho global dos esquemas 87L.

#### 6.0 - REFERÊNCIAS BIBLIOGRÁFICAS

- [1] CIGRE JWG 34/35.11, *Protection Using Telecommunications*, agosto de 2001.
- [2] B. Kasztenny, G. Benmouyal, H. J. Altuve, and N. Fischer, "Tutorial on Operating Characteristics of Microprocessor-Based Multiterminal Line Current Differential Relays," proceedings of the 38th Annual Western Protective Relay Conference, Spokane, WA, outubro de 2011.
- [3] D. Finney, N. Fischer, B. Kasztenny, and K. Lee, "Testing Considerations for Line Current Differential Schemes," proceedings of the 38th Annual Western Protective Relay Conference, Spokane, WA, outubro de 2011.
- [4] IEEE Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations, IEEE 1613-2003, 2003.
- [5] H. Miller, J. Burger, N. Fischer, and B. Kasztenny, "Modern Line Current Differential Protection Solutions," proceedings of the 63rd Annual Conference for Protective Relay Engineers, College Station, TX, março de 2010.
- [6] IEEE Standard for Synchrophasors for Power Systems, IEEE C37.118-2005, 2005.
- [7] K. Fodero, C. Huntley, and D. Whitehead, "Secure, Wide-Area Time Synchronization," proceedings of the 12th Annual Western Power Delivery Automation Conference, Spokane, WA, abril de 2010.
- [8] Telcordia Technologies GR-253-CORE, *Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria*, Issue 4, dezembro de 2005.
- [9] J. S. Warner and R. G. Johnston, "GPS Spoofing Countermeasures," Los Alamos National Laboratory, dezembro de 2003. Disponível em: [http://www.homelandsecurity.org/bulletin/Dual%20Benefit/warner\\_gps\\_spoofing.html](http://www.homelandsecurity.org/bulletin/Dual%20Benefit/warner_gps_spoofing.html).
- [10] U.S. Coast Guard Navigation Center (U.S. Department of Homeland Security), "Overview of the U.S. Federal Government's Policy on Activities Which May Cause Interference to GPS." Disponível em: <http://www.navcen.uscg.gov/?pageName=gpsServiceInterruptions>.